future internet

MDPI

Article

Transactive Energy to Thwart Load Altering Attacks on Power Distribution Systems

Samuel Yankson and Mahdi Ghamkhari *

EECE Department, University of Louisiana at Lafayette, Lafayette, LA 70504, USA; samuel.yankson1@louisiana.edu

* Correspondence: mahdi.ghamkhari@louisiana.edu

Received: 1 October 2019; Accepted: 17 December 2019; Published: 24 December 2019

Abstract: The automatic generation control mechanism in power generators comes into operation whenever an over-supply or under-supply of energy occurs in the power grid. It has been shown that the automatic generation control mechanism is highly vulnerable to load altering attacks. In this type of attack, the power consumption of multiple electric loads in power distribution systems is remotely altered by cyber attackers in such a way that the automatic generation control mechanism is disrupted and is hindered from performing its pivotal role. The existing literature on load altering attacks has studied implementation, detection, and location identification of these attacks. However, no prior work has ever studied design of an attack-thwarting system that can counter load altering attacks, once they are detected in the power grid. This paper addresses the above shortcoming by proposing an attack-thwarting system for countering load altering attacks. The proposed system is based on provoking real-time adjustment in power consumption of the flexible loads in response to the frequency disturbances caused by the load altering attacks. To make the adjustments in-proportion to the frequency disturbances, the proposed attack-thwarting system uses a *transactive energy* framework to establish a coordination between the flexible loads and the power grid operator.

Keywords: load altering attacks; automatic generation control; frequency disturbances; transactive energy; attack thwarting system; cyber security; power distribution systems

1. Introduction

In recent years, Cyber security experts have repeatedly given warnings about major cyber attacks that could be launched against the U.S.'s power grid in the immediate future. Several factors give cause for the concern about the potency of such cyber attacks. Particularly, the widespread implementation of the smart grid and Internet-of-Thing technologies have increased the attack surface of the power grid [1]. Additionally, the emergence of malicious malware such as Triton have testified to the capability of cyber attackers for harming the power systems. Furthermore, recent cyber security studies have called into question the capability of U.S.'s power grid for withstanding a major cyber attack [2–4]. In response to the concerns outlined above, a large body of research work has focused on studying cyber attack detection and prevention in power grids [5–20].

The cyber attacks against a power grid can be categorized in different groups. For instance, one group of attacks aims to impair operation of the power grid by compromising the electricity price data [11,12], state estimation data [13,14], or smart meters' data [15,16]. Another group of attacks aim to infiltrate into the utilities' supervisory control and data acquisition (SCADA) system so as to harm the power grid by sending malicious commands to circuit breakers, reclosers, and switches ([17]; ([18], p. 11)). One more group of cyber attacks aims to put the power grid into abnormal operation by means of disrupting the automatic generation control mechanism in power

generators [5–10,19–22]. The cyber attacks in this last group are referred to as load altering attacks and are the focus of this paper.

To launch a load altering attack against a power grid, an adequate number of electric loads in power distribution systems should be compromised by cyber attackers. These electric loads should be remotely controllable so that they can be manipulated by cyber attackers. Once being compromised, the power consumption of the electric loads are remotely altered by cyber attackers in a way that, the automatic generation control mechanism in power generators is disrupted and is hindered from performing its pivotal role. As a result, the frequency disturbances in sinusoidal voltages cannot be corrected by the automatic generation control mechanism, and rather should be rectified by triggering emergency load curtailment ([23], p. 13) to avert the risk of a major blackout [24].

Most of the literature on load altering attacks are on the definition and implementation of these attacks [5,9,22], yet few prior works have studied the intrusion detection [6,10,21] or location identification [8] of these attacks. However, no prior work has ever studied design and implementation of an attack-thwarting system that can counter the load altering attacks. The attack-thwarting system forestalls the progress of the attack in harming stability and reliability of the power grid, without triggering the emergency load curtailment. To the best of our knowledge, this paper is the first that proposes an attack-thwarting system for guarding against load altering attacks.

Two points are noteworthy about the attack-thwarting systems. First, there is a clear difference between attack thwarting systems and intrusion-detection systems (IDSs). The later systems are preventative security measures that are set up in a power grid to detect cyber attacks by monitoring communication traffic and power consumption data [25]. In contrast, the former systems are set up in a power grid to invoke a response to cyber attacks, so as to halt an attack's progress in damaging the grid [25]. The latter systems are studied well in the literature of load altering attacks [6,7,10,20,21], but the former systems are not. Second, the attack-thwarting systems are an essential part of the new *defense-in-depth* strategy for the protection of cyber-physical systems [25,26]. In this new defense strategy, the physical system in a cyber-physical system should be protected even if the cyber system is intruded. This new strategy ensures that the physical system can continue performing correctly, even if the cyber system is disrupted by the cyber attackers [26].

The proposed attack-thwarting system in this paper is based on provoking real-time adjustment of a flexible loads' power consumption in response to the load altering attack. In fact, the proposed system enables energy exchanges between the power distribution systems and the flexible loads to counter the power imbalances caused by the load altering attack. Such energy exchanges should be carried out in real-time operation of the power grid in accordance with the fast timing of the load altering attack. Also, the energy exchanges should be in-proportion to the power imbalances caused by the load altering attack, so as to preclude exacerbation of frequency disturbances. To fulfill the above requirements, the energy exchanges in the proposed attack-thwarting system are framed in a *transactive energy* framework [27]. The emerging transactive energy framework enables real-time energy exchanges between power consumers and the power distribution systems.

The contributions of this paper to the field can be summarized as follows:

- An attack-thwarting system is proposed that can successfully counter load altering attacks on power distribution systems. The proposed attack-thwarting system uses energy exchanges between the power distribution systems and the flexible loads to counterbalance the harmful impact of the load altering attacks.
- The energy exchanges in the proposed attack-thwarting system are framed in a transactive energy framework, so as to fulfill the essential requirements in thwarting the load altering attacks.
- The performance of the proposed attack-thwarting system is assessed by conducting numerical simulations on IEEE standard 33-bus power distribution system. It is shown that the proposed attack-thwarting system can successfully forestall progress of a load altering attack without triggering emergency load curtailment.

The rest of this paper is organized as follows: Power balancing in power grids is discussed in Section 2. The automatic generation control mechanism in power generators is explained in Section 3. The load altering attacks are reviewed in Section 4. The proposed attack-thwarting system is introduced in Section 5. Numerical simulations are provided in Section 6. Finally, the paper is concluded in Section 7.

2. Power Balancing in Power Grids

Reliable operation of a power grid relies heavily on maintenance of a balance between power generation and power consumption in the grid. In a general sense, a power imbalance can disrupt the normal operation of a power grid; e.g., by damaging power generators ([23], p. 13), triggering reaction of transformer relays [28], triggering curtailment of electric loads [29], or causing blackouts in the power grid [24]. To avert the above harmful consequences of power imbalances, two main mechanisms are incorporated in the operation of the power grid to maintain the required balance between power generation and power consumption: 1—energy trading in wholesale electricity markets [30]; and 2—employing reserve generation [31]. This section briefly explains these two mechanisms.

2.1. Energy Trading in Wholesale Electricity Markets

In regions with deregulated electricity markets, a wholesale market runs every 5 min [32,33] to enable energy trading between bulk power generators and energy utilities. In offering energy to the wholesale market, a bulk power generator submits a cost function to the market specifying the amount of money that must be paid to the generator as a function of the generator's power generation. On the other hand, an energy utility specifies the amount of power that it needs to operate its power distribution system. The independent system operator of the power grid collects all the energy bids from the generators and energy utilities and clears the market by calculating the lowest-cost power dispatch in meeting energy demands of the utilities [34].

2.2. Correcting Power Imbalances by Means of Reserve Power

In purchasing energy from wholesale market, an energy utility should forecast the power consumption of its power distribution system 5 min in advance of the operating time of the power grid. However, load forecasting methods [35] utilized by energy utilities are not perfect and come with limited accuracies. Accordingly, the real time power consumption of the distribution system may fluctuate and deviate from the power consumption scheduled in the wholesale market. The resulting imbalance between power generation and power consumption are compensated for by the reaction of generators that provide reserve power to the power grid. In correcting power imbalances, a mechanism known as automatic generation control comes into operation in these generators. The automatic generation control mechanism is discussed in the next section.

3. Automatic Generation Control

The automatic generation control mechanism is based on this key feature of the alternative current (AC) power grids—that the voltages of all buses follow sinusoidal waveforms. Namely, a power imbalance in AC power grids impacts the frequency of sinusoidal voltages throughout the power grid. For instance, an imbalance between power generation and power consumption in a power distribution system impacts the frequency of sinusoidal voltages not only in the power distribution system, but also in all other parts of the power grid. The generators sense and measure the changes in the frequency of sinusoidal voltages and react to them. In a case where the power distribution system encounters an over-supply of energy, the frequency of the sinusoidal voltages leaps from the rated frequency of 60 Hz. The generators observe the surge in the frequency of sinusoidal voltages and react to it by reducing their power injection into the power grid. Similarly, in a case where the power distribution system encounters an under-supply of energy, the frequency of the sinusoidal voltages

drops below the rated frequency of 60 Hz. The generators observe the frequency drop and react to it by increasing their power injection to the power grid.

3.1. Automatic Generation Control in the Frequency-Domain

In a power grid, several generators may provide reserve generation to the grid. However, for simplifying the proposed analysis we consider a case where only one generator provides reserve generation to the grid. This generator reacts to the changes in the frequency of the sinusoidal voltages Δf by making a change ΔP_t in the power injection of the generator into the power grid. The amount of change ΔP_t in the power injection of the reserve generator depends on the amount of change in the frequency Δf and several design parameters; e.g., the generator's governor speed regulator R, secondary loop gain K_i, angular momentum M, damping constant D, time constant T_g, and turbine time constant T_t. This dependency can be seen from Figure 1 which shows a block diagram of the automatic generation control in the complex frequency domain [36,37].

In the block diagram of Figure 1, the relationship between frequency of the sinusoidal voltages and the response of the generator is represented in complex frequency domain s. Although the frequency domain representation of a feedback control system facilitates the design and analysis of the system, the focus of this paper is on the time-domain characteristics of the automatic generation control. Therefore, in the next section the frequency-domain representation of the automatic generation control is transformed to a time-domain representation.

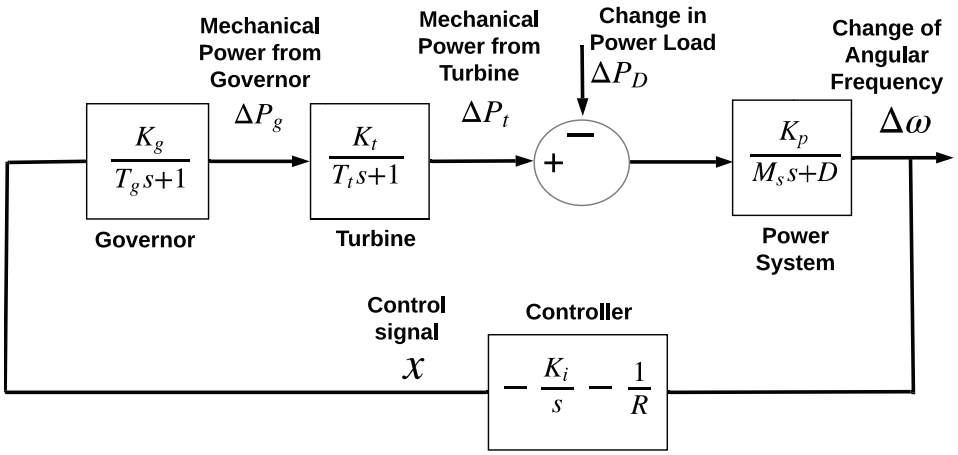

Figure 1. The representation of automatic generation control in complex frequency domain [36,37].

3.2. Automatic Generation Control in the Time-Domain

For deriving the time-domain representation of the block diagram in Figure 1, a time domain relation between input and output variables of each block should be obtained. Toward this end, we consider the specific block with input and output variables ΔP_g and ΔP_t, respectively. This specific block establishes the following relation between the variables ΔP_g and ΔP_t in frequency domain:

$$\Delta P_t(s) = \frac{K_t}{T_t s + 1} \Delta P_g(s), \tag{1}$$

where s is the complex-frequency variable. From (1), one can find the following time-domain relation between $\Delta P_g(t)$ and $\Delta P_t(t)$:

$$\Delta P_t'(t) = -\frac{\Delta P_t(t)}{T_t} + \frac{K_t}{T_t} \Delta P_g(t). \tag{2}$$

In a similar way to the above approach, the frequency-domain relations between input and output variables of all the blocks in Figure 1 can be translated to time-domain relations:

$$\begin{aligned}
\Delta\omega'(t) &= -\frac{D}{M}\Delta\omega(t) + \frac{K_p}{M}\left(\Delta P_t(t) - \Delta P_D\right) \\
\Delta P_g'(t) &= -\frac{\Delta P_g(t)}{T_g} + \frac{K_g}{T_g}x(t) \\
x'(t) &= \left(\frac{D}{MR} - K_i\right)\Delta\omega - \frac{K_p}{MR}\Delta P_t(t) + \frac{K_p}{MR}\Delta P_D,
\end{aligned} \tag{3}$$

where ΔP_D denotes the change in power consumption of the power grid. The Equations (2) and (3) can be summarized in the following matrix form:

$$\begin{bmatrix} \Delta\omega'(t) \\ \Delta P_t'(t) \\ \Delta P_g'(t) \\ x'(t) \end{bmatrix} = \begin{bmatrix} \frac{-D}{M} & \frac{K_p}{M} & 0 & 0 \\ 0 & \frac{-1}{T_t} & \frac{K_t}{T_t} & 0 \\ 0 & 0 & \frac{-1}{T_g} & \frac{K_g}{T_g} \\ \frac{D-MRK_i}{MR} & \frac{-K_p}{MR} & 0 & 0 \end{bmatrix} \begin{bmatrix} \Delta\omega(t) \\ \Delta P_t(t) \\ \Delta P_g(t) \\ x(t) \end{bmatrix} + \begin{bmatrix} \frac{-K_p}{M} \\ 0 \\ 0 \\ \frac{K_p}{MR} \end{bmatrix} \Delta P_D. \tag{4}$$

The Equation (4) is the time-domain representation of the automatic generation control. This equation is also referred to as the state-space representation ([38], p. 24) of the block diagram of Figure 1.

In this paper, the Equation (4) is used to simulate the response of a generator to a change in power consumption of the power grid ΔP_D. More precisely, the state of the variables $\Delta\omega$, ΔP_t ΔP_g, and x is updated in time intervals of length $\tau = 0.01$ seconds as follows:

$$\begin{bmatrix} \Delta\omega(t+\tau) \\ \Delta P_t(t+\tau) \\ \Delta P_g(t+\tau) \\ x(t+\tau) \end{bmatrix} = \begin{bmatrix} \Delta\omega(t) \\ \Delta P_t(t) \\ \Delta P_g(t) \\ x(t) \end{bmatrix} + \begin{bmatrix} \Delta\omega' \\ \Delta P_t'(t) \\ \Delta P_g'(t) \\ x'(t) \end{bmatrix} \tau, \tag{5}$$

where the derivatives of the variables $\Delta\omega$, ΔP_t ΔP_g, and x are calculated from the Equation (4).

We note that Δ and ω in Equations (4) and (5) are the changes in angular frequency of the sinusoidal voltages. Accordingly, the change in frequency of sinusoidal voltages is obtained as follows:

$$\Delta f = \Delta\omega/2\pi. \tag{6}$$

Figure 2 shows the change in frequency of sinusoidal voltages Δf in an exemplary power grid, succeeding a surge in power consumption of the grid. From Figure 2, the frequency of sinusoidal voltages drops below the rated frequency of 60 Hz subsequent to the increase in power consumption of the power grid. The frequency is eventually reverted back to the rated frequency by means of the automatic generation control mechanism.

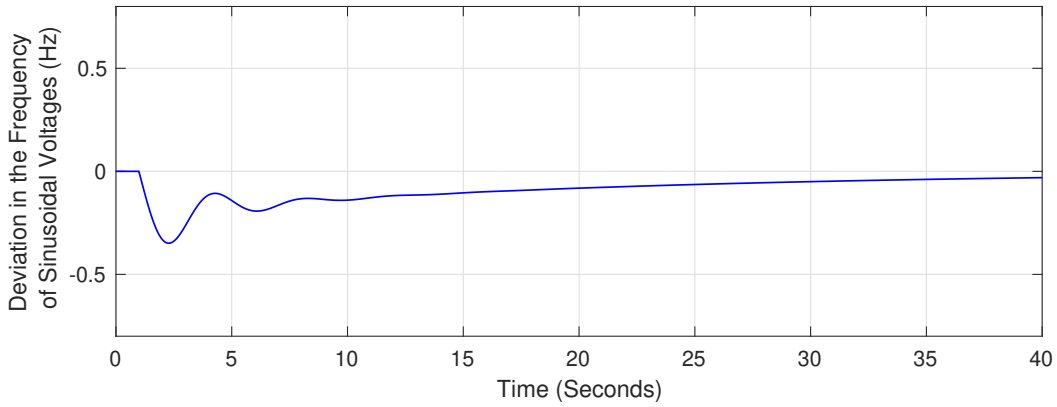

Figure 2. The deviation in frequency of sinusoidal voltages in a power grid, succeeding an increase in the power consumption of the grid and the corresponding response of the automatic generation control mechanism.

4. Load Altering Attacks on Power Grids

This section reviews the load altering attacks against automatic generation control mechanism.

4.1. The Safe Range for the Frequency of Sinusoidal Voltages

The rated frequency of sinusoidal voltages in the U.S. is 60 Hz. However, the frequency of sinusoidal voltages may deviate from this rated frequency in real time operation of the power grid. Such frequency deviations occur quite often in the power grid and stem from the intermittency in the power consumption of the distribution systems. Nevertheless, for securing reliable operation of the grid, it is of paramount importance to confine the frequency of sinusoidal voltages to the following safe range around the rated frequency [39]:

$$59.5 \leq f \leq 60.5. \tag{7}$$

In fact, for preventing damage to generators, the generators are usually configured to disconnect from the grid once the frequency of sinusoidal voltages falls outside of the safe range given in (7), [23] (p. 13), and [40,41]. Therefore, in order to avert disconnection of power generators from the power grid and a subsequent widespread blackout ([23] (Section 2.1)), the constraint in (7) should be maintained at all times.

In normal operation of the power grid, the frequency deviations are quickly corrected by the reaction of the reserve generators through the automatic generation control mechanism. As a result, the frequency of sinusoidal voltages may rarely fall outside of the safe range given in (7). Still, the frequency of sinusoidal voltages can be easily dragged outside of the safe range in (7) by virtue of a load altering attack. Such an attack is mounted on the power grid to break the automatic generation control mechanism and put the stability of the grid in jeopardy. The load altering attacks are explained in the next Section.

4.2. Timeline of a Load Altering Attack

Consider a power grid that is made up of several power distribution systems and a power generator. We assume that an adequate number of electric loads in the distribution systems are compromised by cyber attackers and can be controlled remotely for malicious purposes. The validity of such assumption will be assessed in Section 4.3 by providing discussion about recent cyber attacks. Nevertheless, once being compromised, the electric loads can be used in a load altering attack against the power grid. In this type of attack, the power consumption of the compromised loads are changed in a way that the automatic generation control mechanism breaks and malfunctions. As a result,

the automatic generation control mechanism exacerbates frequency disturbances in the power grid instead of correcting the disturbances. Such frequency disturbances make power generators disconnect from the power grid, thereby causing widespread blackouts.

4.3. Compromise of Controllable Loads in Distribution Systems

For mounting a load altering attack, cyber attackers need to gain control over an adequate number of electric loads in power distribution systems. The compromised loads should be remotely controllable so that their power consumptions can be altered by cyber attackers remotely. Electric vehicles [42], computer servers ([43], page 27; [44]), and energy storage units [22] are among the electric loads that can be used in forming a load altering attack. In fact, the quick response of these electric loads to control commands and their large power consumptions facilitate implementation of a load altering attack.

From the above discussion, the feasibility of a load altering attack can be provn by demonstrating the feasibility of compromising electric loads on a large scale. Sorely, the wide spread of malicious malware such as WanaCry and Petya attest to the viability of large scale compromise of electric loads [45]. Particularly, the WanaCry malware that rose in 2017 could infect more that 230,000 computers within a year from its initial appearance [45]. Although the WanaCry malware is a ransomware which cannot alter power consumption of its targets, the malware still testifies to the fact that similar malware with a power-altering capability could be designed and spread by cyber attackers.

5. Guarding against Load Altering Attacks

The recently adopted reliability standard PRC-024-1 mandates that a generator's protective relays should tolerate frequency disturbances that fall within the interval of (7). According to the same reliability standard, the protective relays can disconnect the generators from the grid whenever the frequency stays out of the interval in (7) for a specific minimum duration. In such cases, the power system operator must resort to emergency actions to bring the frequency back to the safe interval in (7) and prevent disconnection of generators and a subsequent blackout. For instance, when the frequency falls below 59.5 Hz, as a last resort the power system operator must trigger the under-frequency load shedding (UFLS) and curtail the total power consumption in the power grid ([23], p. 13). Although the emergency load curtailment is effective at correcting the frequency disturbances, it causes a large number of electric loads to suffer a disruption in their power supply.

Instead of resorting to the emergency load curtailment, the frequency disturbances can be corrected by the reaction of electric loads with flexible power consumption. In this approach, a group of flexible loads respond to the frequency disturbances long before the power grid reaches a point where emergency load curtailment becomes inevitable. This approach and its role in thwarting load altering attacks are discussed in the next section.

5.1. Transactive Energy to Guard against Load Altering Attacks

The flexibility of the flexible loads in a power grid can be utilized to thwart a load altering attack on the power distribution system. Toward this end, the power consumption of the flexible loads should be reduced when the frequency of sinusoidal voltages drops below the rated frequency of 60 Hz. Similarly, the power consumption of the flexible loads should increase when the frequency of sinusoidal voltages surges above the rated frequency of 60 Hz. The adjustments in power consumption of the flexible loads should be made in such a way that, the responses to the frequency disturbances stay in-proportion to the frequency disturbances. Otherwise, the adjustment in power consumption of the flexible loads may transform an over-supply of energy to an under-supply of energy, and vice versa. Therefore, when reacting to the frequency disturbances there is a need for coordination between flexible loads and the power system operator.

To ensure such coordination, the power system operator should be able to notify the flexible loads about the required adjustment in power consumption of the distribution system. The flexible loads also should be able to indicate their willingness to adjust their power consumption. Once these information are collected, an adequate number of flexible loads among all the available flexible loads should be selected to perform the adjustments in their power consumption. Finally, the above process should be repeated on a moment-to-moment basis, so as to allow update of stakeholders' responses to moment-to-moment changes in voltages' frequencies. Fortunately, all the above prerequisites for ensuring the coordination between stakeholders are accessible in a transactive energy framework.

In the transactive energy framework, an electricity market runs in the power distribution system and enables real time and peer-to-peer energy exchanges between the power consumers and the power system operator [27]. By deploying the transactive energy framework, the power system operator can purchase energy from power consumers when the frequency of sinusoidal voltages drops below the rated frequency. Similarly, the power system operator can sell energy to the power consumers when the frequency of sinusoidal voltages surges above the rated frequency. The transactive energy framework is precisely explained in [27,46]. The next section provides a brief summary of the discussion in [27,46] as is pertinent to this paper.

5.2. Transactive Energy Framework

To enable the real time power exchanges between the the flexible loads and the power distribution system, the operation of the distribution system is divided into successive time intervals of *short* length T; e.g., $T = 10$ milliseconds. Each time interval is referred to as a *transaction cycle*. At the beginning of a transaction cycle, power consumers indicate their energy demands or their energy offers by submitting price bids to the distribution market. A flexible load that can increase its power consumption submits a negative price bid to indicates its willingness for purchasing energy. The absolute value of this price bid reflects the highest rate at which the power consumer is still willing to pay for energy. On the other hand, a flexible load that can reduce its power consumption submits a positive price bid to the market to indicates an energy offer. This price bid reflects the least rate at which the flexible load expects to receive payment for its energy offer to the market.

In each transaction cycle, the power market operator collects all the price bids and clears the market by solving a linear optimization problem that maximizes the social welfare [46]:

$$\text{Social Welfare} = \sum_{k=1}^{N} -|\text{Bid}_k|\,\Delta P_k, \tag{8}$$

where Bid_k is the price bid submitted to the distribution market by the power consumer at bus k. Also, ΔP_k is the amount of energy exchange at bus k, expressed in terms of additional power injection to bus k. Once the market is cleared, the dispatch instructions are sent to the flexible loads. Since each transaction cycle has a short duration T, the maximum energy that a power consumer can sell or purchase in a transaction cycle is upper bounded by $P_{max}T$, where $P_{max} = 0.01$ Mega-Watts. Such an upper bound on the energy purchases ensures that the power consumers can follow the dispatch instructions before the start time of the next transaction cycle.

We note that, in clearing the distribution market the power system operator considers the physical constraints in the operation of the distribution system, including the limited capacity of the distribution lines and the safe range of voltage magnitudes. As a result, power flow equations are included in the social maximization problem that is solved in the distribution market; see [27]. However, since the energy transactions in each transaction cycle are small amounts upper bounded by $P_{max}T$ the nonlinear power flow equations are *accurately* approximated by the following linear differential power flow equation [46]:

$$\Delta P_k = \sum_{i=1}^{N} \frac{\partial P_k}{\partial V_i}\Delta V_i + \frac{\partial P_k}{\partial \theta_i}\Delta\theta_i. \tag{9}$$

6. Case Studies

In this section, the effectiveness of the proposed attack-thwarting system in countering a load altering attack is assessed through numerical simulations.

6.1. Simulation Setup

We consider a simple power grid that is made up of a power generator rated at 300 MW and 77 power distribution systems. The electric loads and the electric networks of all the power distribution systems are set according to the IEEE 33-bus power system. The aforementioned power generator supplies energy to all the 77 power distribution systems. Since the rated power consumption of each power distribution system is 3.9 MW, a total number of 77 power distribution systems are incorporated in the simulations to draw power from the generator at its rated power output; i.e., $77 \times 3.9 \cong 300$. For reducing the computation burden in the simulations, all the power distribution systems are configured identically. For instance, the locations of compromised loads in all the power distribution systems are the buses 11, 12, 13, 14, 16, 18, 20, 21, and 24. Also, the locations of flexible loads in all the power distribution systems are 5, 10, 19, 32, 7, 33, 17, 27, and 15. Furthermore, the power generator is equipped with automatic generation control and provides reserve generation to the power distribution systems. The parameters of the generator and the automatic generation control are as follows: $R = 0.05$, $Ki = 1$, $M = 10$, $D = 0.9$, $Tg = 0.25$, $Tt = 0.6$, $Kp = 1$, $Kg = 1$, and $Kt = 1$; see Figure 1 and [41].

6.2. A Power Grid with No Attack-Thwarting System

Consider a scenario where the power grid described in Section 6.1 is initially operating normally, until a load altering attack is carried out against the power grid. The power grid is lacking any attack-thwarting system and is vulnerable to the cyber attack. Figure 3a shows the total power consumption of the compromised loads in the power distribution systems. Since the power grid is lacking any attack-thwarting system, the attack succeeds at making severe frequency disturbances. Figure 3b shows the frequency of sinusoidal voltages in the power grid under the attack conditions. From Figure 3b, in a short time after the start of the attack, the magnitude of frequency fluctuation becomes large enough to cause violation of the constraint in (7) and trigger emergency load curtailment.

6.3. A Power Grid with the Proposed Attack-Thwarting System

Consider a scenario where the power grid described in Section 6.1 is equipped with the attack-thwarting system proposed in Section 5.1. Figure 4a shows the total power consumption of the compromised loads in the power distribution systems. Also, Figure 4b shows the frequency of sinusoidal voltages in the power grid under the attack condition. From Figure 4b, the proposed attack-thwarting system is effective at constraining the frequency of sinusoidal voltages to the safe range given in (7), thereby countering the load altering attack. From the above discussion, when the attack-thwarting system is in operation, the load altering attack cannot steer the operation of the power grid to a point where the emergency load curtailment becomes unavoidable.

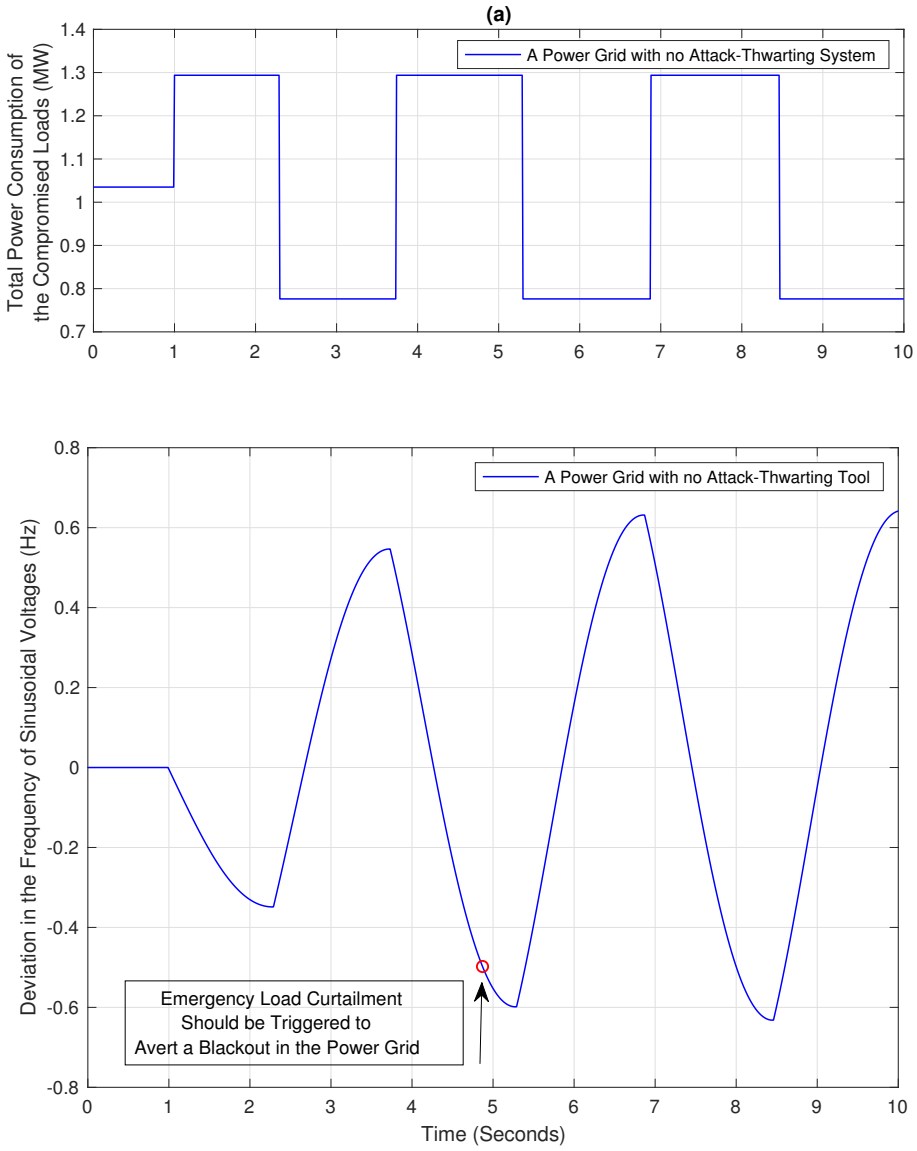

Figure 3. The impact of a Load Altering Attack on a power grid with no attack-thwarting system (**a**) Total power consumption of the compromised loads (**b**) The deviation in frequency of sinusoidal voltages in the power grid.

6.4. Increasing the Safety Margin in Thwarting the Attacks

As it was discussed in Section 4.1, maintaining the frequency of sinusoidal voltages in the interval of (7) secures the reliable operation of the power grid. However, when a load altering attack is detected in a power grid, restricting the frequency of sinusoidal voltages in a closer proximity to rated frequency allows a safety margin to preclude emergency load curtailment. Fortunately, in the proposed attack-thwarting framework the proximity of voltages' frequency to the rated frequency is adjustable. The adjustment is carried out by means of altering the rate of energy exchanges between the power system operator and the flexible loads. Namely, when the frequency of sinusoidal voltages is declining, the pace of frequency drop can be reduced by increasing the rate of energy purchase from the flexible loads. Similarly, when the frequency of sinusoidal voltages is surging, the pace of frequency surge can be reduced by increasing the rate of energy sale to the flexible loads.

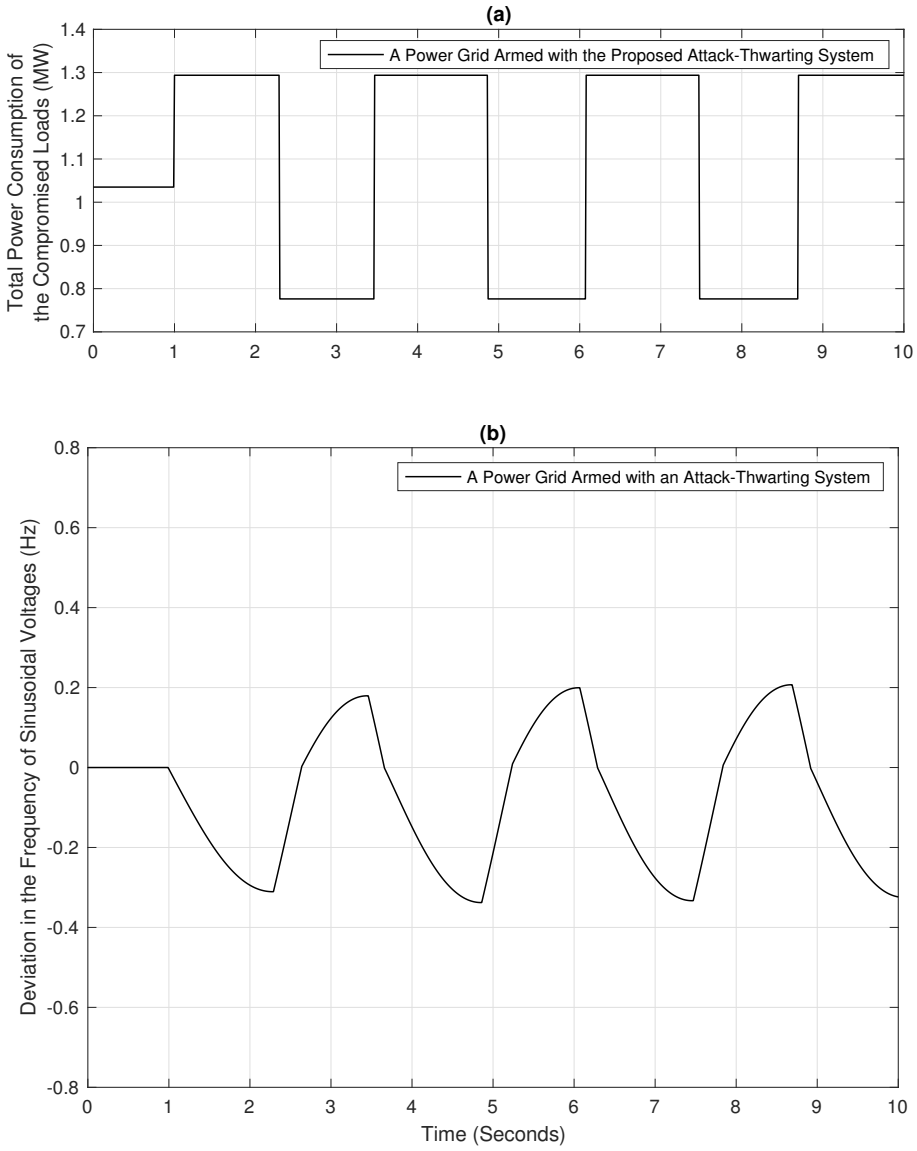

Figure 4. The impact of a Load Altering Attack on a power grid armed with the proposed attack-thwarting system: (**a**) Total power consumption of the compromised loads (**b**) The deviation in frequency of sinusoidal voltages in the power grid.

We note that the energy exchanges in the transactive energy framework are conducted in successive transaction cycles that come one after the other [27]. The amount of energy exchanges in each transaction cycle is upper bounded by a certain fixed amount. Therefore, for altering the rate of energy exchanges in the transactive energy framework the rate of transaction cycles should be modified. Figure 5 shows the frequency of sinusoidal voltages under the attack scenario of Section 6.3 in five different cases. In these cases, the rates of energy transactions in the transactive energy framework are 100, 200, 300, 400, and 500 transaction cycles per second. From Figure 5, increasing the rate of transaction cycle increases the proximity of the voltages' frequency to the rated frequency of 60 Hz.

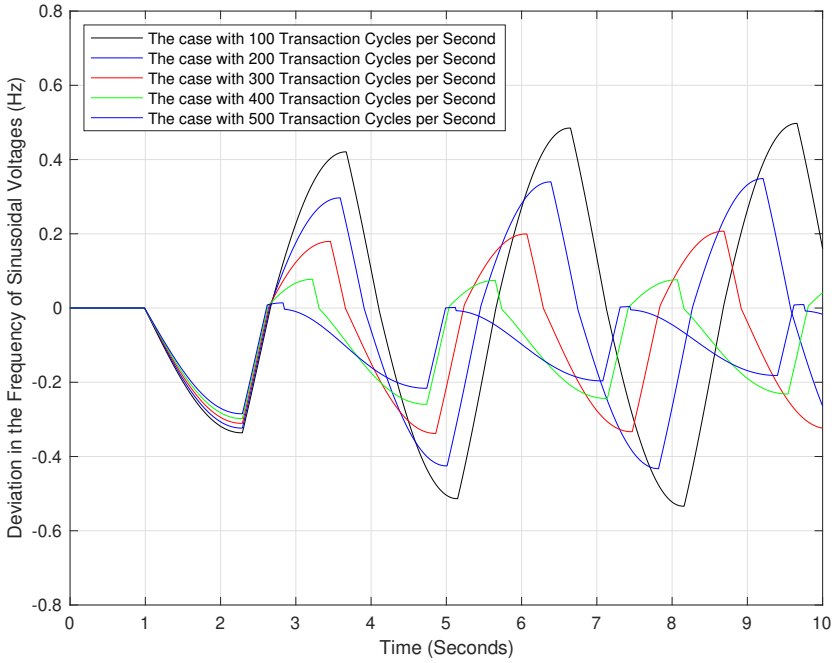

Figure 5. The impact of the rate of power exchanges between the power grid operator and the flexible loads, on the frequency of sinusoidal voltages.

7. Conclusions

In this paper, an attack-thwarting system was proposed that can halt the progress of load altering attacks in harming power grids. The proposed system provokes adjustment in power consumption of the flexible loads to correct frequency disturbances that are caused by the cyber attacks. It was shown that, by employing the proposed system, the frequency of sinusoidal voltages is maintained within a safe range even if a load altering attack is ongoing in the power grid. It was discussed that for thwarting an attack, there is a need for real-time energy exchanges between the flexible loads and the power distribution systems. Furthermore, it was argued that the energy exchanges should be in-proportion to the frequency disturbances that are caused by the attack. To fulfill the above requirements, a transactive energy framework was deployed in the proposed attack-thwarting system. Through the numerical simulations on an IEEE standard 33-bus system, it was shown that the proposed system is effective at thwarting the load altering attacks.

Author Contributions: Investigation, M.G. and S.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Hassanzadeh, A.; Modi, S.; Mulchandani, S. Towards effective security control assignment in the Industrial Internet of Things. In Proceedings of the IEEE World Forum on Internet of Things, Milan, Italy, 14–16 December 2015.
2. Yang, Y.; Nishikawa, T.; Motter, A.E. Small vulnerable sets determine large network cascades in power grids. *Science* **2017**, *358*, eaan3184. [CrossRef]
3. Athari, M.H.; Wang, Z. Impacts of wind power uncertainty on grid vulnerability to cascading overload failures. *IEEE Trans. Sustain. Energy* **2017**, *9*, 128–137. [CrossRef]

4. Sullivan, J.E.; Kamensky, D. How cyber-attacks in Ukraine show the vulnerability of the US power grid. *Electr. J.* **2017**, *30*, 30–35. [CrossRef]
5. Amini, S.; Pasqualetti, F.; Mohsenian-Rad, H. Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes. *IEEE Trans. Smart Grid* **2018**, *9*, 2862–2872. [CrossRef]
6. Amini, S.; Pasqualetti, F.; Abbaszadeh, M.; Mohsenian-Rad, H. Hierarchical Location Identification of Destabilizing Faults and Attacks in Power Systems: A Frequency-Domain Approach. *IEEE Trans. Smart Grid* **2019**, *10*, 2036–2045. [CrossRef]
7. Amini, S.; Pasqualetti, F.; Mohsenian-Rad, H. Detecting dynamic load altering attacks: A data-driven time-frequency analysis. In Proceedings of the International Conference on Smart Grid Communications, Miami, FL, USA, 2–5 November 2015.
8. Izbicki, M.; Amini, S.; Shelton, C.R.; Mohsenian-Rad, H. Identification of destabilizing attacks in power systems. In Proceedings of the American Control Conference, Seattle, WA, USA, 24–26 May 2017.
9. Li, X.; Liang, X.; Lu, R.; Shen, X.; Lin, X.; Zhu, H. Securing smart grid: cyber attacks, countermeasures, and challenges. *IEEE Commun. Mag.* **2012**, *50*, 38–45. [CrossRef]
10. Pasqualetti, F.; Dörfler, F.; Bullo, F. Cyber-physical security via geometric control: Distributed monitoring and malicious attacks. In Proceedings of the IEEE Conference on Decision and Control, Maui, HI, USA, 10–13 December 2012.
11. Esmalifalak, M.; Shi, G.; Han, Z.; Song, L. Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study. *IEEE Trans. Smart Grid* **2013**, *4*, 160–169. [CrossRef]
12. Xie, L.; Mo, Y.; Sinopoli, B. False data injection attacks in electricity markets. In Proceedings of the IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010.
13. Liu, Y.; Ning, P.; Reiter, M. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*, 1–33. [CrossRef]
14. Kosut, O.; Jia, L.; Thomas, R.J.; Tong, L. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In Proceedings of the IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010.
15. Pandey, R.K.; Misra, M. Cyber security threats—Smart grid infrastructure. In Proceedings of the National Power Systems Conference, Bhubaneswar, India, 19–21 December 2016.
16. Xiao, Z.; Xiao, Y.; Du, D.H.C. Exploring malicious meter inspection in neighborhood area smart grids. *IEEE Trans. Smart Grid* **2012**, *4*, 214–226. [CrossRef]
17. Oman, P.; Schweitzer, E.O.; Frincke, D. Concerns About Intrusions Into Remotely Accessible Substation Controllers And SCADA Systems. In Proceedings of the 27th Annual Conference for Protective Relay Engineers, Spokane, WA, USA, 23–26 October 2000.
18. Mission Support Center. *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*; Idaho National Laboratory: Idaho Falls, ID, USA, 2016.
19. Sargolzaei, A.; Yen, K.K.; Abdelghani, M.N. Preventing Time-Delay Switch Attack on Load Frequency Control in Distributed Power Systems. *IEEE Trans. Smart Grid* **2016**, *7*, 1176–1185. [CrossRef]
20. Lin, H.; Slagell, A.; Kalbarczyk, Z.T.; Sauer, P.W.; Iyer, R.K. Runtime Semantic Security Analysis to Detect and Mitigate Control-Related Attacks in Power Grids. *IEEE Trans. Smart Grid* **2018**, *9*, 163–178. [CrossRef]
21. Marnerides, A.K.; Smith, P.; Schaeffer-Filho, A.; Mauthe, A. Power Consumption Profiling Using Energy Time-Frequency Distributions in Smart Grids. *IEEE Commun. Lett.* **2015**, *19*, 46–49. [CrossRef]
22. Mohsenian-Rad, A.; Leon-Garcia, A. Distributed Internet-Based Load Altering Attacks Against Smart Power Grids. *IEEE Trans. Smart Grid* **2011**, *2*, 667–674. [CrossRef]
23. Eto, J.H.; Undrill, J.; Roberts, C.; Mackin, P.; Ellis, J. *Frequency Control Requirements for Reliable Interconnection Frequency Response*; FERC: Washington, DC, USA, 2018.
24. Kerdphol, T.; Rahman, F.S.; Watanabe, M.; Mitani, Y.; Turschner, D.; Beck, H. Extended Virtual Inertia Control Design for Power System Frequency Regulation. In Proceedings of the IEEE PES GTD Grand International Conference and Exposition Asia, Bangkok, Thailand, 19–23 March 2019.
25. Kent, S. On the trail of intrusions into information systems. *IEEE Spectr.* **2000**, *37*, 52–56. [CrossRef]
26. Li, Z.; Shahidehpour, M.; Aminifar, F. Cybersecurity in Distributed Power Systems. *Proc. IEEE* **2017**, *105*, 1367–1388. [CrossRef]
27. Ghamkhari, M. Transactive Energy Pricing in Power Distribution Systems. In Proceedings of the IEEE Green Technologies Conference, Lafayette, LA, USA, 3–6 April 2019.

28. Nimkar, P.R.; Arora, T.G.; Bangde, P.S.; Narnaware, P.J. Over-Flux Protection of The Transformer. In Proceedings of the International Conference on Smart Electric Drives and Power System, Maharashtra, India, 12–13 July 2018.
29. Papangelis, L.; Debry, M.S.; Prevost, T.; Panciatici, P.; Cutsem, T.V. Decentralized model predictive control of voltage source converters for AC frequency containment. *Int. J. Electr. Power Energy Syst.* **2018**, *98*, 342–349. [CrossRef]
30. Cramton, P. Electricity market design. *Oxf. Rev. Econ. Policy* **2017**, *33*, 589–612. [CrossRef]
31. Bakken, B.H.; Grande, O.S. Automatic generation control in a deregulated power system. *IEEE Trans. Power Syst.* **1998**, *13*, 1401–1406. [CrossRef]
32. Yoon, J.H.; Baldick, R.; Novoselac, A. Dynamic demand response controller based on real-time retail price for residential buildings. *IEEE Trans. Smart Grid* **2014**, *5*, 121–129. [CrossRef]
33. Kranz, B.; Pike, R.; Hirst, E. Integrated Electricity Markets in New York: Day-ahead and Real-time Markets for Energy, Ancillary Services, and Transmission. *Electr. J.* **2002**, *16*, 54–65. [CrossRef]
34. Litvinov, E. Design and operation of the locational marginal prices-based electricity markets. *IET Gener. Transm. Distrib.* **2010**, *4*, 315–323. [CrossRef]
35. Hong, T.; Fan, S. Probabilistic electric load forecasting: A tutorial review. *Int. J. Forecast.* **2016**, *32*, 914–938. [CrossRef]
36. Azzam, M. Robust automatic generation control. *Energy Convers. Manag.* **1999**, *40*, 1413–1421. [CrossRef]
37. Mohanty, B.; Panda, S.; Hota, P.K. Robust automatic generation control. *Alex. Eng. J.* **2014**, *53*, 537–552. [CrossRef]
38. Friedland, B. *Control System Design: An Introduction to State-Space Methods*; Dover Publications: Mineola, NY, USA, 2005.
39. Guo, W.; Tang, Y.; Dai, Y.; Guo, Y. The Analysis of the Primary Frequency Regulation in Electric Power System. In Proceedings of the International Forum on Energy, Environment and Sustainable Development, Shenzhen, China, 16–17 April 2016.
40. Australian Energy Market Operator. Frequency Control. Available online: https://www.aemo.com.au/-/media/Files/Electricity/NEM/Security_and_Reliability/Reports/2016/AEMO-Fact-Sheet_Frequency-Control---Final.pdf (accessed on 1 April 2019).
41. Williams, S.; Short, M.; Crosbie, T. Evaluating the role of building thermal inertia for the provision of decentralised demand side primary electrical frequency regulation services. In Proceedings of the Sustainable Thermal Energy Management International Conference (SusTEM2017), Alkmaar, The Netherlands, 28–30 June 2017.
42. Hashem Eiza, M.; Ni, Q. Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. *IEEE Veh. Technol. Mag.* **2017**, *12*, 45–51. [CrossRef]
43. Goel, S.; Hong, Y.; Papakonstantinou, V.; Kloza, D. *Smart Grid Security*; Springer: London, UK, 2015.
44. Dabrowski, A.; Ullrich, J.; Weippl, E.R. Grid shock: coordinated load-changing attacks on power grids. In Proceedings of the Annual Computer Security Applications Conference, Orlando, FL, USA, 4–8 December 2017.
45. Cooper, C. WannaCry: Lessons Learned 1 Year Later. 2018. Available online: https://www.symantec.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later (accessed on 1 April 2019).
46. Ghamkhari, M. Transactive Energy versus Demand Response in Cutting Wholesale Electricity Prices. In Proceedings of the IEEE International Conference on Smart Grid and Smart Cities, Berkeley, CA, USA, 25–28 June 2019.