energies

MDPI

Article

On the Feasibility of Market Manipulation and Energy Storage Arbitrage via Load-Altering Attacks

Juan Ospina *, David M. Fobes and Russell Bent

Los Alamos National Laboratory, Los Alamos, NM 87545, USA
* Correspondence: jjospina@lanl.gov

Abstract: Around the globe, electric power networks are transforming into complex cyber–physical energy systems (CPES) due to the accelerating integration of both information and communication technologies (ICT) and distributed energy resources. While this integration improves power grid operations, the growing number of Internet-of-Things (IoT) controllers and high-wattage appliances being connected to the electric grid is creating new attack vectors, largely inherited from the IoT ecosystem, that could lead to disruptions and potentially energy market manipulation via coordinated load-altering attacks (LAAs). In this article, we explore the feasibility and effects of a realistic LAA targeted at IoT high-wattage loads connected at the distribution system level, designed to manipulate local energy markets and perform energy storage (ES) arbitrage. Realistic integrated transmission and distribution (T&D) systems are used to demonstrate the effects that LAAs have on locational marginal prices at the transmission level and in distribution systems adjacent to the targeted network.

Keywords: AC optimal power flow; energy arbitrage; load-altering attack; market manipulation; nonlinear optimization

Citation: Ospina, J.; Fobes, D.M.; Bent, R. On the Feasibility of Market Manipulation and Energy Storage Arbitrage via Load-Altering Attacks. *Energies* **2023**, *16*, 1670. https://doi.org/10.3390/en16041670

Academic Editors: Paulo Fernando Ribeiro, Yuri Rodrigues, Maira Monteiro and Tek Tjing Lie

Received: 13 December 2022
Revised: 20 January 2023
Accepted: 3 February 2023
Published: 7 February 2023

1. Introduction

Efforts aimed at modernizing the power grid have accelerated the adoption and integration of information and communication technologies (ICT) into the modern power grid infrastructure. This modernization is tailored to improving operational awareness, providing control and monitoring mechanisms, and facilitating the deployment of distributed energy resources (DERs) into older, passive power networks, transforming them into modern cyber–physical energy systems (CPES). However, the large-scale deployment of these technologies, together with an increasing number of Internet-of-Things (IoT) high-wattage consumer appliances, are opening new attack vectors, largely inherited from the IoT ecosystem, that malicious threat actors can leverage to cause disruptions in the power grid infrastructure [1] or induce energy market price manipulation [2,3].

Cybersecurity is clearly becoming a prerequisite in the modernization of power networks. Over the past few years in the US, several executive orders and governmental reports have focused on addressing concerns related to potential cyberattacks targeted at the electric grid [4]. For example, the 2021 Annual Threat Assessment of the US Intelligence Community stated that "*foreign states use cyber operations to steal information, influence populations, and damage industry, including physical and digital critical infrastructure*" [5]. Though *successful* cyberattacks targeted at either disrupting power network operations or manipulating energy markets are still thought to be rare, i.e., there are just a handful of public examples, e.g., the 2015 and 2016 Ukraine cyberattacks [6], a successful high-impact, low probability cyberattack could have catastrophic effects in a nation's society.

Recent attacks by threat actors attempting to compromise the electric grid are increasingly thought to be motivated by financial gain, in contrast to the traditional type of cyberattacks led by nation-states, thought to be intended to destabilize the grid [2,7]. For these malicious actors, money can be obtained by stealing financial information, stealing

intellectual property, or by extortion via a ransomware attack [8]. One novel way of obtaining profits is via the market manipulation of local real-time energy markets [2,9]. The concept of market manipulation stems from the notion of creating or inducing high prices, e.g., by artificially manipulating the supply and demand of a commodity. According to the Federal Energy Regulatory Commission (FERC), the regulatory agency for electricity markets in the US, in 2018, at least 16 potential energy market manipulation cases were identified, thus identifying energy market manipulation as a matter of great concern [2].

Energy market manipulation could be realized in many ways, e.g., famously, Enron traders manipulated the energy market by filing nonexistent transmission schedules, alleviating nonexistent power congestion, and buying artificially price-inflated energy [10,11]. Energy market manipulation can also be accomplished by destabilizing the supply and demand balance of power, increasing energy prices via artificial load increases or generation reductions. For example, researchers previously demonstrated that an attacker could leverage vulnerabilities in IoT high-wattage devices to manipulate energy market based on a manipulation of market via IoT (MaMIoT) attack with the objective of generating profits and/or causing major economic damage to a sector of the energy market [11]. Another example is the research in [12], where authors present a zero-day load-altering attack (LAA) designed to exploit the mutual dependency of the price of electricity and power consumption in demand response programs by altering the power consumption of several electric loads. The authors propose a transactive energy framework capable of mitigating oversupply and undersupply fluctuations caused by the LAA through real-time energy transactions. Further, in [13], researchers explored the effects of a variety of load-altering attacks (LAAs) (prior work used other names, such as "load-changing attacks" [14], "dynamic load-altering attacks" [15], "manipulation of demand via IoT (MadIoT)" [13], among others) aimed at disrupting power grid operations and causing frequency and voltage instabilities. Algorithms attempting to find efficient generator operating points to avoid line overloading during LAAs have even been proposed to defend from these types of attacks [16]. Similarly, in [17], a transactive energy framework is proposed to thwart LAAs targeted at disrupting the automatic generation control (AGC) mechanism to cause frequency fluctuations. The proposed transactive energy framework coordinates flexible loads and the power grid operator by performing real-time adjustments in the power consumption of flexible loads in response to the frequency disturbances caused by the LAAs.

Other research on LAAs has primarily focused on exploring their effects in terms of frequency and voltage stability and analyzing potential attack vectors. In [14,18], the effects on frequency stability of LAAs during low loading and low-inertia conditions caused by pandemic-type events and high penetration of renewable energy resources are explored. Additionally, in [19], the authors investigate a closed-loop dynamic load-changing attack specifically tailored to threaten the frequency stability of a power network by controlling a compromised load based on frequency feedback. Ref. [15] examines the feasibility of a major blackout in the New York area caused by a load-altering attack (LAA) targeted at compromising electric vehicle (EV) charging stations. Finally, [20,21] explore other protection and defense mechanisms using data-driven methods to detect and mitigate LAAs via the use of energy storage (ES) devices.

Contributions

From the literature examined, we can conclude that an abrupt and stealthy manipulation of load demand, e.g., via a coordinated large-scale Botnet-type attack against IoT-connected high wattage loads, has the potential to severely affect the balance between the supply and demand of power. This 'manipulation' could lead to situations where energy suppliers may profiteer due to high operational costs being incurred by the system operator in order to keep the system stable. In this work, we explore the feasibility of energy market manipulation based on a realistic LAA targeted at IoT high-wattage loads connected at the distribution system level, with the main objective being to manipulate the

locational marginal prices (LMPs) of highly unbalanced systems, thus disrupting the local energy market for both consumers and energy suppliers in both the targeted distribution feeder and in adjacent distribution feeders. We also explore the feasibility of implementing an ES arbitrage strategy that benefits from and generates substantial profits from targeted LAAs and optimal dispatch schedules. The research contributions are as follows:

- We define the mathematical and threat models of realistic LAAs targeted at compromising IoT-connected high wattage loads (e.g., smart heating, ventilation, and air conditioning (HVAC) systems, EV charging stations, etc.) in a distribution system.
- We investigate the feasibility of LAA-assisted ES arbitrage performed by energy suppliers at the distribution-system level.
- We study the effects that a coordinated LAA has in the LMPs at both the transmission and distribution levels by analyzing the LMPs in the targeted distribution feeder and exploring how these effects propagate through the transmission system to adjacent distribution feeders.

The rest of the paper is organized as follows. In Section 2, we present the mathematical and theoretical models for performing energy market manipulation and ES arbitrage studies based on the proposed LAA. Section 3 presents the analysis and exploration of the feasibility of an LAA-assisted energy storage arbitrage strategy. Section 4 explores the feasibility of energy price manipulation via LAAs based on the effects that these load increases cause in adjacent distribution feeders. Finally, Section 5 concludes the paper and provides directions for future work.

2. Feasibility of Load-Altering Attacks in Power Networks

2.1. IoT High-Wattage HVAC Load-Altering Attack Scenario

HVAC systems play a crucial role in our modern society, maintaining indoor air quality and providing thermal comfort. According to the U.S. Energy Information Administration (EIA), ∼389 billion kWh were used in the U.S. for residential and commercial space cooling in 2021, accounting for ∼10% of the total U.S. electricity consumption [22]. The residential sector alone was responsible for ∼235 billion kWh and ∼207 billion kWh of energy consumption for cooling and heating, respectively [22].

However, although HVACs are essential for comfort and survival in many regions, experts claim that the U.S. electric power grid may not be capable of sustaining the simultaneous operation of a large amount of HVAC systems in summer months due to a lack of power capacity [23]. In early 2022 in Texas, for example, a heat wave 'knocked' down six power plants [24]. This example could be artificially replicated through an LAA targeted at modifying the power consumption of IoT-connected HVAC systems. In this section, we present the details of a plausible LAA scenario performed via the exploitation of known vulnerabilities in a digital logic controller intended for building automation and HVAC control.

2.1.1. Description of Potential Vulnerability

On 30 September 2021, a critical authentication bypass vulnerability, CVE-2021-41292 (https://nvd.nist.gov/vuln/detail/CVE-2021-41292 (accessed on 1 June 2022)), was discovered and published on the National Vulnerability Database of the National Institute of Standards and Technology (NIST). This vulnerability affects ECOA BAS building automation controllers by allowing unauthenticated attackers the capability of manipulating HVAC and building automation control signals through network access. The unauthenticated attacker can compromise the controller through cookie poisoning, remotely bypassing authentication procedures (CWE-288) and circumventing physical access controls, causing the disclosure of sensitive information. The CVSS v3.x scores assigned by NIST and TWCERT/CC to this vulnerability were 9.1 critical and 9.8 critical, respectively. The described vulnerability is an illustrative example for a potential vulnerability that could be exploited by threat actors trying to destabilize the system or gain financial benefits by compromising several IoT devices connected to the electric grid. Other 0-day or unpatched

vulnerabilities found in similar devices, or in the network devices that connect them, could enable an equivalent type of attack.

2.1.2. Attack Scenario

Based on the vulnerability described, it is therefore not unreasonable to imagine that a sufficiently motivated attacker could exploit the CVE-2021-41292 vulnerability, or other yet undiscovered 0-day vulnerability, and perform the LAA by modifying the operating mode of all the HVAC units controlled in a commercial building, causing them to consume the maximum amount of power possible.

Assuming a large residential or commercial building could have on average 10–30 HVAC units, each rated between 7–16 kW; we could estimate that compromising just one large building with 30 HVAC units could result in a maximum power consumption of ∼480 kW. Thus, an attacker capable of coordinating multiple LAAs targeted at large residential and commercial buildings could significantly increase the power consumption of a zone or region, triggering a spike of the 'real-time' energy prices.

2.2. Mathematical ACP-ACPU OPF Formulation

Here, we present a description of the mathematical optimal power flow (OPF) problem formulation used to evaluate the feasibility of market manipulation and ES arbitrage in integrated T&D systems. The problem formulation used herein is based on the AC-polar ACP-ACPU formulation (ACP-ACPU indicates the transmission system is modeled using a single-phase AC polar formulation and the distribution system(s) is(are) modeled using the *phase unbalanced* AC-polar formulation) presented in detail in [25]. The primary advantage of using an integrated T&D formulation is that it enables us to analyze the effects of distribution-level LAAs at the transmission system-level and vice versa. This capability allows us to identify the potential impact an LAA could have in a real T&D system.

The cost function to minimize in this formulation is:

$$\min \left(\sum_{k \in G^{\mathcal{T}}} \mathcal{C}(P_{g,k}^{\mathcal{T}}) + \sum_{m \in G^{\mathcal{D}}} \sum_{\varphi \in \Phi} \mathfrak{C}(P_{g,m}^{\mathcal{D},\varphi}) \right) \tag{1}$$

where $\mathcal{C}$ and $\mathfrak{C}$ represent the cost components for specific generators in the transmission and distribution networks, respectively. Equation (1) minimizes the total cost of active power generation subject to constraints presented in [25].

2.3. Locational Marginal Prices

Based on the formulated ACOPF problem, the Lagrangian function of the optimization problem can be defined as Equation (2) [26], where λ and ν represent the Lagrange multipliers related to the active and reactive power balance equations (Equations (10), (11), (30) and (31) of [25]). For simplicity, let the vectors x and u represent all state variables and all control variables, respectively. We can then define the transmission and distribution system(s) inequality constraints as $h^{\mathcal{T}}(x,u) \leq 0$ and $h^{\mathcal{D}}(x,u) \leq 0$, respectively; $\mu_z^{\mathcal{T}}$ and $\mu_z^{\mathcal{D}}$ represent the Lagrange multipliers associated with the inequality constraints $h_z^{\mathcal{T}}(x,u)$ and $h_z^{\mathcal{D}}(x,u)$. $\mathcal{H}^{\mathcal{T}}$ and $\mathcal{H}^{\mathcal{D}}$ represent the set of inequality constraints for the transmission and distribution systems. β represents a *boundary* bus, i.e., a bus that belongs to $\mathcal{B}$.

$$\begin{aligned} L(x,u,\lambda^{\mathcal{T}},\nu^{\mathcal{T}},\mu^{\mathcal{T}},\lambda^{\mathcal{D}},\nu^{\mathcal{D}},\mu^{\mathcal{D}}) = & \sum_{k \in G^{\mathcal{T}}} \mathcal{C}(P_{g,k}^{\mathcal{T}}) \\ & + \sum_{m \in G^{\mathcal{D}}} \sum_{\varphi \in \Phi} \mathfrak{C}(P_{g,m}^{\mathcal{D},\varphi}) \\ & - \sum_{i \in N^{\mathcal{T}}} \lambda_i^{\mathcal{T}} \cdot \left(\sum_{k \in G_i^{\mathcal{T}}} P_{g,k}^{\mathcal{T}} - P_{d,i}^{\mathcal{T}} - \sum_{\substack{(i,\beta) \in \Lambda \\ \beta \in N^{\mathcal{D}} \cap N^{\mathcal{B}}}} P_{i\beta}^{\mathcal{T}} - \Re\{V_i^{\mathcal{T}} \cdot (I_i^{\mathcal{T}})^*\} \right) \end{aligned}$$

$$
\begin{aligned}
&- \sum_{i \in N^{\mathcal{T}}} \nu_i^{\mathcal{T}} \cdot \Bigg(\sum_{k \in G_i^{\mathcal{T}}} Q_{g,k}^{\mathcal{T}} - Q_{d,i}^{\mathcal{T}} - \sum_{\substack{(i,\beta) \in \Lambda \\ \beta \in N^{\mathcal{D}} \cap N^{\mathcal{B}}}} Q_{i\beta}^{\mathcal{T}} - \Im\{V_i^{\mathcal{T}} \cdot (I_i^{\mathcal{T}})^*\} \Bigg) \\
&+ \sum_{z \in \mathcal{H}^{\mathcal{T}}} \mu_z^{\mathcal{T}} \cdot h_z^{\mathcal{T}}(x,u) \\
&- \sum_{i \in N^{\mathcal{D}}} \sum_{\varphi \in \Phi} \lambda_i^{\mathcal{D},\varphi} \Bigg(\sum_{m \in G_i^{\mathcal{D}}} \sum_{\varphi \in \Phi} P_{g,m}^{\mathcal{D},\varphi} - \sum_{\varphi \in \Phi} P_{d,i}^{\mathcal{D},\varphi} - \sum_{\substack{(i,\beta) \in \Lambda \varphi \in \Phi \\ \beta \in N^{\mathcal{T}} \cap N^{\mathcal{B}}}} \sum P_{i\beta}^{\mathcal{D},\varphi} \\
&- \Re\{V_i^{\mathcal{D},\varphi} \cdot (I_i^{\mathcal{D},\varphi})^*\} \Bigg) \\
&- \sum_{i \in N^{\mathcal{D}}} \sum_{\varphi \in \Phi} \nu_i^{\mathcal{D},\varphi} \Bigg(\sum_{m \in G_i^{\mathcal{D}}} \sum_{\varphi \in \Phi} Q_{g,m}^{\mathcal{D},\varphi} - \sum_{\varphi \in \Phi} Q_{d,i}^{\mathcal{D},\varphi} - \sum_{\substack{(i,\beta) \in \Lambda \varphi \in \Phi \\ \beta \in N^{\mathcal{T}} \cap N^{\mathcal{B}}}} \sum Q_{i\beta}^{\mathcal{D},\varphi} \\
&- \Im\{V_i^{\mathcal{D},\varphi} \cdot (I_i^{\mathcal{D},\varphi})^*\} \Bigg) \\
&+ \sum_{z \in \mathcal{H}^{\mathcal{D}}} \mu_z^{\mathcal{D}} \cdot h_z^{\mathcal{D}}(x,u)
\end{aligned} \tag{2}
$$

Assuming the formulated ACOPF problem has an optimal (x^*, u^*), the marginal cost to supply the next increment of load demand can be estimated as [26,27]:

$$LMP_i^{\varphi} = \left. \frac{\partial f}{\partial P_{d,i}} \right|_{x^*,u^*} = \lambda_i^{\varphi} \tag{3}$$

where λ_i^{φ} is the Lagrange multiplier related to the active power balance equation at bus i and phase φ. This term represents the locational marginal price (LMP) of the specific load and phase. Consequently, we can deduce that every bus in the system will have a different LMP dependent on its location and phase, primarily due to the unbalanced nature of distribution systems. We note that transmission system buses will have only one LMP due to the representation of the transmission system being a single-phase positive sequence model, while distribution system buses will have a maximum of three LMPs due to their representation as three-phase (kron-reduced) models. Based on the LMPs computed from the ACOPF solution, we are able to estimate the impact of load variations in a 'real-time' energy price, since in a 'real-time' energy market, LMPs are the primary drivers behind energy price variations.

2.4. Energy Storage Arbitrage Optimization

To evaluate the feasibility of LAA-assisted energy storage arbitrage, we modify the ACOPF formulation to include ES optimization and time-series support. We assume the optimization of the ES to be optimal from the attacker's perspective in order to estimate the maximum profit an attacker could be capable of obtaining.

Equation (1) is modified to account for ES cycling costs, assuming in this case that the ES is a lithium-ion battery connected at the distribution-system level (i.e., is multi-conductor).

$$\min \sum_{t=1}^{T} \left(\sum_{k \in G^{\mathcal{T}}} \mathcal{C}(P_{g,k}^{\mathcal{T},t}) + \sum_{m \in G^{\mathcal{D}}} \sum_{\varphi \in \Phi} \mathfrak{C}(P_{g,m}^{\mathcal{D},\varphi,t}) + sd_t \cdot r_{ES} \right) \tag{4}$$

where sd_t is the active power discharge of the ES at time t, r_{ES} is the cost of cycling the ES battery, and T is the total number of time steps. The cost, or price, for cycling the ES is estimated by:

$$r_{ES} = \frac{c_{ES}}{cyc \cdot e^u \cdot dod \cdot (\eta^c \cdot \eta^d)} \tag{5}$$

where c_{ES} is the total cost of the ES system, cyc is the number of cycles the ES system has under warranty at a specific depth-of-discharge (dod), e^u is the energy rating, and η^c and η^d are the charging and discharging efficiencies [28].

The following additional constraints related to the ES system must also be added [29]:

$$e_t - e_s = te\left(\eta^c sc_t - \frac{sd_t}{\eta^d}\right) \tag{6}$$

$$sc_t \cdot sd_t = 0 \tag{7}$$

$$S_{es,t} + (sd_t - sc_t) = j \cdot sqc_t + S^l_{es} + Z_{es}|I_{es,t}|^2 \tag{8}$$

$$q^l_{es} \leq \Im(S_{es,t}) \leq q^u_{es} \tag{9}$$

$$|S_{es,t}| \leq s^u_{es} \tag{10}$$

$$|I_{es,t}| \leq i^u_{es} \tag{11}$$

where Equation (6) represents the ES storage state at time t based on the previous storage state, charge and discharge efficiencies, time elapsed, and charge and/or discharge active power values. Equation (7) ensures that the charging and discharging operations are mutually exclusive, and Equation (8) computes the losses of the ES. Lastly, Equations (9)–(11) enforce the reactive power limits, thermal injection limits, and current injection limits, respectively.

2.5. Load-Altering Attack Model

In this section, we present the mathematical and threat models for the LAA.

2.5.1. Mathematical Model

In order to mathematically define the LAA, let us consider a simple CPES represented by:

$$x(t+1) = Gx(t) + Bu(t) \tag{12}$$

$$y(t) = Cx(t) + e(t) \tag{13}$$

where Equation (12) computes the physical system state at time $t+1$ based on the control variables $u(t) \in \mathbb{R}^l$, the physical system states $x(t) \in \mathbb{R}^n$ at time t, and matrices $G \in \mathbb{R}^{n \times n}$ and $B \in \mathbb{R}^{n \times l}$ that characterize the system. In turn, Equation (13) calculates the physical system measurements $y(t) \in \mathbb{R}^m$ from the physical system states $x(t)$, the matrix $C \in \mathbb{R}^{m \times n}$, and the input measurement noise $e \in \mathbb{R}^m$. The cyber-layer of the CPES can be expressed as:

$$u(t+1) = Hy(t) \tag{14}$$

where Equation (14) computes the control variables at time $t+1$ based on the the system's measurements and the control matrix $H \in \mathbb{R}^{l \times m}$ [14]. Based on this mathematical formulation, an LAA can be defined as a data integrity attack (DIA) that compromises the measurements, y, or the controls, u, of the CPES via modification. In our case, the controls can be 'altered' (u^a) by adding a Δ value that represents the adversary injected control variations as:

$$u^a = u + \Delta u \tag{15}$$

This modification affects the CPES states and measurements by altering them as:

$$x^a(t+1) = Gx(t) + Bu^a(t) \tag{16}$$

$$y^a(t+1) = C\Big(x^a(t+1)\Big) + e(t+1) \tag{17}$$

where x^a and y^a represent the altered system's states and measurements. From the attacker's perspective, the LAA is performed in the internal control loop of the high-wattage IoT-connected load. In essence, the power output of the load can be altered as $P_{iot}(t) = P_{iot}(t) + \Delta P_{iot}(t)$. However, from the ACOPF perspective, the LAA is reflected as

an alteration in the total load demand of the compromised power system bus or node at time t:

$$P_d(t) = P_d(t) + \Delta P_d(t) \tag{18}$$

2.5.2. Threat Model

We present the threat model of the LAA considered in this work in Table 1, developed using the modeling technique presented in [30].

Table 1. Threat model for LAA.

Threat Model \Threat	LAA
Knowledge	Semi-Oblivious
Access	Non-possession
Specificity	Targeted
Resources	Class II
Frequency	Iterative
Reproducibility	Multiple-times
Attack Func. Level	L1
Asset	High-wattage IoT devices
Technique	Control logic modification
Premise	Cyber: Integrity

As seen in the table, we consider a *semi-oblivious* attacker, i.e., with partial knowledge of the operation and loading conditions of the power system. We note that a *strong-knowledge adversary*, e.g., an *insider* threat actor, could alternatively be considered. In our scenario, the attacker is capable of compromising *non-possessed* high-wattage IoT-connected appliances via a coordinated Botnet-type LAA deployed through the cyber-layer of the system. In terms of specificity, the threat is catalogued as a *targeted* attack that directly affects the LMPs of the power system's buses. The adversary's resources are classified as *Class II* due to the fact that the adversary needs the sufficient motivation and resources to carry out the LAA without being easily detected. The frequency and reproducibility of the threat are categorized as *iterative* and *multiple-times* considering that the attack must be performed in an iterative fashion while being undetectable when performed multiple-times, so that the altered energy prices can last a sufficient amount of time to obtain profits. The LAA is considered to target the *L1* level, where the control logic of the asset is *modified* via the *cyber: integrity* premise of the compromised high-wattage IoT-connected loads.

3. Analysis of Energy Storage Arbitrage via Load Altering Attacks

In this section, we present the experimental setup used for analyzing and exploring the feasibility of an LAA-assisted ES arbitrage strategy. For this analysis, we only consider the effects of the LAAs within the scope of a single mixed-voltage distribution system, i.e., the effects of the LAAs are evaluated within the local energy market of the modeled distribution system. Results are analyzed and discussed in terms of ES utilization and potential profits generated by the attacker, who owns the ES system and performs the LAA.

3.1. Test Systems

Our synthetic integrated T&D system, modeled and solved using *PowerModelsITD.jl* [25], consists of modified versions of the PJM 5-bus system (transmission), the R1-12.47-3 PNNL feeder (medium voltage (MV) distribution) [31] and a reduced version of the IEEE European low voltage test feeder (low voltage (LV) distribution) [32].

The following modifications are applied to the base data: (1) an additional bus is added to the transmission system, to which the MV substation is connected, (2) the HV/MV substation transformer ratings are modified to 230/7.2 kV and 10 MVA, (3) load *18* in the MV network is replaced with the LV network and the MV/LV substation transformer ratings are modified to 7.2/0.48 kV and 2000 kVA, and (4) a 720 kWh ES system capable of charging or discharging 80% of its rated power per time step (1 h) is connected at bus *lv_113.1.2.3*. Figure 1 shows the network topology of the test system, which has 519 nodes and 518 edges. We consider a time horizon of 24 hours, resulting in a total of 12,456 nodes and 12,432 edges in the overall optimization problem.

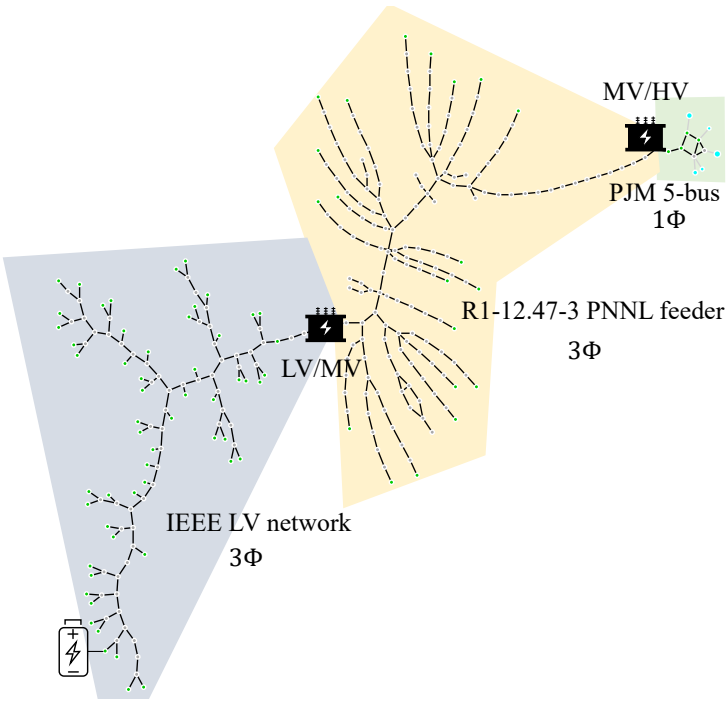

Figure 1. Energy arbitrage test system. PJM 5-bus (single-phase) + PNNL feeder (three-phase) + IEEE LV network (three-phase). The green nodes represent buses where loads are connected, gray nodes represent connecting buses, and the light blue nodes represent generation buses.

3.2. Case Studies

We consider the following case studies, all of which have a 24 h time horizon with 1 h time steps:

1. **Normal with ES**: Load is nominal and ES system is optimized.
2. **20% LAA increase with ES**: Compromised loads are increased by 20%, and ES system is optimized.
3. **50% LAA increase with ES**: Compromised loads are increased by 50%, and ES system is optimized.
4. **70% LAA increase with ES**: Compromised loads are increased by 70%, and ES system is optimized.
5. **100% LAA increase with ES**: Compromised loads are increased by 100%, and ES system is optimized.

The LAA is programmed to be executed between the hours of 5 and 9 pm, targeting 76 community and residential loads in the MV and LV networks. The lower right panel graph of Figure 2 shows example load profiles for the normal scenario and the 70% LAA scenario where compromised loads have a 70% increase in power consumption during the attack hours. The load profiles for the three loads connected at the transmission system level are based on residential (bus #2), community (bus #3), and commercial (bus #4) base load profiles derived from [33]. All load profiles, both normal and altered, are generated

stochastically. The r_{ES}, Equation (5), used for the optimization of the ES is USD 0.0870/kWh. This value is calculated based on c_{ES} = USD 216,000, dod = 0.8, cyc = 4400 [34], $\eta^c \cdot \eta^d$ = 0.98, and e^u = 720 kWh.

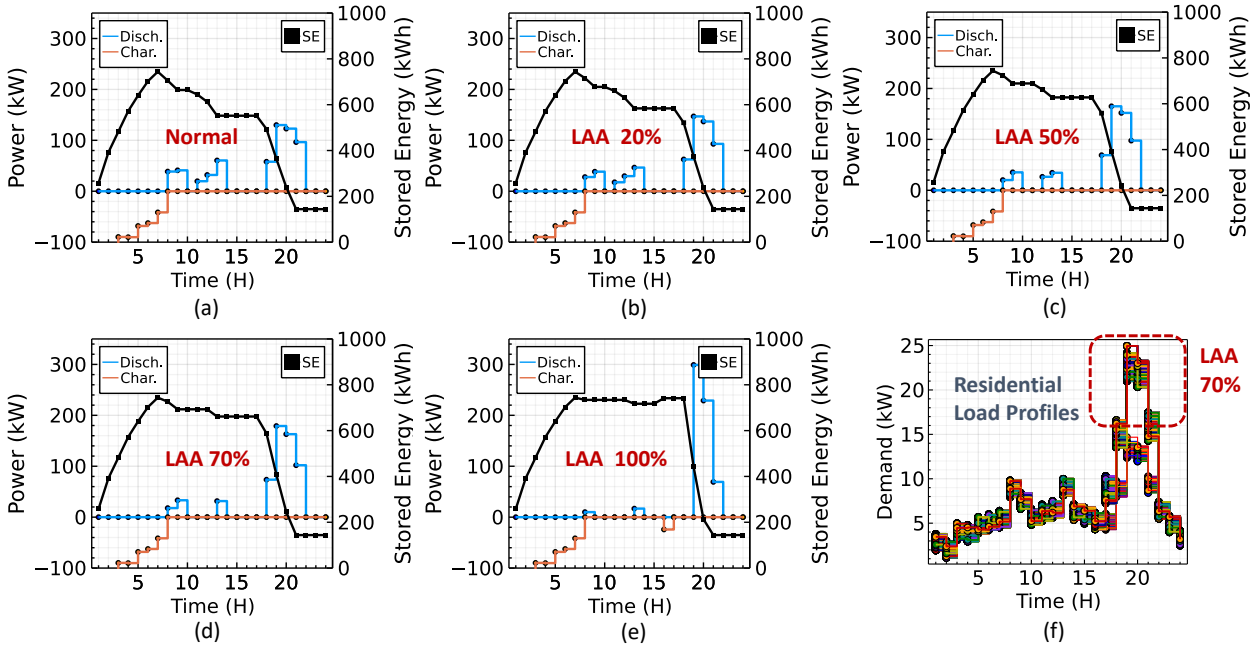

Figure 2. Energy storage (ES) charging and discharging operations for the: (**a**) normal scenario; (**b**) 20% LAA increase scenario; (**c**) 50% LAA increase scenario; (**d**) 70% LAA increase scenario; and (**e**) 100% LAA increase scenario. The blue line represents the discharging operations of the ES system, the orange line represents the charging operations of the ES system, and the black line represents the stored energy of the ES system. (**f**) shows the load profiles for the normal scenario and the 70% LAA scenario where compromised loads have a 70% increase in power consumption during the attack hours (i.e., during the 5 to 9 pm period).

3.3. Results

In order to explore the feasibility of an LAA-assisted ES arbitrage strategy, we compare the profit generated by the optimal operation of the ES in a normal day with the money generated in days where the LAAs are performed. Figure 2 shows the ES operation in all the presented scenarios. As seen in the figure, the ES system is charging at times where loading is low, thus the LMPs are low, and is discharging at times where loading is high. This operation is designed to generate profits by charging at times where low loading conditions are predicted and discharging at times where the attacker performs the LAA that generates artificial high loading conditions, thus selling the ES energy at higher prices. We importantly note that the act of charging and discharging the ES does modify the LMPs, per se, so in a real scenario, where not only the LMPs are considered as the buying or selling prices for energy, the results may deviate. Figure 3 shows the active power dispatch by the transmission generators (first two graphs) and the active power flowing at the boundary of the transmission-distribution system. These graphs clearly display the effect of the LAA in the system in terms of power generation and power flow at the T&D boundary.

In this study, we define profit as the total money received from dispatching the ES minus the total money paid for charging the ES, computed by multiplying the energy charged or discharged with the LMP at the ES-connected bus during the corresponding hour of the day. Based on our test cases, we find that the user in the normal scenario would generate around $243.37, the attacker that performs the 20% LAA would generate $253.75, the one that performs the 50% LAA would generate USD 269.89, the one that performs the 70% LAA would generate USD 279.67, and the attacker that performs the 100% LAA would generate around USD 317.92. Table 2 presents the profits differences of all the LAA

scenarios compared to the normal scenario. In this table, we can also observe the profit generated in 30 days and in 365 days if the LAAs are performed stealthily and persistently.

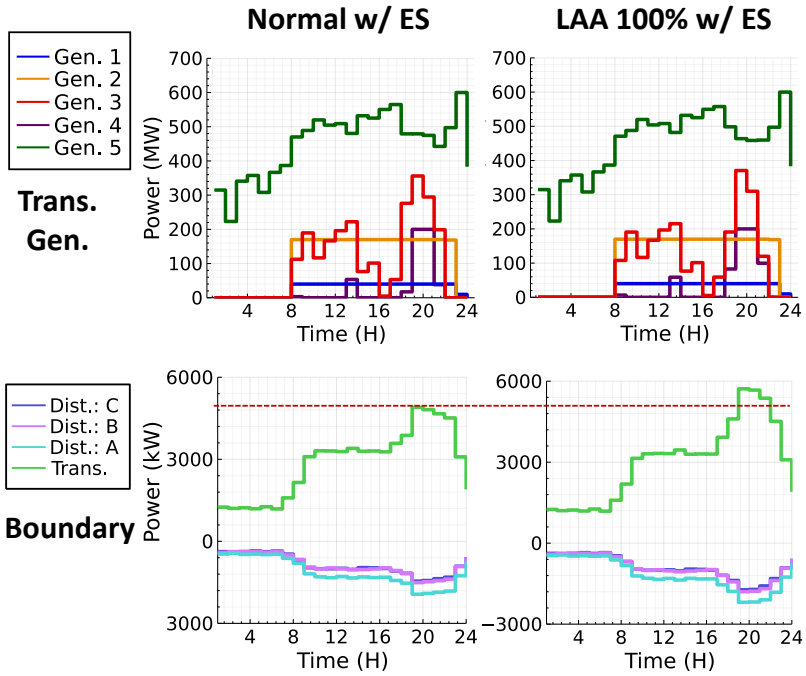

Figure 3. 24 h active power dispatch from transmission generators and active power flowing at the transmission–distribution boundary. The graphs on the left show the active power for the normal scenario where the ES system is optimized for energy arbitrage. The graphs on the right show the scenario where the LAA increases loads in the distribution system by 100%, and the ES system is optimized for energy arbitrage.

Table 2. Profit difference between normal case study scenario and LAA scenarios.

Profit Difference (LAA Scenario—Normal Scenario)		30 Days	365 Days
LAA 20%	USD 10.38	USD 311.30	USD 3787.49
LAA 50%	USD 26.52	USD 765.64	USD 9680.23
LAA 70%	USD 36.30	USD 1088.97	USD 13,249.14
LAA 100%	USD 74.55	USD 2236.44	USD 27,210.02

The total ES system cost is estimated by using NREL's 2021 utility-scale battery storage cost projection of approximately USD 300/kWh (lower bound); so, for a 720 kWh ES system the total cost would be approximately USD 216,000 [35]. Based on this total ES cost, the estimated payback period (in months) for someone optimizing this specific ES system would be ∼29 months for the normal case, while an attacker performing the 20%, 50%, 70%, and 100% LAAs consistently would have payback periods of ∼28 months, ∼26 months, ∼25 months, and ∼22 months, respectively, thus reducing the payback period by approximately 208 days (∼6 months). These results clearly demonstrate that at current ES prices, energy arbitrage could become feasible in specific sectors where energy prices have a high level of fluctuation throughout the day. However, it might be *unprofitable* for an attacker to perform ES arbitrage via low-impact LAAs (e.g., 20–50%), where a significant monetary benefit may not be achievable. Additionally, the risk behind performing this type of attack (currently) outweighs the potential benefits, and only compromising a significant number of devices (such as the 100% load increase scenario) for an extended period (at

least 365 days) may be profitable in terms of energy arbitrage. Notwithstanding, if other assumptions are considered, such as significant lower total ES system costs, higher energy dispatch prices, and higher number of loads compromised, LAA-assisted ES arbitrage could be a possibility.

4. Market Manipulation via Load Altering Attacks

In this section, we now consider the feasibility of energy market manipulation from a more global perspective. In particular, we focus on analyzing how the effects caused by the LAA on the LMPs can propagate through the transmission system to neighboring distribution systems from the targeted distribution system(s). Specifically, we consider statistical variations of the LMPs obtained at the neighboring distribution systems, which are modeled using the same detailed phase unbalanced models discussed previously, to properly visualize the effects that the LAAs have in all nodes of the affected distribution systems.

4.1. Test Systems

The test case used in this section, shown in Figure 4 and modeled and solved using *PowerModelsITD.jl* [25], consists of the IEEE 24-bus RTS network (transmission) and 4 distribution feeders connected at buses #4, #5, #7, and #10. Connected at bus #4 is Feeder 3: R1-12.47-3 (cktr13), connected at bus #5 is Feeder 7: R2-12.47-2 (cktr22), connected at bus #7 is Feeder 15: R4-12.47-2 (cktr42), and connected at bus #10 is Feeder 17: R5-12.47-1 (cktr51), all developed by PNNL [31]. The total number of nodes and edges for the problem are 3921 and 4113, respectively.

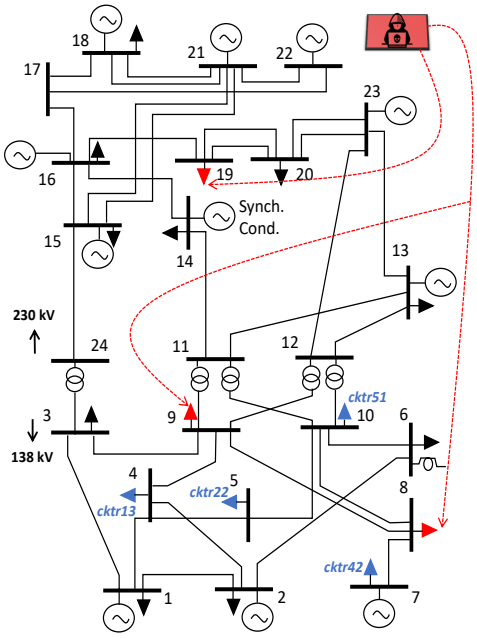

Figure 4. IEEE RTS 24-bus test system used for market manipulation feasibility studies. The 'blue' loads represent the loads that are replaced with the multi-conductor models for the cktr13, cktr22, cktr42, and cktr51 distribution systems. The 'red' loads represent the loads (distribution systems) that are targeted by LAAs.

4.2. Case Studies

We conduct case studies where load is (a) nominal, (b) 50% LAA-induced load increase, and (c) 100% LAA-induced load increase. No ES systems are considered, since the primary objective is to compare the LMPs between the different case studies and analyze the impact that load increases, at different load buses modeled in the transmission system (representing other distribution systems), have in the LMPs of the four analyzed distribution systems. The loads targeted by the 50% and 100% LAAs are located at buses #8, #9, and #19. The first two loads are in close proximity to the distribution systems, while bus #19 is the farthest.

4.3. Results

By statistically comparing the LMPs of the four modeled distribution systems based on load increases performed in adjacent buses, the feasibility of energy market manipulation is explored. Figure 5 presents box plots for the LMPs of each distribution system based on the load increase (e.g., 50% or 100%) in the respective compromised transmission system bus compared to the nominal case. A 50% load increase in bus #8 translates to a 85.5 MW increase, in bus #9 to a 87.5 MW increase, and in bus #19 to a 90.5 MW increase. Similarly, a 100% load increase in bus #8 translates to a 171 MW increase, in bus #9 to a 175 MW increase, and in bus #19 to a 181 MW increase. The cases where all three loads (i.e., #8, #9, and #19) are altered by 50% and 100% simultaneously yield a total load increase of approximately 263 and 527 MW, respectively. These amounts of load increase may seem too large to be considered 'stealthy' LAAs; however, based on the load forecasting error, an LAA that alters a maximum of 580 MW can still be considered as 'stealthy', e.g., in a large system such as the New York ISO (NYISO) [11]. Thus, massive botnet LAAs (∼200,000 bots) artificially producing these load variations could be realizable in a highly connected IoT power grid.

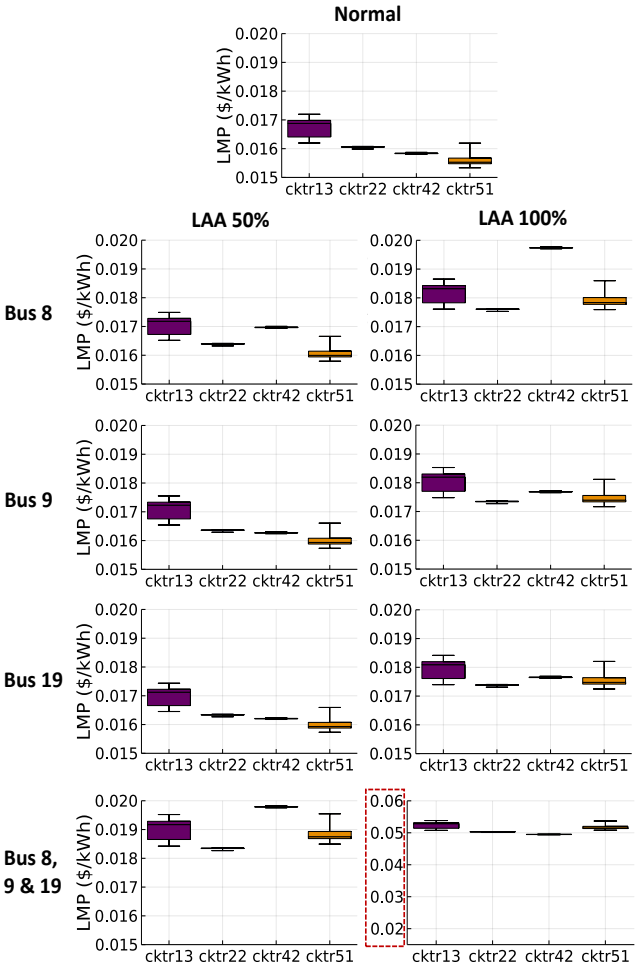

Figure 5. Box plots for LMPs in the distribution systems (i.e., cktr13, cktr22, cktr42, and cktr51). Rows indicate the bus targeted by the LAA, and columns represent the percent load increase at that bus (i.e., 50% or 100%). The red box indicates that in the last graph the *y*-limits are different, so that the corresponding LMP values could be visible.

Furthermore, as can be seen in Figure 5, LMPs can be significantly affected when specific buses are targeted, and by only targeting these three buses, using an LAA that increases load consumption by 100% in these three buses when compared to the *normal* scenario, an attacker is able to increase the LMPs for multiple distribution systems from

USD 0.016/kWh (USD 16/MWh) to around USD 0.055/kWh (USD 55/MWh). Another example showcasing the potential sensitivity of LMPs in a real-time energy market can be observed in the scenario where only bus #8 is targeted by an LAA that increases load by 100% at this bus. For this scenario, the LMPs of cktr42 increase from USD 0.016/kWh (USD 16/MWh) to around USD 0.0198/kWh (USD 19.8/MWh). These LMP variations may cause a variety of economic disruptions to both energy companies and customers, sometimes making energy approximately three times more expensive at specific periods (e.g., from USD 16/MWh to USD 55/MWh).

In terms of overall cost increase for energy companies, we observe a maximum total cost increase of approximately USD 16,831 when comparing the normal scenario against the 100% LAA in buses #8, #9, and #19. Figure 6 shows the OPF costs for all the cases evaluated, in which we can observe that the load increases can have a significant impact in the economic dispatch of energy suppliers and energy customers. In the near future, these LAA-induced load increases could become a reality due to the rapid deployment of electric vehicle (EV) charging and smart IoT devices.

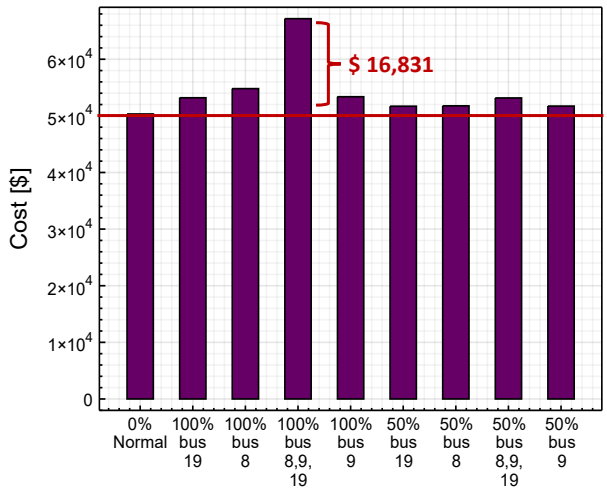

Figure 6. Optimal power flow (OPF) costs for the nine scenarios evaluated.

5. Conclusions

In this article, we have explored the feasibility of energy market manipulation and energy storage (ES) arbitrage via realistic load-altering attacks (LAAs) targeted at IoT high-wattage loads connected to the power grid infrastructure by modeling and describing a realistic LAA threat targeted at vulnerable HVAC system controllers capable of producing high-impact variations in the loading conditions of the analyzed power networks. Using integrated T&D system models of the power network, we have described in detail (1) the feasibility for an attacker gaining monetary benefits via LAA-assisted ES arbitrage, where high energy prices, based on locational marginal prices (LMPs), are artificially induced via stealthy and persistent LAAs, thus producing the perfect conditions for generating substantial monetary benefits from ES arbitrage, and (2) the feasibility for an attacker to manipulate the real-time energy market of a future power grid. The feasibility of market manipulation is explored using integrated T&D system models, allowing us to evaluate the impacts of LAAs on the economic operation of the entire power network.

We conclude that future transactive energy markets may be at risk from these types of threats; therefore, protection mechanisms against market manipulation strategies must be developed. Stakeholders and policy makers should take caution when defining pricing mechanisms and structures to avoid creating potential energy market manipulation conditions that threat actors could leverage to obtain monetary benefits. In addition, cybersecurity of high-wattage loads must be standardized and improved, and better LAA detection mechanisms must deployed to protect power grid infrastructure from attackers. To increase the realism of the LAA analysis, we believe that future work should also include the explicit modeling of

the communications/cyber layer, e.g., using a co-simulation framework that combines the T&D infrastructure with the communications/cyberinfrastructure.

Author Contributions: Conceptualization, J.O.; methodology, J.O.; software, J.O.; validation, J.O.; writing—original draft preparation, J.O. and D.M.F.; writing—review and editing, J.O., D.M.F., and R.B.; supervision, D.M.F. and R.B.; funding acquisition, D.M.F., and R.B. All authors have read and agreed to the published version of the manuscript.

Funding: This work was performed with the support of the U.S. Department of Energy (DOE) Office of Electricity (OE) Advanced Grid Modeling (AGM) Research Program under program manager Ali Ghassemian. The research work conducted at Los Alamos National Laboratory is done under the auspices of the National Nuclear Security Administration of the U.S. Department of Energy under Contract No. 89233218CNA000001.

Data Availability Statement: Not applicable.

Acknowledgments: We gratefully acknowledge Ali Ghassemian's support of this work.

Conflicts of Interest: The authors declare no conflict of interest.

Nomenclature

$\mathcal{T}$	Belongs to transmission network.
$\mathcal{D}$	Belongs to distribution network.
$\mathcal{B}$	Set of boundary buses.
Λ	Set of boundary links.
N	Set of buses.
G	Set of generators.
G_i	Generator at bus i.
$\Re$	Real part.
$\Im$	Imaginary part.
$\Phi = a, b, c$	Multi-conductor phases.
$\chi \rightarrow \mathcal{T}, \mathcal{D}$	Belongs to $\mathcal{T}$ or $\mathcal{D}$.
$\mathcal{C}$	Transmission gen. cost components.
$\mathfrak{C}$	Distribution gen. cost components.
$P_{d,i}^{\chi}$	Active power demand at bus i.
$Q_{d,i}^{\chi}$	Reactive power demand at bus i.
e^u	ES energy rating.
sc^u	ES charge rating.
sd^u	ES discharge rating.
η^c	ES charge efficiency.
η^d	ES discharge efficiency.
te	time elapsed.
S_{es}^l	ES power losses.
Z_{es}	ES injection impedance.
q_{es}^l, q_{es}^u	ES reactive power injection limits.
s_{es}^u	ES thermal limit.
i_{es}^u	ES current limit.
$P_{g,k}^{\mathcal{T}}$	Gen. k active power output.
$Q_{g,k}^{\mathcal{T}}$	Gen. k reactive power output.
$I_i^{\mathcal{T}}$	Complex current flowing out of bus i.
$V_i^{\mathcal{T}}$	Complex voltage at bus i.
$P_{g,m}^{\mathcal{D},\varphi}$	Gen. m active power output on phase φ.
$Q_{g,m}^{\mathcal{D},\varphi}$	Gen. m reactive power output on phase φ.
$I_i^{\mathcal{D},\varphi}$	Complex current flowing out of bus i phase φ.

$V_i^{\mathcal{D},\varphi}$	Complex voltage at bus i phase φ.
$e_t \in (0, e^u)$	Energy stored at time t.
$sc_t \in (0, sc^u)$	Charge power at time t.
$sd_t \in (0, sd^u)$	Discharge power at time t.
$sqc_t \in (0, sd^u)$	Reactive power slack at time t.
$S_{es,t}$	Complex bus power injection at time t.
$I_{es,t}$	Complex bus current injection at time t.

References

1. Riley, M. Bloomberg Businessweek Technology. What Happens When Russian Hackers Come for the Electrical Grid. Available online: https://www.bloomberg.com/news/features/2022-01-26/what-happens-when-russian-hackers-cyberattack-the-u-s-electric-power-grid (accessed on 19 May 2022).
2. Kovacs, E. SecurityWeek: Cybersecurity News, Insights & Analysis. High-Wattage IoT Botnets Can Manipulate Energy Market: Researchers. Available online: https://www.securityweek.com/high-wattage-iot-botnets-can-manipulate-energy-market-researchers (accessed on 19 May 2022).
3. Haskell, M.R.; McAllister, L. Policing Market Manipulation: A Review of Evolving Federal Energy Regulatory Commission Policy. *Electr. J.* **2011**, *24*, 34–43. [CrossRef]
4. Dvorkin, Y. IEEE Spectrum. Executive Order Shines a Light on Cyberattack Threat to the Power Grid. Available online: https://spectrum.ieee.org/executive-order-shines-a-light-on-cyberattack-threat-to-the-power-grid#toggle-gdpr (accessed on 19 May 2022).
5. Office of the Director of National Intelligence. Annual Threat Assessment of the US Intelligence Community. Available online: https://www.odni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf (accessed on 19 May 2022).
6. Grasso Macola, I. Power Technology. The Five Worst Cyberattacks against the Power Industry Since 2014. Available online: https://www.power-technology.com/analysis/the-five-worst-cyberattacks-against-the-power-industry-since2014/ (accessed on 19 May 2022).
7. Walton, R. Utility Dive Transmission & Distribution, Grid Security & Reliability. Sophisticated Hackers Could Crash the US Power Grid, but Money, Not Sabotage, Is Their Focus. Available online: https://www.utilitydive.com/news/sophisticated-hackers-could-crash-the-us-power-grid-but-money-not-sabotag/603764/ (accessed on 19 May 2022).
8. Michael Kerner, S. TechTarget. Colonial Pipeline Hack Explained: Everything You Need to Know. Available online: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know (accessed on 19 May 2022).
9. Klóters, J.; Neumann, C.; Hein, L.; Moser, A. Monitoring and Mitigation of Market Manipulation in Redispatch Markets. In Proceedings of the 2022 18th International Conference on the European Energy Market (EEM), Ljubljana, Slovenia, 13–15 September 2022; pp. 1–9. [CrossRef]
10. McLean, B.; Elkind, P. *The Smartest Guys in the Room: The Amazing Rise and Scandalous Fall of Enron*; Portfolio: A Member of Penguin Group: New York, NY, USA, 2013.
11. Shekari, T.; Irvene, C.; Cardenas, A.A.; Beyah, R. MaMIoT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets. In *CCS '21: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2021; pp. 1338–1356.
12. Yankson, S.; Ghamkhari, M. Transactive energy to guard against a zero-day load altering attack on power distribution systems. In Proceedings of the 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 12–14 August 2019; pp. 171–177.
13. Soltan, S.; Mittal, P.; Poor, H.V. BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; pp. 15–32.
14. Ospina, J.; Liu, X.; Konstantinou, C.; Dvorkin, Y. On the feasibility of load-changing attacks in power systems during the COVID-19 pandemic. *IEEE Access* **2020**, *9*, 2545–2563. [CrossRef]
15. Acharya, S.; Dvorkin, Y.; Karri, R. Public plug-in electric vehicles+ grid data: Is a new cyberattack vector viable? *IEEE Trans. Smart Grid* **2020**, *11*, 5099–5113.
16. Soltan, S.; Mittal, P.; Poor, H.V. Protecting the grid against MAD attacks. *IEEE Trans. Netw. Sci. Eng.* **2019**, *7*, 1310–1326. [CrossRef]
17. Yankson, S.; Ghamkhari, M. Transactive energy to thwart load altering attacks on power distribution systems. *Future Internet* **2019**, *12*, 4. [CrossRef]
18. Lakshminarayana, S.; Ospina, J.; Konstantinou, C. Load-Altering Attacks Against Power Grids under COVID-19 Low-Inertia Conditions. *IEEE Open Access J. Power Energy* **2022**, arXiv:2201.10505.
19. Amini, S.; Pasqualetti, F.; Mohsenian-Rad, H. Dynamic load altering attacks against power system stability: Attack models and protection schemes. *IEEE Trans. Smart Grid* **2016**, *9*, 2862–2872. [CrossRef]
20. Lakshminarayana, S.; Sthapit, S.; Maple, C. Data-Driven Detection and Identification of IoT-Enabled Load-Altering Attacks in Power Grids. *arXiv* **2021**, arXiv:2110.00667.
21. Germanà, R.; Giuseppi, A.; Di Giorgio, A. Ensuring the stability of power systems against dynamic load altering attacks: A robust control scheme using energy storage systems. In Proceedings of the 2020 European Control Conference (ECC), Saint Petersburg, Russia, 12–15 May 2020; pp. 1330–1335.

22. U.S. Energy Information Administration. How Much Electricity is Used for Cooling in the United States? Available online: https://www.eia.gov/tools/faqs/faq.php?id=1174&t=1 (accessed on 2 June 2022).
23. Marsh, R.; CNN. Energy Experts Sound Alarm about US Electric Grid: 'Not Designed to Withstand the Impacts of Climate Change'. Available online: https://www.cnn.com/2022/05/31/us/power-outages-electric-grid-climate-change/index.html (accessed on 2 June 2022).
24. Simonson, A.; Ward, T.; Paget, S.; Sanchez, R. CNN. Texans Asked to Turn Up Thermostats after Sweltering Heat Knocks Six Power Plants Offline. Available online: https://www.cnn.com/2022/05/14/us/texas-heat-wave-ercot-conserve/index.html. (accessed on 2 June 2022).
25. Ospina, J.; Fobes, D.M.; Bent, R.; Wächter, A. Modeling and Rapid Prototyping of Integrated Transmission-Distribution OPF Formulations with PowerModelsITD.jl. *IEEE Trans. Power Syst.* **2023**, 1–14. [CrossRef]
26. Yang, R.; Zhang, Y. Three-phase AC optimal power flow based distribution locational marginal price. In Proceedings of the 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 23–26 April 2017; pp. 1–5.
27. Liu, H.; Tesfatsion, L.; Chowdhury, A. Locational marginal pricing basics for restructured wholesale power markets. In Proceedings of the 2009 IEEE Power & Energy Society General Meeting, Calgary, AB, Canada, 26–30 July 2009; pp. 1–8.
28. Ospina, J.; Gupta, N.; Newaz, A.; Harper, M.; Faruque, M.O.; Collins, E.G.; Meeker, R.; Lofman, G. Sampling-based model predictive control of PV-integrated energy storage system considering power generation forecast and real-time price. *IEEE Power Energy Technol. Syst. J.* **2019**, *6*, 195–207. [CrossRef]
29. Coffrin, C.; Bent, R.; Sundar, K.; Ng, Y.; Lubin, M. PowerModels.jl: An open-source framework for exploring power flow formulations. In Proceedings of the 2018 Power Systems Computation Conference (PSCC), Dublin, Ireland, 11–15 June 2018; pp. 1–8.
30. Zografopoulos, I.; Ospina, J.; Liu, X.; Konstantinou, C. Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access* **2021**, *9*, 29775–29818. [CrossRef]
31. Schneider, K.P.; Chen, Y.; Chassin, D.P.; Pratt, R.G.; Engel, D.W.; Thompson, S.E. *Modern Grid Initiative Distribution Taxonomy Final Report*; Technical Report; Pacific Northwest National Lab. (PNNL): Richland, WA, USA, 2008.
32. Khan, M.A.; Hayes, B. A Reduced Electrically-Equivalent Model of the IEEE European Low Voltage Test Feeder. In Proceedings of the 2022 IEEE Power & Energy Society General Meeting (PESGM), Denver, CO, USA, 17–21 July 2022.
33. HOMER: Create a Synthetic Load from Profile. Available online: https://www.homerenergy.com/products/pro/docs/3.11/creating-a-synthetic-load-from-profile.html (accessed on 4 August 2022).
34. Qadrdan, M.; Jenkins, N.; Wu, J. Chapter II-3-D - Smart Grid and Energy Storage. In *McEvoy's Handbook of Photovoltaics*, 3rd ed.; Kalogirou, S.A., Ed.; Academic Press: Cambridge, MA, USA, 2018; pp. 915–928. [CrossRef]
35. Cole, W.; Frazier, A.W.; Augustine, C. *Cost Projections for Utility-Scale Battery Storage: 2021 Update*; Technical Report; National Renewable Energy Lab. (NREL): Golden, CO, USA, 2021.