On the Feasibility of Load-Changing Attacks in Power Systems During the COVID-19 Pandemic

JUAN OSPINA[ID]**1, (Member, IEEE), XIAORUI LIU**[ID]**1, (Student Member, IEEE),
CHARALAMBOS KONSTANTINOU**[ID]**1, (Senior Member, IEEE),
AND YURY DVORKIN**[ID]**2, (Member, IEEE)**
[1]Center for Advanced Power Systems, FAMU-FSU College of Engineering, Florida State University, Tallahassee, FL 32310, USA
[2]Department of Electrical and Computer Engineering, Center for Urban Science and Progress, New York University, Brooklyn, NY 11201, USA

Corresponding author: Charalambos Konstantinou (ckonstantinou@ieee.org)

ABSTRACT The electric power grid is a complex cyberphysical energy system (CPES) in which information and communication technologies (ICT) are integrated into the operations and services of the power grid infrastructure. The growing number of Internet-of-things (IoT) high-wattage appliances, such as air conditioners and electric vehicles, being connected to the power grid, together with the high dependence of ICT and control interfaces, make CPES vulnerable to high-impact, low-probability load-changing cyberattacks. Moreover, the side-effects of the COVID-19 pandemic demonstrate a modification of electricity consumption patterns with utilities experiencing significant net-load and peak reductions. These unusual sustained low load demand conditions could be leveraged by adversaries to cause frequency instabilities in CPES by compromising hundreds of thousands of IoT-connected high-wattage loads. This article presents a feasibility study of the impacts of load-changing attacks on CPES during the low loading conditions caused by the lockdown measures implemented during the COVID-19 pandemic. The load demand reductions caused by the lockdown measures are analyzed using dynamic mode decomposition (DMD), focusing on the March-to-July 2020 period and the New York region as the most impacted time period and location in terms of load reduction due to the lockdowns being in full execution. Our feasibility study evaluates load-changing attack scenarios using real load consumption data from the New York Independent System Operator (NYISO) and shows that an attacker with sufficient knowledge and resources could be capable of producing frequency stability problems, with frequency excursions going up to 60.5 Hz and 63.4 Hz, when no mitigation measures are taken.

INDEX TERMS Cyberphysical energy systems, COVID-19 pandemic, load-changing attacks, dynamic mode decomposition, electric power systems, frequency stability.

I. INTRODUCTION

The wide-scale deployment of information, sensing, and communication technologies in electric power systems (EPS) contribute to various power grid functionalities. For example, Internet-of-Things (IoT) devices are widely utilized in industrial assets to provide control and monitoring support for supervisory control and data acquisition (SCADA), advanced metering infrastructure (AMI), and other types of communication and control infrastructures. As a result, during the last few years, the efficiency, robustness, and reliability of cyberphysical energy systems (CPES) have been greatly improved. At the same time, the vulnerabilities inherited from the IoT ecosystem have expanded the CPES threat surface.

The associate editor coordinating the review of this manuscript and approving it for publication was Noor Zaman[ID].

The roll-out of customer-end IoT-controllable high-wattage devices and distributed energy resources (DERs) unlocks new vulnerabilities on the demand-side of CPES and opens new avenues for adversaries to launch large-scale coordinated remote attacks on power system's assets. For example, DERs or modern controllable loads use IoT devices to coordinate their operations with other CPES (e.g., via IoT-based smart meters or other home assistants such as Amazon Echo and Google Home). Naturally, these IoT interfaces become great attack vectors due to the countless vulnerabilities engendered by the complex IoT supply chains. Insecure remote login passwords of IoT devices can be exploited for malware infection as in the Mirai botnet which, in 2016, successfully compromised thousands of household IoT devices in a distributed denial-of-service campaign [1]. Firmware updates are another source of contamination [2], making

consumer devices such as printers [3] and relay controllers [4], [5] vulnerable to firmware attacks. Ghost domain name system (DNS) attacks can infect IoT devices by routing them to malicious DNS servers [6]. Attacks on electricity consumers and DERs are essentially facilitated by the negligence of the customers that use default or weak security credentials [7].

Adversaries capable of compromising IoT-controllable high wattage loads and DERs of CPES can maliciously affect the stability of the grid, causing degradation of grid equipment or even power outages and large-scale blackouts [8]. Although currently hypothetical due to the low penetration rates of high-wattage loads and DERs (prosumers), these types of attacks are projected to become realistic in the near future as the penetration rates are anticipated to grow exponentially [9]. Due to the distributed nature of *load-changing attacks*, which disturb the system from the demand-side, as well as the various ways of attack payload weaponization [10], it is difficult for system operators to detect and mitigate such attacks in order to maintain frequency stability and ensure that voltage and frequency levels are within operational limits. In addition, IoT-based attacks to CPES do not require operational knowledge of the power system and are very easy to repeat.

Starting in early 2020, the COVID-19 pandemic has directly affected businesses and individuals, significantly increasing their dependency on the Internet (e.g., remote work). This reliance expanded the number of cyberspace-related incidents as malicious attempts have proliferated to exploit this sudden unplanned shift in society. COVID-19 drives criminal and political cyberattacks across networks, cloud, and mobile phones; pandemic-related attacks increased exponentially from under 5,000 per week in February 2020, to over 200,000 per week in late April 2020 [11]. For instance, COVID-19 scams often use phishing emails and malicious websites to promote fake vaccines and cures, fraudulent charity drives, and false information on government aid, while at the same time delivering malware to unsuspecting users and insecure services. Table 1 shows a summary of some of the most prominent threats and vulnerabilities exacerbated due to the COVID-19 pandemic and lockdown measures. Example attack categories range from malware, Zoom bombing, and phishing attacks all the way to sophisticated critical infrastructure attacks that

could compromise the integrity of the power grid. Due to the barrage of cyberattacks during COVID-19, the malicious exploitation potential of ICT and control interfaces of IoT-controllable loads could, more than ever before, constitute a realistic cyber-threat to power grid operations.

II. RELATED WORK & CONTRIBUTIONS
A. LOAD-CHANGING ATTACKS
Existing work on load-changing attacks[1] has focused on the modeling and analysis of attack vectors in which system conditions, e.g., electric power demand and electricity prices, make use of forecasting models which do not account for sudden reductions in peak demand and delivered energy nor modification of consumption patterns [24]. The authors in [25] have demonstrated that load-changing attacks can cause controlled load shedding but not cascading failures. Sudden IoT attacks increasing the system load demand will cause under frequency load shedding (UFLS) control to split the frequencies of the buses into islands of different operating regions of the grid when the system cannot handle the load and the frequency drops. In [22], the authors investigated the feasibility of a load-changing attack using compromised electric vehicles (EVs). After canvassing publicly available data, they recovered the exact configuration of the high-voltage power grid and public EV charging stations (EVCS) in Manhattan, NY. Using this publicly available data, the work designed a data-driven attack mechanism requiring from around 500 to about 5,000 compromised Tesla EVs, depending on grid conditions and attack parameters, to destabilize the frequency, leading to a major blackout. Furthermore, a dynamic load-changing attack against power system stability is studied in [20]. The authors formulated the problem as a close-loop attack in which a dilettante adversary controls the changes in the compromised load based on the system frequency feedback.

B. IMPACT OF COVID-19 IN POWER SYSTEMS
The recent novel coronavirus disease (COVID-19) severely affected the entire globe as a public health and economic crisis. At the same time, the COVID-19 pandemic caused substantial changes in the operations of bulk power systems and electricity markets. One of the most evident effects of the health crisis on EPS is the reduction in peak demand and consumed energy; electricity demand remains lower than typical expectations during the pandemic in many regions of the world. For example, the electricity demand in June 2020 in EU countries was 10% below the 2019 levels. In Italy, the 2019-2020 year-on-year change in electricity demand, weather corrected, reached 28% during the 15th week of 2020 [26]. Similarly in Spain, the electricity consumption decreased by 13.5% during the

TABLE 1. Threats and vulnerabilities increased during COVID-19 pandemic.

Threats and vulnerabilities	Online resource
Malware and phishing	[12] [13]
Spyware and phishing	[14]
Ransomware	[14]
ZOOM bombing	[15] [16]
Health check – ISPs, cloud providers, UCaaS during pandemic	[17]
Critical power grid infrastructure attacks	[18] [19]

[1]Prior work has used the names "manipulation of demand via IoT attack (MadIoT)" [8], "dynamic load-altering attack (DLAA)" [20], "coordinated load changing attack" [21], "demand-side cyberattacks" [22], and "power botnet attacks" [23]. Our terminology of *load-changing attacks* refers to such attack strategies aiming in a coordinated way to control IoT connected high-wattage appliances and DERs.

March-to-April period when compared to the average load consumption of the last five years due to the lockdown measures implemented to stop the spread of the COVID-19 pandemic [27]. The reduction was mainly observed during working days with an average 14.5% reduction while during weekends the reduction observed was around 10.6%. In the African region, one example is the study conducted by researchers in [28], where an exploratory research aimed at investigating the impacts caused by the COVID-19 pandemic in the South African power grid was performed. According to the authors, the electricity consumption and peak demand in South Africa decreased by 28.1% and 20.2%, respectively; exacerbating issues in the reliability of the South African electric grid. Furthermore, in the East Asian region, and more specifically in China, a 13% electricity demand drop, during the lockdown period, was observed [29].

COVID-19 lockdown measures are also being analyzed for several cities and regions of the United States (U.S.). One example is the study conducted in [29], where researchers found that New York City's (NYC) hourly demand in mid-April 2020 ranged from roughly 5% to 21% below typical levels while reductions in electric consumption averaged 21% below expected values during the 8 am hour. Similarly, researchers in [30] explored the impacts that the stay-at-home orders (SAHO), issued in response to the COVID-19 pandemic, had on the regional electricity generation fuel mixes in three major Regional Transmission Operators (RTOs) in the U.S., i.e., New York Independent System Operator (NYISO), Midcontinent Independent System Operator (MISO), and Pennsylvania Jersey Maryland (PJM). The authors use of the Shannon-Wiener diversity index, an index designed to measure the fuel diversity of a generation portfolio, in order to compare the before and after SAHO periods in terms of electricity generation fuel mixes. Even though they did not find any significant difference in the average diversity index between the two periods, the variance (i.e., σ^2) of the index for MISO, NYISO, and PJM was significant, with a lower 35% value for the first two RTOs and an 8% higher value for the latter.

The impact on energy consumption and peak demand as well as the alternation of the consumption patterns has brought numerous challenges for utilities and system operators. Different practices have been followed to proactively mitigate technical issues and maintain normal operating conditions of CPES [24]. Examples include switching off and on automatic voltage control systems, capacitors, and reactors, utilizing STATCOM (static synchronous compensator) and UPFC (unified power flow controller) devices to absorb reactive power, or the use of automatic UFLS and reserve arrangements, among others. In [31], a comprehensive review of the implications of the COVID-19 pandemic for the electric industry is presented. In this review, the impacts that the pandemic caused in the power balance and electricity prices are explored, with the main focus on exploring how the uncertainty of load demand, voltage violation conditions, and other challenges have posed higher pressure on system

operators and system maintenance. According to the authors, in most countries that applied lockdown measures, the total load demand decreased, and this, in turn, increased the uncertainty of load and posed higher requirements for load forecasting accuracy and system reserves. A similar study is presented in [32], where authors explore the impacts of the pandemic on the U.S. electricity demand and supply. The work performs an analysis of the electricity consumption data up to the end of May 2020 and examines some of the variables (e.g., daily peak, demand ramp rate, demand forecast error, and net electricity interchange, etc.) that could indicate stress on the power grid. The study conducted is limited to three states: California, Florida, and New York, and concluded that the effect of the pandemic may not only be a simple reduction in the load, but there exist noticeable differences among the examined regions during the SAHOs. Focusing on smaller electric grids, the research in [33] presents a detailed study regarding the impact that the COVID-19 pandemic had on the operation of the Estonian, Israeli, and Finnish grids with a special focus on three major effects: changing patterns in generation and consumption, frequency stability, and high integration of renewables. The authors concluded that the reduction of load consumption during a pandemic-type event affects considerably the management and control of generation units and leads to voltage and frequency deviations that reduce the reliability of the system. For these reasons, the addition of tools and regulation devices designed to manage abnormal events and mitigate reliability problems is suggested in the long-term planning of the grid infrastructure.

C. CONTRIBUTIONS & METHODOLOGY

This article focuses on analyzing the feasibility of load-changing attacks in power systems during the 2020 COVID-19 pandemic while using the previous year (2019) as a baseline. The methodological approach to investigate the feasibility of load-changing attacks in CPES is presented in Fig. 1. The contributions of this article, highlighting also the differences between the proposed work and the reviewed literature, can be summarized as follows:

- A methodology for investigating the feasibility of load-changing attacks in CPES during pandemic-type events is proposed as depicted in Fig. 1. The proposed methodological approach consists of three main steps: *(i)* An analysis of the impact of the COVID-19 lockdown measures in load consumption, *(ii)* Modeling of realistic high-impact, low-probability load-changing attacks, and *(iii)* A feasibility analysis that evaluates the impact of the modeled load-changing attacks in a compromised CPES.
- In order to accomplish *(i)*, dynamic mode decomposition (DMD) and statistical analyses of load consumption data during the COVID-19 outbreak are performed. The objective of these analyses is identifying dynamic load patterns that could cause abnormal loading conditions in CPES, and thus create vulnerable circumstances that attackers could use in their advantage to perform
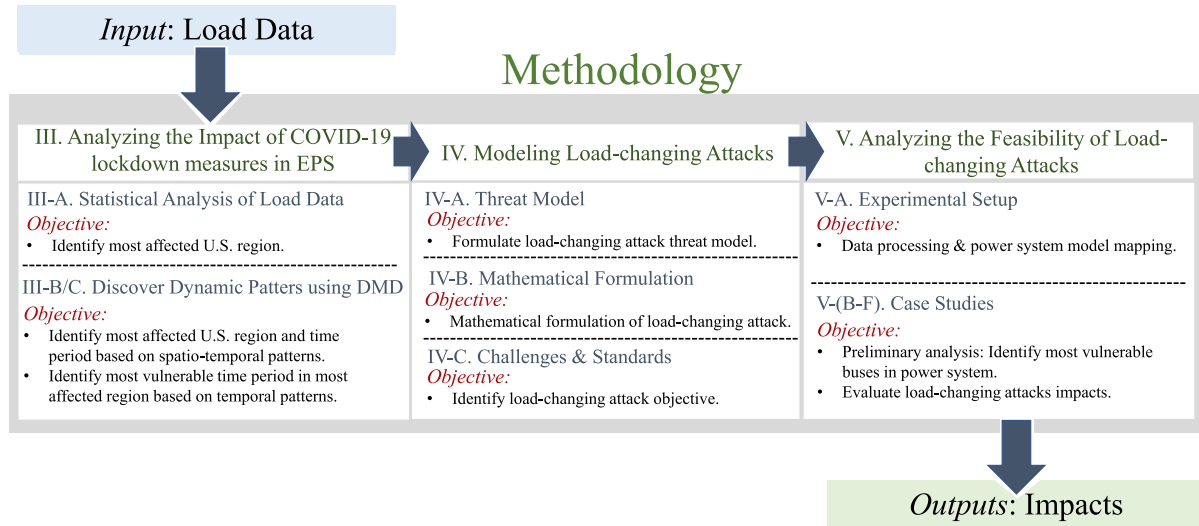
FIGURE 1. Methodological approach for analyzing the feasibility of load-changing attacks.

load-changing attacks. Using these analyses, we are able to identify the most affected U.S. region and time periods by recognizing spatio-temporal patterns.

- In order to realize *(ii)*, mathematical and threat model formulations are designed in order to methodically examine a realistic high-impact, low-probability threat targeted at creating frequency instabilities. We investigate the possibility of attackers compromising power system stability taking into consideration abnormal loading conditions caused by lockdown measures as the ones observed during the COVID-19 pandemic.
- In order to accomplish *(iii)*, the analyses and threat model developed are used in conjunction to experimentally examine and simulate load-changing attack scenarios. The investigation demonstrates that such events can adversely impact the frequency of CPES during the decreased load demand conditions caused by COVID-19 lockdown measures.

The rest of the paper is organized as follows. In Section III, the impact of the lockdown measures is evaluated based on the COVID-19 pandemic response timeline using DMD and statistical analyses. The most affected region in the U.S. is identified and then used jointly with the threat model presented in Section IV. In Section IV, the threat model of load-changing attacks and the operational standards for frequency stability are presented. Section V presents the experimental setup and results of the case studies used to evaluate the feasibility of load-changing attacks during low net-load demand periods, as the ones observed during the COVID-19 pandemic. Finally, Section VI presents conclusions and future work.

III. ANALYZING THE IMPACT OF COVID-19 LOCKDOWN MEASURES IN EPS THROUGHOUT THE U.S

Before examining the feasibility of load-changing attacks in CPES during the COVID-19 pandemic, it is important

to first understand the impact that the lockdown measures, due to the novel COVID-19 pandemic, had in the electricity consumption around the U.S. In order to understand this impact, we obtained and analyzed electricity consumption data obtained from a cross-domain open-source data hub, COVID-EMDA [34]. This data hub integrates weather, satellite imaging, mobile device location, and electricity market data from seven regions that cover some of the top hardest-hit states in the U.S, i.e., California, Texas, Midcontinent Central region, Kansas, Illinois, New York, and Massachusetts. In this article, we focus our attention in analyzing seven main representative urban areas that belong to the major RTOs in the U.S. Urban areas have been the most affected areas by COVID-19 spread and lockdown measures; according to the United Nations (UN), they have become the epicentre of the pandemic with more than 90% of all reported cases [35], [36]. The representative urban areas analyzed and their corresponding RTO are:

1) Houston - ERCOT
2) Boston - ISO-NE
3) Central - MISO
4) New York City (NYC) - NYISO
5) Chicago - PJM
6) Kansas City - SPP
7) Los Angeles - CAISO

A. COVID-19 OUTBREAK TIMELINE & QUANTIFICATION OF LOAD DEMAND CHANGES DUE TO COVID-19: 2019 VS. 2020

In order to understand the load demand changes and the magnitude of the COVID-19 impacts across the seven major regions examined, we first analyze the possible reasons of why such changes occurred. Thus, we compiled a series of important events, in a timeline, that correlate with the load variation during the outbreak. Fig. 2 shows the timeline for the different regions analyzed. As seen in this timeline,
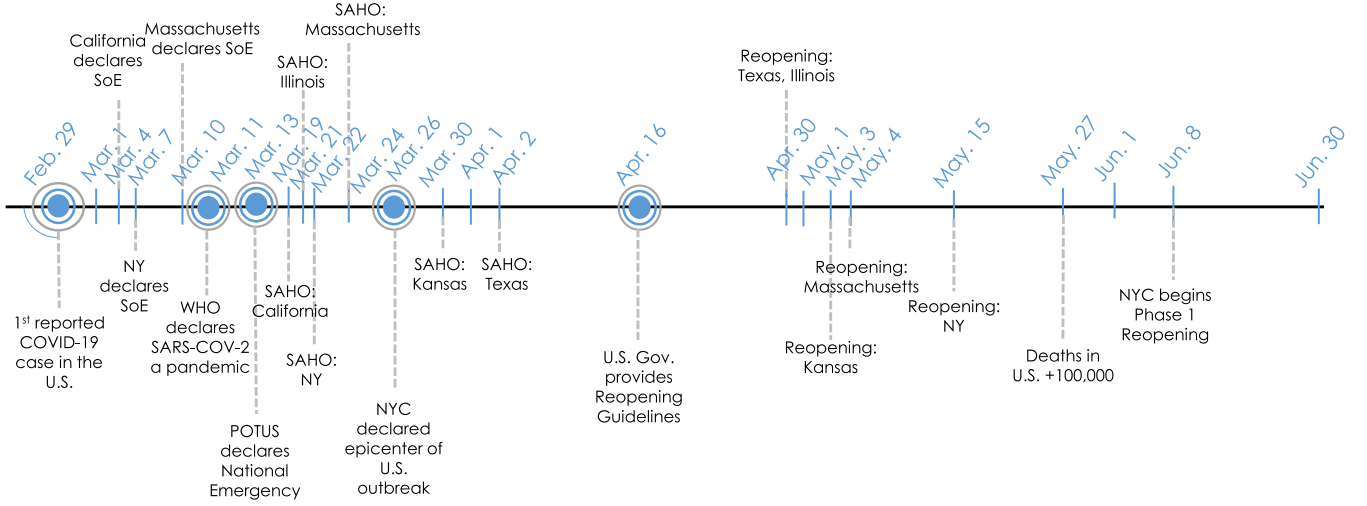
FIGURE 2. COVID-19 response timeline from March 1st to June 30th, 2020, with the most important events for the seven states analyzed. SoE - state of emergency, SAHO - stay-at-home-order, WHO - World Health Organization, POTUS - President of the United States.

the majority of the lockdown measures in the analyzed states occurred during the March-to-May period of 2020. Also, it should be noted that re-openings in most of these places occurred during the second and third weeks of May. Based on this timeline, we selected the period ranging from March 1st to June 30th as the one to compare with the previous year (2019) for load consumption comparisons and impact analysis.

In Fig. 3, we can observe how the electricity consumption in the major U.S. zones and RTOs during the COVID-19 pandemic of 2020 was notably reduced, compared to 2019, during the period of March 1st to June 30th. The most affected time periods are the ones between 6 am and 12 pm in all regions. Also, the most affected city due to the lockdown measures is clearly NYC since a significant load demand reduction can be observed at all times during the lockdown period. In regions such as Central-MISO and NYC-NYISO, overall low net-load demand conditions can be observed throughout the day. In NYC, the highest load difference between the average load of 2019 and 2020 is found at the time period of 11 am to 12 pm, where a load difference of around 860 MW exists (around 10% of the total maximum load). Similarly, in Central-MISO, the highest load difference between the average load of 2019 and 2020 is found at the time period of 7 am to 8 am, where the load difference is around 2,020 MW (around 5% of the total maximum load). These results indicate that NYC is one of the most affected regions by the COVID-19 lockdown measures, and thus, we focus our attention on this region.

B. DISCOVERING DYNAMIC PATTERNS IN THE REDUCTION OF LOAD CONSUMPTION CAUSED BY COVID-19 ACROSS THE U.S

DMD is a recently developed method capable of performing spatio-temporal decomposition of high-dimensional data [37]. This process captures snapshots or measurements

in time from a given system and decomposes them into dynamic modes or patterns that can be used to explain the system's behavior. In our case, our 'system' is determined by the load consumption data during the time period of the COVID-19 outbreak of some of the most affected regions in the U.S. In order to apply DMD, we structure the load consumption data: x_{m+1} represents future measurements (snapshots) and x_m represents previous measurements from the vector $x \in \mathbb{R}^n$; where n represents the number of spatial points at each snapshot. For data pairs in x, a best-fit linear operator matrix A is defined as:

$$x_{m+1} = Ax_m \tag{1}$$

where x_m is equal to $x_m = [x_1, x_2, \ldots x_n]$ at snapshot *m*. In our case, the spatial points *n* represent the individually normalized load consumption values for different affected regions across the U.S. It is important to note that according to [37], the relationship presented in Eq. (1) does not need to be exact since other theoretical works have demonstrated the approximation of A (i.e., the full high-dimensional system matrix) as $\tilde{A}$ (i.e., the rank-reduced representation) can be used for complex non-linear system applications [38]. This approximation is useful as it avoids the computational complexity of performing the full eigendecomposition of the high-dimensional system matrix. Using this relationship, we can essentially separate our dynamic system into datasets:

$$X = \begin{bmatrix} x_1 & x_2 & \ldots & x_{m-1} \end{bmatrix} \tag{2}$$

$$X' = \begin{bmatrix} x_2 & x_3 & \ldots & x_m \end{bmatrix} \tag{3}$$

where X and $X' \in \mathbb{R}^{n \times m-1}$. Combining Eq. (1), (2), and (3), the relationship of the states in our system can be described as:

$$X' \approx AX \tag{4}$$
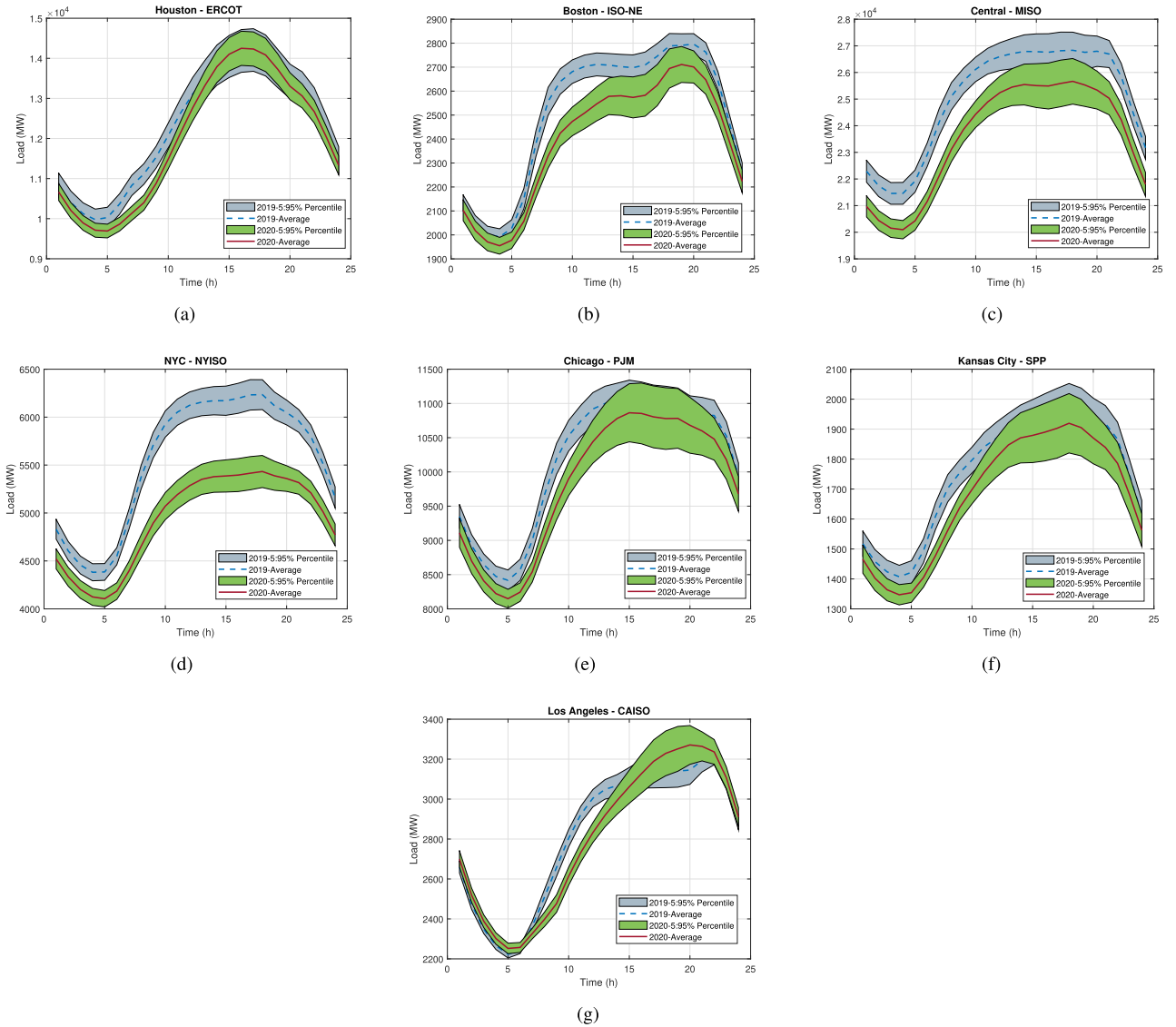
FIGURE 3. 2019 and 2020 load demand 5% to 95% percentiles for: a) Houston - ERCOT, b) Boston - ISO-NE, c) Central region - MISO, d) New York City (NYC) - NYISO, e) Chicago - PJM, f) Kansas City - SPP, and g) Los Angeles - CAISO.

where the DMD modes, also called dynamic modes of the evaluated dynamical system, are the eigenvectors of A, while each DMD mode corresponds to a particular eigenvalue of the matrix A [37]. However, as mentioned before, in a high-dimensional system, the matrix A may be intractable to be analyzed directly. So, in order to avoid the full eigendecomposition of A, DMD makes use of its rank-reduced representation in terms of the proper orthogonal decomposition-projected matrix, Ã. All the steps necessary for performing DMD in a given dataset are presented below:

1) Perform the singular value decomposition (SVD) of X:

$$X \approx U\Sigma V^* \qquad (5)$$

where * denotes the conjugate transpose, and $U \in \mathbb{C}^{n \times r}$, $\Sigma \in \mathbb{C}^{r \times r}$, and $V \in \mathbb{C}^{m \times r}$. Here, r is the rank

of the reduced (truncated) SVD approximation to X. For more details regarding the process and benefits of truncation in DMD see [37].

2) Calculate the matrix A using the pseudoinverse of X obtained using SVD:

$$A \approx \tilde{A} = X'V\Sigma^{-1}U^* \qquad (6)$$

3) Compute the eigendecomposition of Ã:

$$\tilde{A}W = W\Lambda \qquad (7)$$

where the columns of W are eigenvectors and Λ is the diagonal matrix that contains the respective eigenvalues.

4) Finally, the reconstruction of A can be performed using W and Λ, where the eigenvalues of A are determined using Λ and the eigenvectors, that represent the patterns
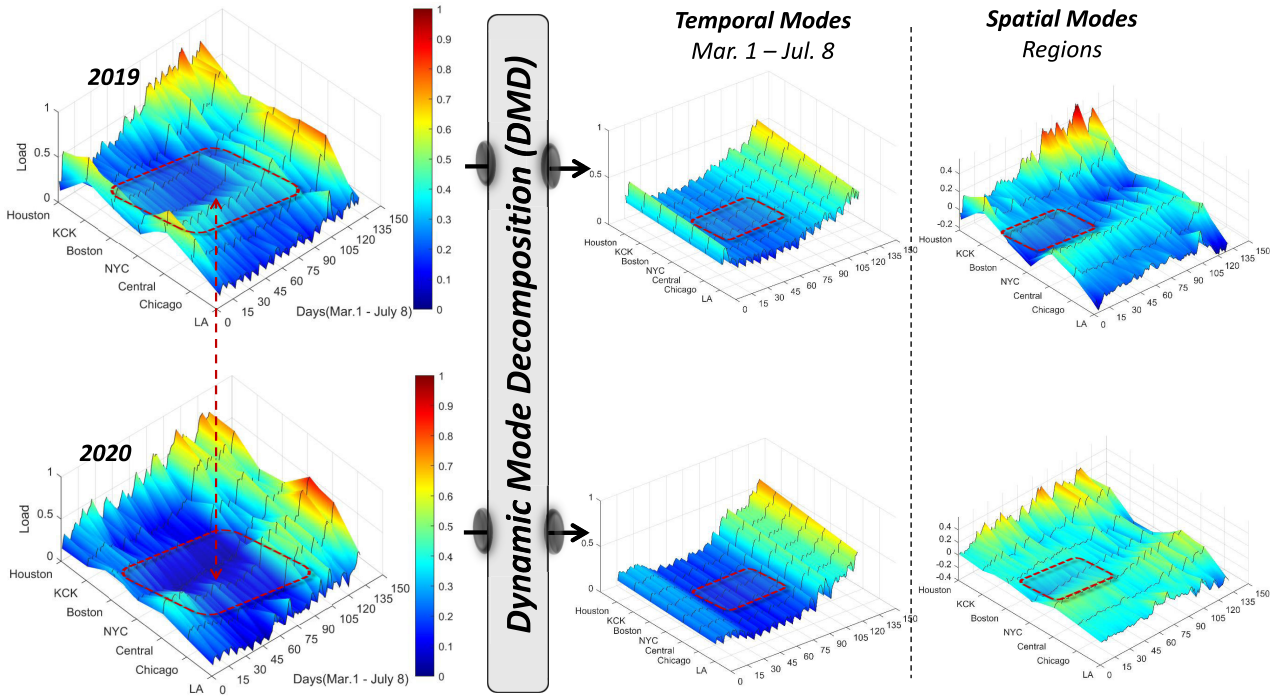
FIGURE 4. Surface plots depicting the load consumption data and outputs of the dynamic mode decomposition (DMD) process applied to 2019 and 2020 data during the time-periods of March 1st to July 8th. All surface plots show on the z-axis the load consumption data for all seven regions (CAISO-Los Angeles, PJM-Chicago, MISO-Central, NYISO-NYC, ISONE-Boston, SPP-KCK, and ERCOT-Houston) normalized individually. The x-axis represents the temporal dimension in terms of days during the time period of March 1st to July 8th (130 days) and the y-axis represents the spatial dimension that covers all seven regions, from the first city (Los Angeles) implementing SAHO to the last city (Houston) implementing SAHO according to the COVID-19 response timeline.

of the DMD modes, are determined by the columns of Φ. Φ is then computed as follows:

$$\Phi = X'V\Sigma^{-1}W \qquad (8)$$

The utilization of the discussed DMD method can identify coherent spatio-temporal patterns (modes – Φ) in the dataset by calculating the respective eigenvectors and eigenvalues. Each eigenvalue describes the growth or decay and oscillatory patterns observed in each dynamic mode (eigenvector) identified in the dynamic system. Therefore, DMD is applied to spatio-temporal raw load consumption data, across different regions/cities in the U.S., in order to identify the effects and patterns that the COVID-19 outbreak caused in load consumption reduction across these regions. The Δt chosen are 1-hour and 1-day resolutions so that the variations of the patterns across the selected temporal scales can be easily translated to load consumption variations during the different COVID-19 related events.

The first step performed in our examination is a spatio-temporal analysis designed to capture the variations in load consumption patterns between the years 2019 and 2020. As mentioned previously, we focus on the March-to-July time periods of the aforementioned years since these were the periods when COVID-19-related actions, such as SoE and SAHO, were in full execution. To perform the proposed DMD analysis, we processed and organized the raw load consumption data from the seven different regions (cities)

across the U.S. This data is used to create X and X' matrices, where *m* (temporal snapshots) represents different days in the time-period evaluated (March 1 to July 8th), and *n* (spatial) represents the different regions/cities evaluated (LA, Chicago, NYC, MISO-Central, Boston, KCK, and Houston).

Fig. 4 shows the raw data and outputs of the DMD process executed using the 2019 and 2020 load consumption data, respectively. As seen in this figure, there are significant differences in the load consumption from the years 2019 and 2020 for most of the cities evaluated. By analyzing the temporal and spatial modes identified by the DMD process, we can characterize how the COVID-19 countermeasures impacted load consumption patterns in the seven studied regions. In essence, we can observe, through load consumption data, how COVID-19 was spreading through the U.S. and along the response timeline. In addition, we can also observe that, from the seven cities analyzed, NYC was one of the most affected regions in terms of significant load variation across the U.S. Cross-referencing these results with the timeline presented in Fig. 2, Fig. 4 clearly depicts how this low load-valley period is more prominent during the NYC SoE and SAHO events.

The second analysis using the DMD approach is performed based on temporal load consumption data available from NYC. According to the statistical analysis performed in the previous subsection and the spatio-temporal
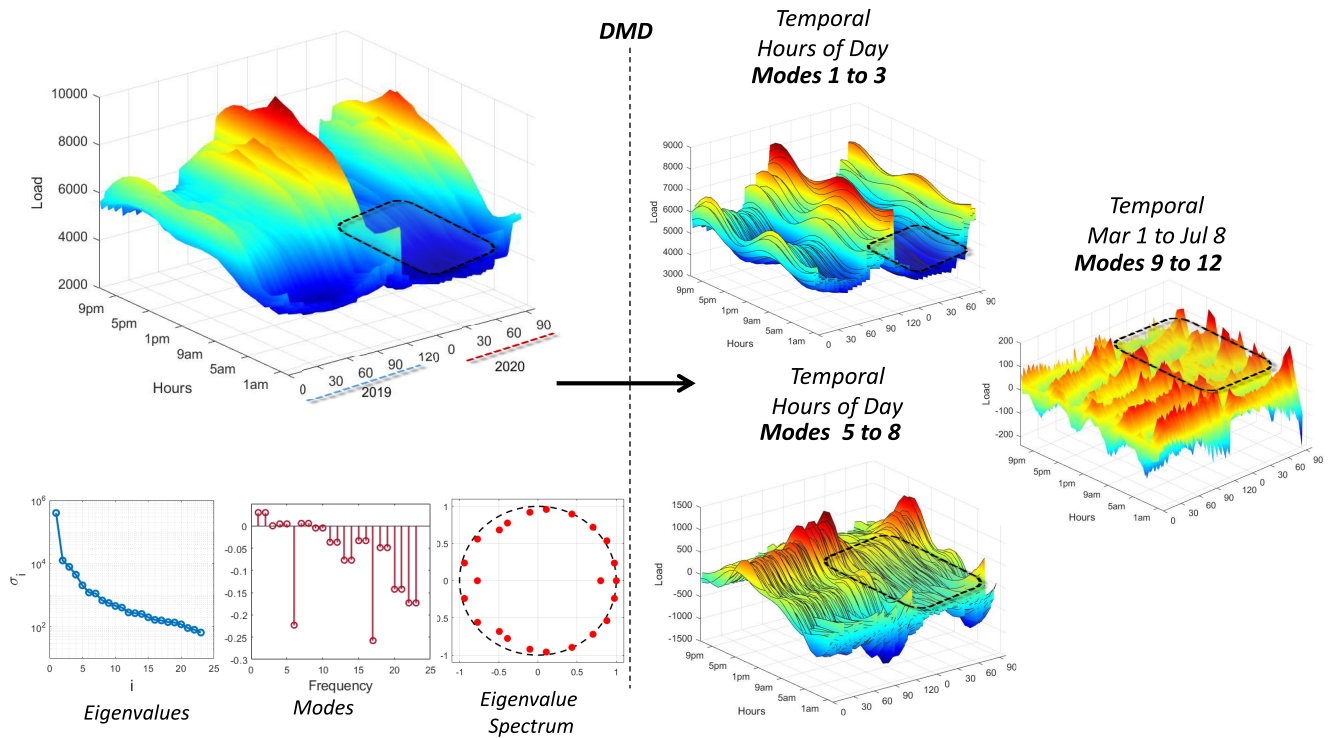
FIGURE 5. Surface plots depicting the load consumption data and outputs of the dynamic mode decomposition (DMD) process applied to 2019 and 2020 NYC data during the time-periods of March 1st to July 8th. All surface plots show on the z-axis the load consumption data for NYC. The x-axis represents the temporal dimension in terms of days during the time-period of March 1st to July 8th (130 days) for both the 2019 and 2020 periods combined and the y-axis represents another temporal dimension that covers the different times during the day (12 am to 11pm). The plots shown in the lower left quadrant show the direct outputs of the DMD process, where the first one shows the eigenvalues of Ã, the second one depicts the modes identified in terms of frequency, and the third one shows the eigenvalue spectrum of Ã.

DMD analysis of all the U.S. regions, the NY region was one of the most affected by the COVID-19 lockdown measures in terms of load consumption variation. In Fig. 5, it can be observed how the DMD process is applied in order to identify temporal modes for load consumption during the daily 24 hours and, at the same time, identify the temporal modes in a slower frequency rate (i.e., 1-day resolution) during the March-to-July time periods of 2019 and 2020. The lower left side of the figure shows the eigenvalues, identified modes, and eigenvalue spectrum outputted by the DMD process while the right side shows the reconstructions of some of the most prominent modes that characterize each temporal domain. Noticeable differences between the 2019 and 2020 load consumption can be seen in the figures shown on the right side. For example, based on modes 1 to 3, we observe how the 2020 data is significantly lower (represented with a darker blue) during the morning hours of the day, while modes 5 to 8 show how the evening load is flattened out as the lockdown measures were implemented during the COVID-19 response timeline. On the other hand, the plot reconstructing modes 9 to 12 shows a clear side-by-side comparison that demonstrates how, during the same time period of 2019 vs. 2020, load demand significantly decreased as the COVID-19 outbreak worsened throughout NYC.

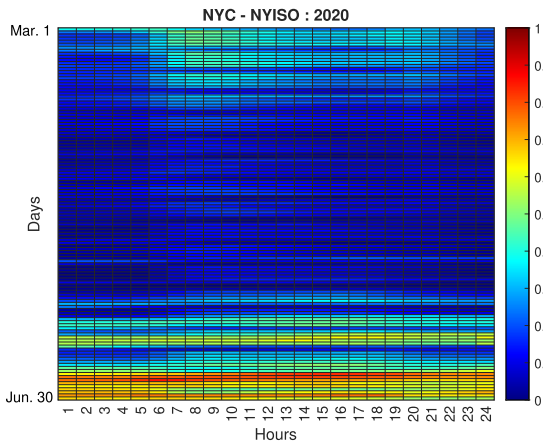## C. IMPACT OF COVID-19 LOCKDOWN MEASURES IN NYC NET-LOAD DEMAND

Based on all the analyses conducted, further investigations are carried out to evaluate the impact of the lockdown measures in NYC, i.e., the most affected city during the analyzed period. Fig. 6 and Fig. 7 show heatmaps comparing the normalized load consumption of NYC during the March 1st to June 30th time period. The vertical represent the different days in the period and the horizontal represent the time of the day. As seen, there is a clear difference between the same periods during 2019 (pre COVID-19 pandemic) and 2020 (during the COVID-19 pandemic). It can also be observed that the most significant variations in load demand reduction are concentrated during the SAHO declared in NYC, that began in March 22 and ended in May 15, as seen in the presented timeline (Fig. 2). The variation observed during this period can be characterized by a 20% to 30% reduction in load demand during weekdays.

In order to avoid bias from load changes due to non-pandemic related events, we analyzed the weather conditions, and specifically temperature data for NYC during the same period of time. Figs. 8 and 9 show the normalized temperature values for NYC during the period of March 1st to June 30th. The temperature data is normalized using −7.22 Celsius as the minimum value and 33.9 Celsius as the
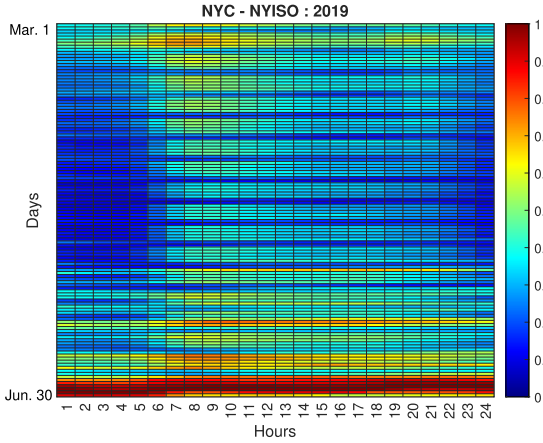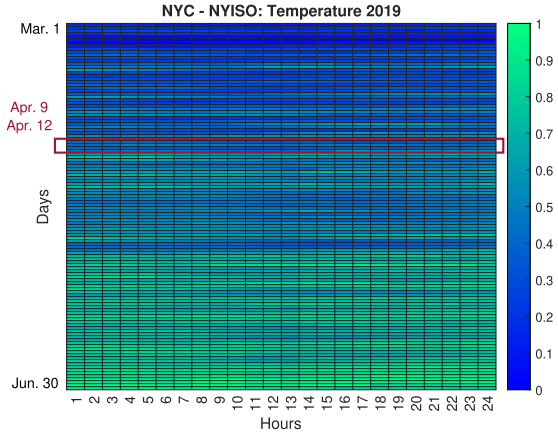
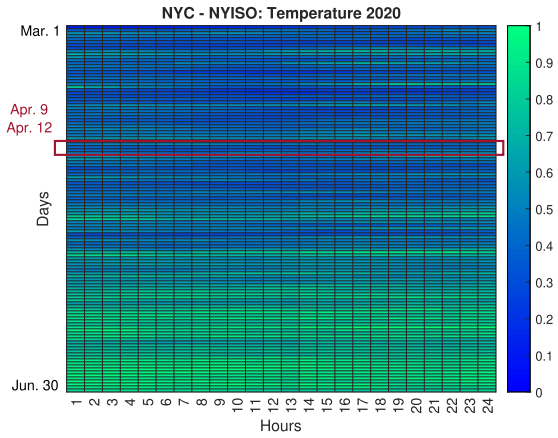**FIGURE 6.** Normalized load demand heatmap for NYC during March 1st to June 30th Period, 2019.

FIGURE 8. Normalized temperature heatmap for NYC during March 1st to June 30th Period, 2019.

FIGURE 7. Normalized load demand heatmap for NYC during March 1st to June 30th Period, 2020 (during COVID-19 outbreak).

FIGURE 9. Normalized temperature heatmap for NYC during March 1st to June 30th Period, 2020 (during COVID-19 outbreak).

maximum value. Based on this data, four days are selected as candidates for investigating the feasibility of load-changing attacks due to low net-load demand conditions, April 9, April 10, April 11, and April 12. These days are selected due to their similarity in temperature values between 2019 and 2020 and falling inside the SAHO time period declared in New York. Choosing these days allowed us to discard temperature as a driving factor of the significant variation in electricity consumption, and helped us to focus on the possible repercussions a pandemic-type event, as the one being experienced, could cause in the cyberphysical security of EPS.

To characterize the temperature similarities between the days during the March 1st to June 30th period, average percentage differences are calculated between the respective days of 2019 and 2020. From the 122 days analyzed in the aforementioned time period, April 11 is under 10% of the days that had lower average temperature differences between 2019 and 2020. April 12 is under 20%, April 9 is under 35%, and April 10 lies under 50% of the days that had lower average temperature differences between 2019 and 2020.

In addition, we also took into account that April 9 and 10 were weekdays while April 11 and 12 from 2020 were weekend days.

IV. MODELING LOAD-CHANGING ATTACKS: THREAT MODEL & MATHEMATICAL FORMULATION

Modern EPS integrate different technologies, such as intelligent controls and real-time measurement devices, providing system operators with real-time visibility and thus improving system security, stability, and reliability. However, this integration can be a double-edged sword since the use of more interconnected IoT devices exposes the power grid to new cyberattack vectors altering completely the threat model. As more high-wattage loads are equipped with IoT devices, the feasibility of a load-changing attack significantly increases. In this section, we focus on describing load-changing attacks that can be performed by attackers with sufficient motivation, capabilities, and resources to cause major disturbances in transmission and distribution systems via the use of botnets capable of simultaneously controlling large groups of high-wattage loads and DERs.

A. THREAT MODEL: LOAD-CHANGING ATTACK

In this work, we consider an attacker capable of leveraging vulnerabilities of IoT devices to compromise and control high-wattage appliances, such as HVACs, water heaters, or EV chargers. By simultaneously switching on and off or granularly adjusting the power consumption of hundreds or thousands of compromised devices, the attacker may be able to cause severe adverse impacts, such as frequency instabilities and over/under voltage conditions, in the CPES.

Table 2 shows the threat model used for the load-changing attack according to related work in the area [39]. As observed, for the load-changing attack, the attacker can be considered as an *oblivious* (i.e., no detailed knowledge of EPS topology) or *semi-oblivious* (i.e., has limited information of the EPS topology) adversary. In addition, since the attack can be performed through IoT-connected devices, *no possession* is required. This means that the attacker does not needs to physically possess the attacked device(s) since they can be compromised through the communication network. For specificity, the attack is considered a *targeted attack* since the adversary's target are devices (e.g., IoT connected high-wattage loads) capable of directly affecting the power grid and possibly cause instabilities that could lead to blackouts and frequency fluctuations in the system. In layman's terms, specificity relates to how specific the attack is, i.e., *targeted* or *non-targeted*. As for adversary's resources, in the investigated load-changing attack, we consider a *Class II* adversary categorization, where *Class I* represents an adversary that does not need and/or has sufficient resources to carry out very complex attacks without being detected, and *Class II* represents an adversary that needs and/or disposes of sufficient motivation and resources to materialize the coordinated load-changing attack without being easily detected. This *Class II* categorization is assumed due to the complexity related to performing a coordinated load-changing attack capable of simultaneously affecting multiple load zones in the power grid that could cause significant damage in the system. This type of attack differs from the dilettante attack mechanism in [22] and requires significant resources and knowledge, such as the appropriate instruments and training for being able to infect

and/or compromise multiple high-impact load zones, to be effectively carried out.

In addition, the load-changing attack is considered to have an *iterative attack* frequency and a *multiple-times* reproducibility in terms of the *attack model formulation* of the threat modeling approach. This means that the attack needs to be performed in an iterative manner, i.e., the adversary must attack multiple loads and iteratively change their set-points in order to accomplish the desired effect of destabilizing the system (*iterative attack*). Also, the attack is considered a *multiple-times* attack since it can be performed or reproduced multiple times before being detected and mitigated by operators. Furthermore, the attack level in the *attack model formulation* is considered as a *Level 1* (L1) or *Level 2* (L2) attack according to the level at which the vulnerable assets (e.g., smart HVACs, IoT-connected motors, PLCs, HMIs, breakers, controllers, etc.) are compromised. These levels can be at the industrial network layer or the local network layer. The *attack technique* describes the attack method used by the adversary. In the case of the load-changing attack considered, the *attack technique* is assumed to be a modification of control logic or a wired/wireless compromise of the controllable loads that affects the integrity of the data in the system. The load-changing attack is considered as a subset of *data integrity attacks* (DIA) due to the fact that the attack is targeted at affecting the integrity of either the system's measurements (e.g., current, voltage, power, or status measurements) or the system's controls (e.g., power set-points or status control changes, etc.). Finally, the *premise* of the attack is related to the integrity of the cyber-system, i.e., how the attack affects primarily the integrity of the ICT devices that make up the communication network. More details regarding the mathematical formulation of the load-changing attack as a DIA is presented in the next subsection.

B. FORMULATION OF LOAD-CHANGING ATTACKS

The load-changing attack presented in this work can be characterized as a DIA-type of attack. In order to present its mathematical formulation, we first consider a cyberphysical system (CPS) plant described by:

$$x(k + 1) = Gx(k) + Bu(k) \qquad (9)$$
$$y(k) = Cx(k) + e(k) \qquad (10)$$

where $x(k) \in \mathbb{R}^n$ represents the physical system's states, $u(k) \in \mathbb{R}^l$ represents the control variables, and $y(k) \in \mathbb{R}^m$ represents the system's measurements. The matrices $G \in \mathbb{R}^{n \times n}$, $B \in \mathbb{R}^{n \times l}$, and $C \in \mathbb{R}^{m \times n}$ represent the system, input, and output matrices, respectively. The system input measurement noise is represented by the term $e \in \mathbb{R}^m$. The cyber-system of the CPS can be generally expressed as:

$$u(k + 1) = Hy(k) \qquad (11)$$

$H \in \mathbb{R}^{l \times m}$ represents the control matrix [40]. Fig. 10 shows a diagram that depicts the variables affected by the DIA load-changing attack in the CPS structure.

TABLE 2. Threat model formulation of load-changing attacks.

Threat Model \Threat	Load-changing Attack
Knowledge	Oblivious or Semi-Oblivious
Access	Non-possession
Specificity	Targeted
Resources	Class II
Frequency	Iterative
Reproducibility	Multiple-times
Level	L1 or L2
Asset	Smart HVAC, IoT-connected motors, PLCs, EV chargers, water heaters, etc.
Technique	Modify control logic or wireless compromise
Premise	Cyber: Integrity

As observed in Fig. 10, in a DIA, either the measurements (y) or the controls (u) could be compromised by the adversary via fabrication or modification. More specifically for a load-changing attack, the controls (u) of the IoT-controllable loads are 'altered/attacked' as:
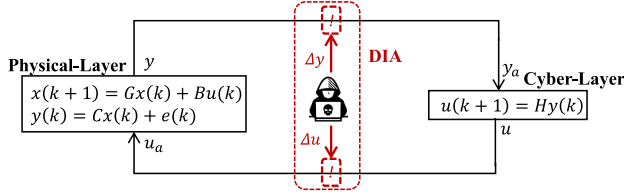
$$u_a = u + \Delta u \quad (12)$$

FIGURE 10. Diagram of CPS model and load-changing DIA cyberattack.

where u_a represents the 'altered/attacked' control variables, u represent the original control variables, and Δu represent the variations injected by the adversary in the control variables. This modification of controls affects the CPS by:

$$x_a(k+1) = Gx(k) + Bu_a(k) \quad (13)$$
$$y_a = C\big(x(k+1) + B\Delta u(k)\big) + e(k+1) \quad (14)$$

where y_a and x_a represent the input measurements and states of the CPS affected by 'altered' control variables.

Mapping the above formulation to a load-changing attack, we can modify the term u_a so it represents 'altered' load demand in a CPES as follows:

$$p_a(k) = p_i(k) + \Delta p(k) \quad (15)$$

where p represents the controllable load demand in the system, p_i is the initial 'un-altered' load demand, Δp represents the portion of the total load demand affected by the load-changing attack, and p_a represents the total load demand 'altered' by the load-changing attack at one bus. If the attackers simultaneously compromise more than one load/bus in the system, Eq. (15) can be extended as:

$$P_T(k) = \sum_{l=0}^{m} p_{i,l}(k) + \sum_{j=0}^{n} p_{a,n}(k) + P_{loss} \quad (16)$$

where P_T represents the total demand in the system, m is the number of total 'unaltered' loads in the system, n is the total number of loads compromised by adversaries, and P_{loss} represents the total losses.

Due to the network power balance, to maintain frequency stability, the sum of all the generation needs to be approximately equal to the total demand and losses in the system:

$$P_T(k) \approx \sum_{g=0}^{N_g} P_g(k) \quad (17)$$

where N_g represents the number of g generators in the system. Hence, in order to understand the effect of load changes in the frequency stability at each generator bus, we can investigate

the swing equation which describes the behavior of rotor dynamics in transient stability studies. The swing equations shown in Eq. (18) - Eq. (20) describe the relationship between the input mechanical power (P_m), output electrical power (P_e), and the rotational speed of the generator (ω) [41]. The term P_e is directly related to P_g as seen in Eq. (21), since it represents the generator power output plus electrical losses of the generating unit.

$$\frac{2H}{\omega_s}\frac{d^2\delta}{dt^2} = P_m - P_e \quad (18)$$

$$\frac{d\delta(t)}{dt} = \omega(t) - \omega_s \quad (19)$$

$$\frac{2H}{\omega_s}\frac{d\omega(t)}{dt} = P_m - P_e \quad (20)$$

$$P_e = \frac{V_s V_r}{X}sin(\delta) \quad (21)$$

H represents the constant normalized inertia, ω_s is the synchronous speed (i.e., 50 or 60 Hz), and δ is the power angle. V_s is the voltage at the generator bus, V_r is the voltage at receiving bus, and X is the reactance based on the classical model of a generator. The relationship between the electrical frequency $\omega(t)$ with the power angle δ is shown in Eq. (19). Therefore, it is evident based on these relationships that any sudden change in load demand caused by high-wattage loads turning on/off in the CPES will affect P_e, and thus cause frequency fluctuations as seen in Eq. (20).

C. OPERATIONAL CHALLENGES & STANDARDS: FREQUENCY THRESHOLDS FOR NERC, ERCOT, AND NYISO

Before analyzing the feasibility of load-changing attacks in a system experiencing low net-load demand conditions such as the ones observed in our investigations, we first explore what are the operational challenges that exist in EPS and are related to load demand changes. According to the Electric Power Research Institute (EPRI) [42], there are different types of challenging operational conditions, related to net-load demand changes, that could cause steady-state or dynamic threats to the contingency security of EPS. These challenging operational conditions are:

1) **Peak-demand conditions**: Congested networks or limited generation capacity.
2) **Rapid change in demand or supply conditions**: A rapid change in demand or supply. For example: morning demand ramps, PV-related net demand ramps, or sudden failure of EPS elements.
3) **Low net-demand conditions**: Periods when the system load demand is significantly reduced. During these periods, system voltages may rise and system inertia may be affected. Excess generation may be forced to remain online to meet the demand at a later time.

In addition to handling these operational challenges, system operators must provide protective mechanisms to resolve system instabilities, protect system assets, and maintain normal operations. Some of these mechanisms are, for

example, underfrequency relays designed to trip when the system's frequency is lower than some predefined values. These predefined values are generally given as frequency bounds programmed into protection mechanisms, and thus are essential to determine the types of remedial actions needed to maintain system stability. The North American Electric Reliability Corporation (NERC) is a nonprofit corporation that provides comprehensive standards for EPS operation in North America. More specifically, NERC requires power systems to operate within a frequency range of 59.5 Hz to 62.2 Hz. If the frequency is out of these bounding ranges, underfrequency or overfrequency protection relays trip parts of the system with the objective of protecting the respective system assets and the overall grid infrastructure [43]. Similarly, the Electric Reliability Council of Texas (ERCOT) sets its own frequency thresholds to be 59.3 Hz for underfrequency and 61.8 Hz for overfrequency, respectively. In addition, some system operators may have more complex protection mechanisms that provide rules to shed a certain percentage of the load in the system in case of frequency stability issues [44].

Since our load data and load-changing attack scenarios are based on NYISO and NYC, we utilize the operational standard (frequency thresholds) provided by NYISO. In comparison with NERC and ERCOT, NYISO has more strict criteria to mitigate underfrequency and overfrequency scenarios. NYISO defines a major system disturbance as any event that causes the frequency to drop below 59.9 Hz or increase over 60.1 Hz [45]. The specific thresholds given by NERC, ERCOT, and NYISO are provided in Table 3.

More specifically, for underfrequency scenarios, NYISO requires fast UFLS to be performed at different percentages when the frequency is rapidly declining. Consecutive 7% load shedding is performed when the frequency drops below 59.5 Hz, 59.3 Hz, 59.1 Hz, and 58.9 Hz. At this point, if the frequency is still declining, transmission operators must take the necessary steps to minimize damage and service interruption. However, the UFLS required in ERCOT differs from the one applied in NYISO due to its different operational thresholds. In ERCOT, the UFLS starts at 59.3 Hz, where 5% of the system load is tripped. Then, an additional 10% of the load is tripped at 58.9 Hz and an additional 10% at 58.5 Hz. It is important to remember that the intent of UFLS is not to recover the frequency but to stop the frequency decline [46].

On the other hand, for overfrequency scenarios, both ERCOT and NYISO have similar procedures to follow in order to maintain compliance with the NERC Balancing Authority ACE Limit (BAAL) standard. Specifically for the NYISO case, a sustained high frequency of 60.10 Hz is considered an indication of a major load-generation imbalance, and if it continues to decline it can be declared as a 'major emergency' [45]. In order to address this emergency NYISO takes the following actions [45]:

1) Request all over generating suppliers to adjust their generation and match schedules.

TABLE 3. Operational frequency thresholds for NERC, ERCOT, and NYISO.

Category	NERC	ERCOT	NYISO
Overfrequency (Hz)	62.20	61.80	60.10
Underfrequency (Hz)	59.50	59.30	59.90

2) Reduce the applicable dispatchable generation to minimum operating limits.
3) Request internal generators to voluntarily operate in 'manual' mode and below minimum dispatchable levels.
4) Attempt to schedule variable load or storage to alleviate the problem.
5) Request reduction or cancellation of all transactions that are contributing to the imbalance event.
6) If the overgeneration (i.e., overfrequency) scenario persists, NYISO will declare a 'major emergency' and de-commit applicable internal generators until the violation is eliminated.

V. ANALYZING THE FEASIBILITY OF LOAD-CHANGING ATTACKS: EXPERIMENTAL SETUP & RESULTS

In this section, we present the experimental setup used for evaluating the feasibility of a load-changing attack in a system such as NYISO during low load demand periods such as the ones encountered during the COVID-19 pandemic. As presented in Section III, four days are selected as candidates for investigating the feasibility of load-changing attacks during low net-load demand periods. These days are April 9, 10, 11, and 12 of 2019 and 2020.
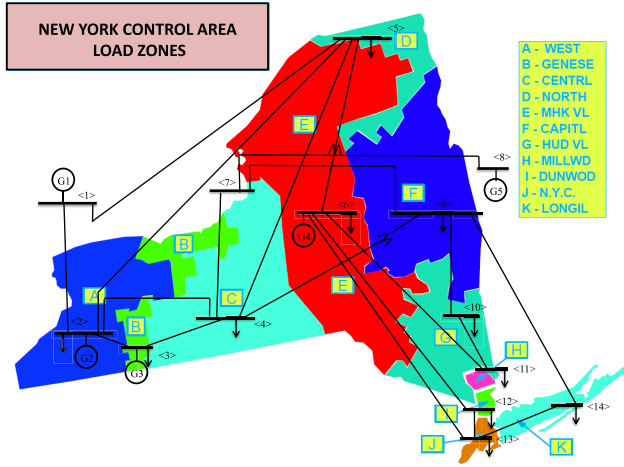
A. TEST SYSTEM: IEEE-14 BUS SYSTEM

For our experimental analysis, 5-minute resolution load data are obtained from the 11 load zones that exist in NYISO. Due to the lack of NYISO topological information, we utilize NYISO load data and the respective NYISO load zones are mapped to every load bus in the IEEE-14 bus test system [47], [48]. Below, we describe how to prepare the data in order to examine our load-changing attack case studies. First, the mapping of the NYISO regions to IEEE-14 bus system is performed as follows:

1) A - WEST → Bus #2
2) B - GENESE → Bus #3
3) C - CENTRL → Bus #4
4) D - NORTH → Bus #5
5) E - MHK VL → Bus #6
6) F - CAPITL → Bus #9
7) G - HUD VL → Bus #10
8) H - MILLWD → Bus #11
9) I - DUNWOD → Bus #12
10) J - N.Y.C. → Bus #13
11) K - LONGIL → Bus #14

Fig. 11 shows the NYISO map with the corresponding mappings. In order to adapt the NYISO load values to the IEEE-14 test system, we performed a normalization process

FIGURE 11. NYISO control area load zones mapped to IEEE-14 bus system.

that consists of obtaining the average load consumption of each zone (based on historical data), calculating a ratio of load demand, and finally computing the corresponding load value for the IEEE-14 test system. Fig. 12 demonstrates all the steps of the process based on the WEST zone. All other regions follow the same process for computing their corresponding values. The adapted version of the IEEE-14 bus test system, with its respective 2019 and 2020 load profiles, is modeled and evaluated using the Power System Analysis Toolbox (PSAT) [49]. PSAT is an open-source MATLAB toolbox specifically designed to perform power system analysis and simulation.

B. DESCRIPTION OF CASE STUDIES

Four 24-hour runs for the days April 9, 10, 11, and 12 are analyzed and inputted into the adapted IEEE-14 bus test system modeled in PSAT. The objective of this study is to find times where the system could be more vulnerable to load-changing attacks due to low net-load demand conditions caused by action events of the COVID-19 pandemic.

For each case study, or day analyzed, a preliminary analysis is conducted to determine the time of day when the 2020 system is more vulnerable (i.e., has lower demand) than the 2019 system, and also to determine the loads (or buses) that have the highest impact in frequency stability of the system. In other words, this analysis indicates the period where the biggest difference in the total load demand of the system exists, when comparing 2019 and 2020 load profiles, and then clearly shows which buses, if compromised, would have the highest impact in the 2020 system. The *total load demand difference* is calculated by subtracting the total load demand of 2019 minus the total load demand of 2020:

$$LD = TL_{2019} - TL_{2020} \qquad (22)$$

where LD is the total load demand difference between 2019 and 2020, and TL is the total load demand of the respective years.

$$WEST_{avg} = mean(WEST_{total}) \Big/ \quad WEST_{avg} = 1443.03$$

Date	2019	2020
Jan 1, 2018 00:00:00	1452	1429.6
...	...	...

$$WEST_{RatioToAvg} = WEST_{Load}/WEST_{avg}$$

Date	2019	2020
Jan 1, 2019 00:00:00	1452/1443.03 = 1.006	1429.6/1443.03 = 0.990
...	...	...

(From IEEE 14 Test System)
$$B2_P = 21.7\ MW$$
$$B2_P = 12.7\ MW$$

$$B2W_P = B2_P \times WEST_{RatioToAvg} \Big/ B2W_Q = B2_P \times WEST_{RatioToAvg}$$

Date	2019	2020
Jan 1, 2019 00:00:00	1.006 X 21.7 = 21.83	0.990 X 21.7 = 21.48
...	...	...

FIGURE 12. Normalization process for IEEE 14 test system using NYISO load data.

Additionally, in order to determine the buses (or loads) that, if compromised, would have the highest impact on the 2020 system when compared to the 2019 system, a ratio of the load at each bus and the total load for the specific year (i.e., 2019 or 2020) is calculated. Then, these ratios are subtracted to compute the *load impact index difference* (*LIID*) for each individual bus in the system as seen in Eq. (23).

$$LIID_i = \frac{L_{2019}^i}{TL_{2019}} - \frac{L_{2020}^i}{TL_{2020}} \qquad (23)$$

where L is the load at the respective load i for the respective year, 2019 or 2020. It should be noted that all the values used in this analysis are in per unit (p.u.).

After the preliminary analysis is conducted and the 'ideal' period of time to attack the system is identified, a load-changing attack is conducted in each selected day and period, while the frequency of the system is monitored. The selection of the compromised bus(es) for each case study depends on the results obtained in the preliminary analysis. More details regarding the specific case studies are presented below.

C. CASE STUDY 1: APRIL 9
1) PRELIMINARY ANALYSIS
A preliminary analysis is performed in order to identify the 'ideal' time period and bus(es) that would need the minimum effort to cause a high impact in the system when a load-changing attack is performed; or simply the period when a peak of LD matches with a negative peak in LIID. Figs. 13 and 14 show the LD and the LIID for April 9. Based on the results from the analysis, the period when
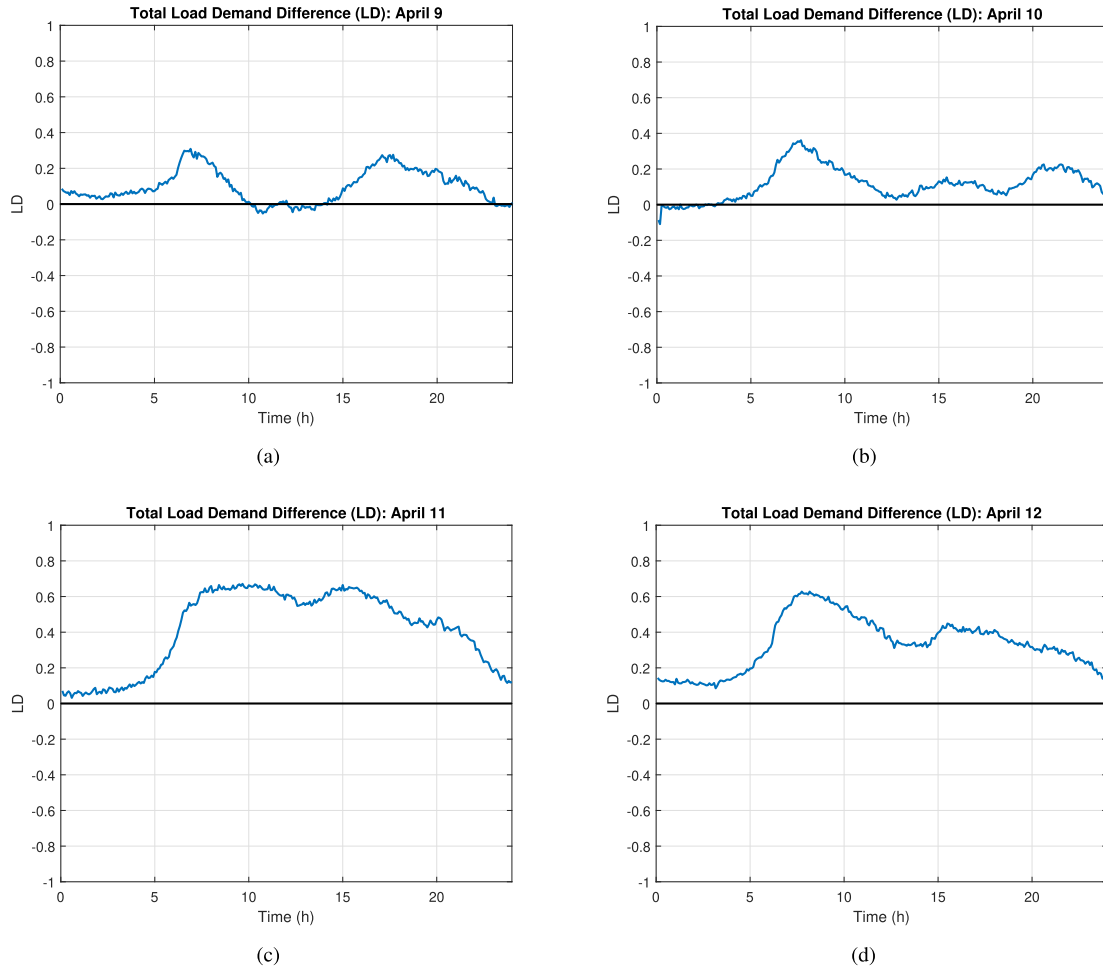
FIGURE 13. Total load demand difference (LD) calculated for the days: a) April 9, b) April 10, c) April 11, and d) April 12.

the highest difference in load demand between 2019 and 2020 arises is in the hours between 6:30 am to 7:30 am and 4:30 pm to 6:00 pm. The highest LD value during the morning period is 0.309. However, in order to find the discussed 'ideal' period for the load-changing attack, we also need to find out the most negative LIID value observed during the examined periods and then correlate it to the high LD value period observed in the LD graph. As seen in Fig. 14, the 'lowest' negative LIID values occur during the 11:30 am to 1:30 pm period, with a peak of −0.0248. Nonetheless, when correlating these two values, we can clearly see that our LIID peak period does not match with any of the two LD identified periods, so no bus(es) in the system can be identified as the one(s) that could cause a high impact in the 2020 system when compared to the 2019 system scenario. Any load-changing attack implemented in 2020 system will have a similar effect on 2019 system, making April 9 a difficult day to analyze in terms of how more vulnerable the system is when low net-load demand conditions exist.

2) LOAD-CHANGING ATTACK IMPACT
According to the analysis obtained from the *preliminary analysis* step, we recognized that for this particular day

there are no time periods where an attacker could effectively compromise the frequency of the system when compared to 2019 with minimum effort. Both systems (2019 and 2020 scenarios) would have a fairly similar response, thus making it very hard to evaluate the feasibility of a load-changing attack when low net-loading conditions exist. This is indicated by the fact that the lowest (most negative) value of LIID does not align with the highest value of LD in the analyzed scenario. In a nutshell, April 9 is a day when an attacker would no see any significant differences between attacking a system with lower loading conditions, based on how the 2020 system scenario compares to the 2019 system scenario.

D. CASE STUDY 2: APRIL 10
1) PRELIMINARY ANALYSIS
Figs. 13(b) and 14(b) show the LD and the LIID for April 10. Based on these results, we identify that the period when the highest difference in load demand between 2019 and 2020 occurs is in the hours between 5:00 am and 10:00 am, more specifically, at 7:30 am when the LD value is 0.356. Following a similar approach as the one presented in the previous case study, we correlate the most negative LIID value of the analyzed day, which occurs between
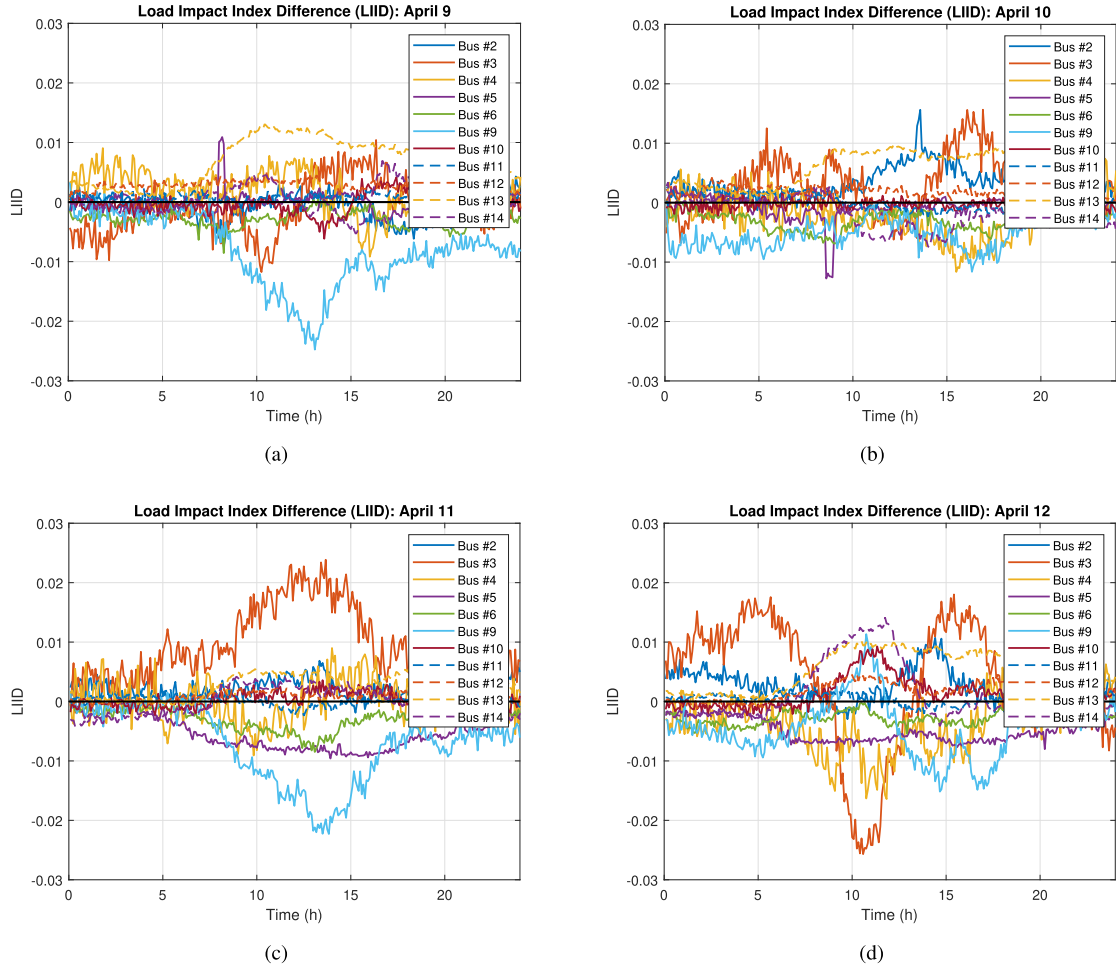
FIGURE 14. Load impact index difference (LIID) calculated for each bus in the system for the days: a) April 9, b) April 10, c) April 11, and d) April 12.

8:30 am and 9:00 am (i.e., the negative peak of the purple line), with the period of maximum LD. It is worthwhile to remember that the negative LIID value tells us which bus(es) in the system will have the greatest impact in the 2020 system while requiring the minimum effort (minimum load change required) when compared to the 2019 system. Based on the observed correlation, we conclude that attacking bus #5 (purple line) between 8:30 am and 9:00 am (i.e., the negative peak of the purple line), together with bus #9 (light blue line), would cause the greatest impact on the frequency stability of the 2020 system scenario.
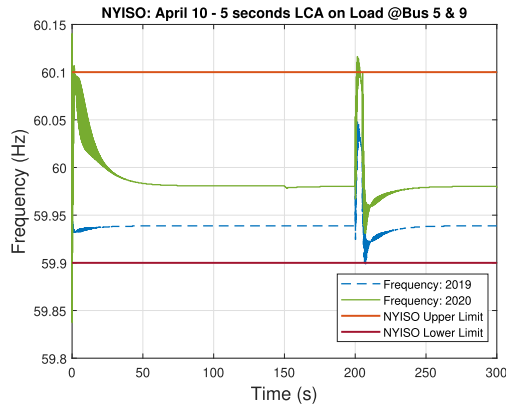
2) LOAD-CHANGING ATTACK IMPACT
Based on the preliminary analysis, we simulate a load-changing attack on the loads connected to bus #5 and bus #9 for both the 2019 and 2020 system scenarios. Fig. 15 shows the impact of the 5-second load changing attack during 300 seconds (i.e., 5 minutes from 8:40 am to 8:45 am), where the load-changing attack is executed at 200 seconds. As seen in the graph, the frequency of the 2020 system scenario crosses the overfrequency NYISO limit of 60.1 Hz

when the load-changing attack disconnects the compromised loads (i.e., loads at bus #5 and bus #9). On the other hand, the 2019 system scenario presents no overfrequency problems and thus we can see that the low net-load demand of the 2020 system makes more feasible the implementation of a high-impact load-changing attack that could compromise the stability of the system. It should also be noted that a more sustained attack (e.g., a 1 or 5-minute attack) has the potential of causing more severe problems.

E. CASE STUDY 3: APRIL 11
1) PRELIMINARY ANALYSIS
Similar to April 10, April 11 seems to be a day where a load-changing attack could be feasible if mitigation measures are not taken. But, to confirm this, we perform the preliminary analysis and identify the highest LD values and the most negative LIID values based on Figs. 13(c) and 14(c). These figures show the LD and the LIID for April 11. Based on these results, the period when the highest difference in load demand between 2019 and 2020 exists is in the hours between 7:30 am and 3:00 pm. Similarly to the previous case study,

FIGURE 15. Load-changing attack impact on the frequency of the system during April 10 of 2019 and 2020. The upper and lower limits given by NYISO are provided for reference.
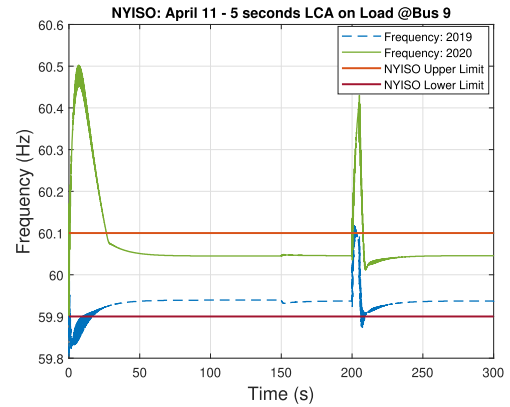
FIGURE 16. Load-changing attack impact on the frequency of the system during April 11 of 2019 and 2020. The upper and lower limits given by NYISO are provided for reference.

in order to find the 'ideal' period for the load-changing attack, we need to find out the most negative LIID value observed during the examined period and then correlate it to the high LD value period observed in the LD graph. Correlating these two graphs, we observe that attacking bus #9 (light blue line) between 1:00 pm and 2:00 pm (i.e., the negative peak of the light blue line) would cause the greatest impact on the frequency stability of the 2020 system scenario.

2) LOAD-CHANGING ATTACK IMPACT

A load-changing attack on the load connected to bus #9 is implemented for both the 2019 and 2020 system scenarios, according to the results obtained in the preliminary analysis. Fig. 16 shows the impact of the 5-second load changing attack during 300 seconds (i.e., 5 minutes from 1:40 pm to 1:45 pm), where the load-changing attack is executed at 200 seconds. This graph shows how the frequency of the 2020 system scenario crosses the overfrequency limit of 60.1 Hz and goes up to 60.5 Hz when the load-changing attack compromises the load connected at bus #9. Differently, the 2019 system scenario presents no major overfrequency problems, so we can conclude again that the low net-load demand of the 2020 system makes more feasible the implementation of a high-impact load-changing attack that could negatively impact the stability of the system.

F. CASE STUDY 4: APRIL 12
1) PRELIMINARY ANALYSIS

Using a similar approach as the ones implemented in the previous case studies, a preliminary analysis is conducted to determine the 'ideal' time period to attack the April 12 system scenario. Figs. 13(d) and 14(d) show LD and the corresponding LIID values for April 12. As seen in these graphs, the period when the highest difference in load demand between 2019 and 2020 appears is in the hours between 6:30 am to 12:30 pm, with a peak value of 0.628 at 8:10 am. This period can be correlated to the period when the most negative LIID values are observed, which in turn, is the period

between 10:00 am and 11:30 am (i.e., the negative peak of the orange line with a peak negative value of -0.0257 at 10:35 am). Using this information, we conclude that attacking bus #3 (orange line) between 10:00 am and 11:30 am would produce the greatest impact in the frequency stability of the 2020 system scenario, while requiring the minimum attacker's effort, when compared to the 2019 system.
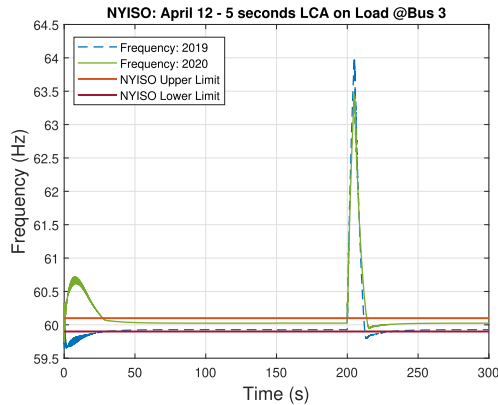
2) LOAD-CHANGING ATTACK IMPACT

Following the same approach described in previous case studies and based on the preliminary analysis results, we perform a load-changing attack on the load connected to bus #3 for both the 2019 and 2020 system scenarios. Fig. 17 shows the impact of the 5-second load changing attack during 300 seconds (i.e., 5 minutes from 10:33 am to 10:38 am), where the load-changing attack is executed at 200 seconds. Different from previous results, both the 2019 and 2020 systems have severe frequency stability problems since the frequency peaks at around 64.02 Hz and 63.46 Hz for the 2019 and the 2020 system scenarios, respectively. Diving deeper into these results, we discovered that bus # 3 is one of the most critical buses in the system due to the fact that it represents an average of around 37% of the total load of the 2019 system scenario and 36% of the total load of the 2020 system scenario. This makes bus #3 one of the most critical buses in the system, and the results that are shown in Fig. 17 clearly demonstrate that no matter if the system is experiencing low loading conditions (2020 system) or not (2019 system), a load-changing attack that disconnects this high-impact load zone would cause severe frequency fluctuations. In a nutshell, an attacker with enough capabilities to perform an attack targeted at bus #3 of the analyzed system will cause severe problems in the frequency stability of the system.

G. DISCUSSION OF CASE STUDIES

Based on the results of the four case studies investigated, it can be observed that each one of them enables different insights regarding the feasibility of load-changing attacks in a CPES experiencing low loading conditions. Evaluating

FIGURE 17. Load-changing attack impact on the frequency of the system during April 12 of 2019 and 2020. The upper and lower limits given by NYISO are provided for reference.

all these four cases provides a good perspective on some probable scenarios of the load-changing attack spectrum. For instance, case study 1 (April 9) demonstrates a scenario where an attacker, implementing a load-changing attack, would not perceive any difference between compromising a system experiencing low loading conditions, such as the 2020 scenario, and a nominal system, such as the 2019 scenario. On the other hand, both case study 2 and case study 3 (April 10 and April 11) clearly show how the low net-load demand conditions, that exist during the COVID-19 pandemic lockdowns, make the 2020 system scenario more vulnerable to low probability, high-impact load changing attacks when compared to the 2019 scenario. In both case studies, it can be observed how the same load-changing scenario has minor impacts on the 2019 system's frequency while producing major problems on the 2020 system's frequency. Finally, case study 4 (April 12) is an example of how compromising a critical bus in a CPES will cause severe frequency stability problems no matter if low loading conditions are being experienced. From a planning, operation, and cybersecurity perspective, system operators need to ensure these nodes are identified, and they must take appropriate mitigation strategies to handle any possible attacks to these critical buses.

VI. CONCLUSION AND FUTURE WORK

This article explores the feasibility of load-changing attacks in CPES that experience abnormal low loading conditions caused by events such as the COVID-19 pandemic and its corresponding lockdown measures. We explore the differences in loading conditions of the main affected regions in the U.S. and analyze the abnormal load patterns caused by lockdown measures in these regions, with a primary focus on the NYSIO region, by applying DMD to load consumption data from the years 2019 and 2020. Based on these analyses, we formulate a load-changing attack and further explore the feasibility of such attack in a system experiencing the low loading patterns identified by the DMD process. Finally, we simulate and evaluate the impacts of load-changing attacks in a test grid system experiencing low

loading conditions (2020), when compared to the 2019 historical loading conditions, using NYISO data. Our results demonstrate that low loading conditions can be leveraged by attackers with the objective of compromising the frequency stability of power systems. Specifically, the presented case studies show that an attacker with sufficient resources and capabilities would require less effort to compromise a system experiencing low loading conditions such as the ones experienced during the COVID-19 pandemic of 2020.

Future work will focus on considering distribution systems with high penetration of renewable energy resources while evaluating both frequency and voltage stability problems caused by load-changing attacks. Systems with high penetration of intermittent renewable energy resources (such as PV and wind energy) are expected, due to the non-existent coordination of voltage regulation devices and the impacted system inertia (e.g, the removal of synchronous generators results in less system inertia with impacts on transient and small-signal stability), to be more vulnerable to load-changing attacks when considering their effects in other system areas and control routines such as voltage regulation. Another area of research will be the impact evaluation of other types of cyberattacks, such as false data injection attacks and time-delay attacks, in systems experiencing low loading conditions, such as the one investigated throughout this research.

REFERENCES

[1] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, and D. Kumar, "Understanding the Mirai botnet," in *Proc. 26th USENIX Secur. Symp.*, 2017, pp. 1093–1110.

[2] C. Konstantinou, A. Keliris, and M. Maniatakos, "Taxonomy of firmware trojans in smart grid devices," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.

[3] A. Cui, M. Costello, and S. J. Stolfo, "When firmware modifications attack: A case study of embedded exploitation," in *Proc. NDSS*, 2013, pp. 1–13.

[4] C. Konstantinou and M. Maniatakos, "Impact of firmware modification attacks on power systems field devices," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2015, pp. 283–288.

[5] X. Wang, C. Konstantinou, M. Maniatakos, and R. Karri, "ConFirm: Detecting firmware modifications in embedded systems using hardware performance counters," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2015, pp. 544–551.

[6] J. Jiang, J. Liang, K. Li, J. Li, H.-X. Duan, and J. Wu, "Ghost domain names: Revoked yet still resolvable," in *Proc. NDSS*, 2012, pp. 1–3.

[7] A. Greenberg. (2018). *The White House Warns on Russian Router Hacking, but Muddles the Message*. Accessed: Sep. 20, 2020. [Online]. Available: https://www.wired.com/story/white-house-warns-russian-router-hacking-mu%ddles-message/

[8] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. 27th USENIX Secur. Symp.*, 2018, pp. 15–32.

[9] X. Liu, J. Ospina, and C. Konstantinou, "Deep reinforcement learning for cybersecurity assessment of wind integrated power systems," *IEEE Access*, vol. 8, pp. 208378–208394, 2020.

[10] G. Raman, B. AlShebli, M. Waniek, T. Rahwan, and J. C.-H. Peng, "How weaponizing disinformation can bring down a city's power grid," *PLoS ONE*, vol. 15, no. 8, Aug. 2020, Art. no. e0236517.

[11] *Cyber Attack Trends: 2020 Mid-Year Report*. Accessed: Sep. 20, 2020. [Online]. Available: https://pages.checkpoint.com/cyber-attack-2020-trends.html?utm_source=b%log&utm_medium=cp-website&utm_campaign=cm_wr_20q3_ww_mid_year_trends_report

[12] (Aug. 2020). *INTERPOL Report Shows Alarming Rate of Cyberattacks During COVID-19*. Sep. 15, 2020. [Online]. Available: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-s%hows-alarming-rate-of-cyberattacks-during-COVID-19

[13] (Jan. 2020). *Watch Out for Coronavirus Phishing Scams*. Accessed: Sep. 16, 2020. [Online]. Available: https://www.wired.com/story/coronavirus-phishing-scams/

[14] (Jun. 2020). *How Hackers are Using COVID-19 to Find New Phishing Victims*. Accessed: Sep. 16, 2020. [Online]. Available: https://www.securitymagazine.com/articles/92666-how-hackers-are-using-c%ovid-19-to-find-new-phishing-victims

[15] (Mar. 2020). *After 'Zoom Bombings', Other Incidents, FBI Warns of Videoconferencing Hijacking Amid Coronavirus*. Accessed: Sep. 16, 2020. [Online]. Available: https://abcnews.go.com/US/fbi-warns-video-conference-hijacking-amid-cor%onavirus-pandemic/story?id=69901757

[16] (Mar. 2020). *Zoombombing-Attacks Disrupt Classes*. Accessed: Sep. 17, 2020. [Online]. Available: https://www.insidehighered.com/news/2020/03/26/zoombombers-disrupt-onli%ne-classes-racist-pornographic-content

[17] (Nov. 2020). *Weekly Internet Health Check, US and Worldwide*. Accessed: Nov. 5, 2020. [Online]. Available: https://www.networkworld.com/article/3534130/covid-19-weekly-health-che%ck-of-isps-cloud-providers-and-conferencing-services.html

[18] (Oct. 2020). *Cybersecurity to be a Crucial Priority in Power Utilities's Agenda as Threats Continue to Grow Amid COVID-19, Says GlobalData*. Accessed: Oct. 29, 2020. [Online]. Available: https://www.power-technology.com/comment/cybersecurity-power-utilities-%agenda-covid-19-globaldata/

[19] (Oct. 2020). *The US Power Sector Has Prevented Millions of Cyberattacks in 2020—That Takes 24/7 Commitment*. Accessed: Oct. 30, 2020. [Online]. Available: https://www.utilitydive.com/news/the-us-power-sector-has-prevented-mill%ions-of-cyberattacks-in-2020-that-t/587949/

[20] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2862–2872, Jul. 2018.

[21] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well," in *Proc. 33rd Annu. Comput. Secur. Appl. Conf.*, Dec. 2017, pp. 303–314.

[22] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable?" *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5099–5113, Nov. 2020.

[23] L. Wang, L. Pepin, Y. Li, F. Miao, A. Herzberg, and P. Zhang, "Securing power distribution grid against power botnet attacks," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2019, pp. 1–5.

[24] A. Passo, S. Bahramirad, J. Beerten, E. Bernabeu, B. Chiu, B. Enayati, B. Hederman, L. Jones, Y. Jun, H. Koch. (2020). *Sharing Knowledge on Electrical Energy Industry's First Response to COVID-19*. Accessed: Sep. 20, 2020. [Online]. Available: https://resourcecenter.ieee-pes.org/publications/white-papers/PES_TP_CO%VID19_050120.html

[25] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against IoT demand attacks," in *Proc. 28th USENIX Secur. Symp.*, 2019, pp. 1115–1132.

[26] (2020). *COVID-19 Impact on Electricity*. Accessed: Sep. 20, 2020. [Online]. Available: https://www.iea.org/reports/covid-19-impact-on-electricity

[27] I. Santiago, A. Moreno-Munoz, P. Quintero-Jiménez, F. Garcia-Torres, and M. J. Gonzalez-Redondo, "Electricity demand during pandemic times: The case of the COVID-19 in spain," *Energy Policy*, vol. 148, Jan. 2021, Art. no. 111964.

[28] J. V. B. Andrade, R. S. Salles, M. N. S. Silva, and B. D. Bonatto, "Falling consumption and demand for electricity in south Africa–A blessing and a curse," in *Proc. IEEE PES/IAS PowerAfrica*, Aug. 2020, pp. 1–5.

[29] *COVID-19 Related Updates*. Accessed: Sep. 20, 2020. [Online]. Available: https://www.nyiso.com/covid

[30] D. Eryilmaz, M. Patria, and C. Heilbrun, "Assessment of the COVID-19 pandemic effect on regional electricity generation mix in NYISO, MISO, and PJM markets," *Electr. J.*, vol. 33, no. 7, Aug. 2020, Art. no. 106829. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1040619020301214

[31] H. Zhong, Z. Tan, Y. He, L. Xie, and C. Kang, "Implications of covid-19 for the electricity industry: A comprehensive review," *CSEE J. Power Energy Syst.*, vol. 6, no. 3, pp. 489–495, 2020.

[32] D. Agdas and P. Barooah, "Impact of the COVID-19 pandemic on the U.S. electricity demand and supply: An early view from data," *IEEE Access*, vol. 8, pp. 151523–151534, 2020.

[33] D. Carmon, A. Navon, R. Machlev, J. Belikov, and Y. Levron, "Readiness of small energy markets and electric power grids to global health crises: Lessons from the COVID-19 pandemic," *IEEE Access*, vol. 8, pp. 127234–127243, 2020.

[34] G. Ruan, D. Wu, X. Zheng, H. Zhong, C. Kang, M. A. Dahleh, S. Sivaranjani, and L. Xie, "A cross-domain approach to analyzing the short-run impact of COVID-19 on the US electricity sector," *Joule*, vol. 4, no. 11, pp. 2322–2337, Nov. 2020.

[35] (Jul. 2020). *Policy Brief: COVID-19 in an Urban World*. Accessed: Sep. 21, 2020. [Online]. Available: https://www.un.org/sites/un2.un.org/files/sg_policy_brief_covid_urban_w%orld_july_2020.pdf

[36] R. Paul, A. A. Arif, O. Adeyemi, S. Ghosh, and D. Han, "Progression of COVID-19 from urban to rural areas in the United States: A spatiotemporal analysis of prevalence rates," *J. Rural Health*, vol. 36, no. 4, pp. 591–601, Sep. 2020.

[37] J. N. Kutz, S. L. Brunton, B. W. Brunton, and J. L. Proctor, *Dynamic Mode Decomposition: Data-Driven Modeling of Complex Systems*. Philadelphia, PA, USA: SIAM, 2016.

[38] J. L. Proctor and P. A. Eckhoff, "Discovering dynamic patterns from infectious disease data using dynamic mode decomposition," *Int. Health*, vol. 7, no. 2, pp. 139–145, Mar. 2015.

[39] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou. (2020). *Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies*. Accessed: Dec. 27, 2020. [Online]. Available: http://dss-lab.github.io/pub/journals/CPESsecurity.pdf

[40] Z. Zhang, Y. Wang, and L. Xie, "A novel data integrity attack detection algorithm based on improved grey relational analysis," *IEEE Access*, vol. 6, pp. 73423–73433, 2018.

[41] J. D. Glover, M. S. Sarma, and T. Overbye, *Power System Analysis & Design*. Boston, MA, USA: Cengage Learning, 2012.

[42] E. Lannoye and A. Tuohy, *COVID-19: Flexibility and the Grid: Improving Available Flexibility for Abnormal Grid Operating Conditions*, document Product ID: 3002019550, Electric Power Research Institute (EPRI), 2020.

[43] *NERC Reliability Standard*. Accessed: Sep. 20,2020. [Online]. Available: https://www.nerc.com/pa/Stand/Generator%20Verification%20Project%202%00709%20Related%20File/PRC-024-1_WebEx_Slides_2009Feb26.pdf

[44] ERCOT Nodal Operating Guides. *Section 2: System Operations and Control Requirements*. Accessed: Sep. 21, 2020. [Online]. Available: http://www.ercot.com/mktrules/guides/noperating/library

[45] *NYISO Emergency Operations Manual*. Accessed: Sep. 21, 2020. [Online]. Available: https://www.nyiso.com/documents/20142/2923301/em_op_mnl.pdf/99ef389d-4b%ca-fc0e-f12e-d91c0763cdca

[46] *ERCOT Fundamentals Training Manual*. Accessed: Sep. 21, 2020. [Online]. Available: http://www.ercot.com/content/wcm/lists/161158/ERCOT_Fundamentals_Manual%.pdf

[47] C. Konstantinou and M. Maniatakos, "A case study on implementing false data injection attacks against nonlinear state estimation," in *Proc. 2nd ACM Workshop Cyber-Phys. Syst. Secur. Privacy CPS-SPC*, 2016, pp. 81–92.

[48] O. M. Anubi and C. Konstantinou, "Enhanced resilient state estimation using data-driven auxiliary models," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 639–647, Jan. 2020.

[49] *Power System Analysis Toolbox (PSAT)*. Accessed: Sep. 22, 2020. [Online]. Available: http://faraday1.ucd.ie/psat.html

JUAN OSPINA (Member, IEEE) received the dual B.Sc. degree in electrical and computer engineering and the M.S. and Ph.D. degrees in electrical engineering from Florida State University, Tallahassee, FL, USA, in 2016, 2018, and 2019, respectively. He is currently a Postdoctoral Research Associate with Florida State University and the Center for Advanced Power Systems, Tallahassee. His research interests include the development of intelligent systems for electric power systems (EPS) and smart-grid applications, machine learning and reinforcement learning models for DER control, renewable energy integration, cybersecurity, and real-time simulation. He is a member of IEEE PES.
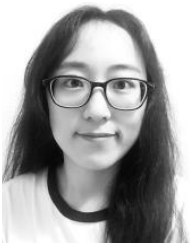
XIAORUI LIU (Student Member, IEEE) received the M.S. degree in electrical engineering from Florida State University, Tallahassee, FL, USA, in 2017, where she is currently pursuing the Ph.D. degree in electrical engineering. Her research interests include real-time simulation of power systems, cybersecurity, and machine learning.

CHARALAMBOS KONSTANTINOU (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from New York University, NY, in 2018. He is currently an Assistant Professor of electrical and computer engineering with Florida A&M University, and the FAMU-FSU College of Engineering and the Center for Advanced Power Systems, Florida State University, Tallahassee, FL. His research interests include cyberphysical and embedded systems security with a focus on power systems. He was a recipient of the Best Paper Award at the International Conference on Very Large Scale Integration (VLSI-SoC) in 2018, the Southeastern Center for Electrical Engineering Education (SCEEE) Young Faculty Development Award in 2019, and the 2020 Myron Zucker Student-Faculty Grant Award from IEEE Foundation.

YURY DVORKIN (Member, IEEE) received the Ph.D. degree from the University of Washington, under the supervision of Prof. Daniel S. Kirschen. He is currently an Assistant Professor and a Goddard Junior Faculty Fellow with the Department of Electrical and Computer Engineering, New York University's Tandon School of Engineering and the Center for Urban Science and Progress. His research interests include energy economics, civil infrastructure systems, and energy transition. Before joining NYU, he was a Graduate Student Researcher with the Los Alamos National Laboratory, Center for Nonlinear Studies, under the supervision of Dr. Michael Chertkov and Dr. Scott Backhaus. His research work has been supported by the U.S. National Science Foundation, including the 2019 NSF CAREER Award, the Alfred P. Sloan Foundation, the U.S. Department of Energy and Advanced Research Projects Agency–Energy, and the Electric Power Research Institute. For his dissertation work, titled "Operations and Planning in Sustainable Power Systems," he was awarded the Inaugural 2016 Scientific Achievement Award by the Clean Energy Institute, University of Washington.

. . .