Confronting the Threat

Analysis of the Impact of MaDIoT Attacks in Two Power System Models

Perez , Nestor Rodriguez ; Domingo, Javier Matanza ; Sigrist, Lukas ; Rueda Torres, José ; López, Gregorio López

DOI
10.3390/en16237732

Publication date
2023

Document Version
Final published version

Published in
Energies

Citation (APA)
Perez , N. R., Domingo, J. M., Sigrist, L., Rueda Torres, J., & López, G. L. (2023). Confronting the Threat: Analysis of the Impact of MaDIoT Attacks in Two Power System Models. *Energies*, *16*(23). https://doi.org/10.3390/en16237732

energies

MDPI

Article

Confronting the Threat: Analysis of the Impact of MaDIoT Attacks in Two Power System Models

Néstor Rodríguez-Pérez [1,*], Javier Matanza Domingo [1], Lukas Sigrist [1], Jose Luis Rueda Torres [2] and Gregorio López López [1]

[1] Institute for Research in Technology, Comillas Pontifical University, 28015 Madrid, Spain
[2] Faculty of EEMCS, Delft University of Technology, 2628 CD Delft, The Netherlands
* Correspondence: nestor.rodriguez@iit.comillas.edu

Abstract: The increasing penetration of Internet of Things (IoT) devices at the consumer level of power systems also increases the surface of attack for the so-called Manipulation of Demand through IoT (MaDIoT) attacks. This paper provides a comparison of the impact that MaDIoT attacks could have on power systems with different characteristics, such as the IEEE 39-Bus (New England) and the PST-16 system (simplified European model), by assuming that the attacker does not have advanced knowledge of the grid. The results for the IEEE 39-Bus system expand and complement the results obtained by previous work. The simulation results show that these systems present significant differences between them with respect to the success probability of an attack, being in general much higher for the IEEE 39-Bus system. In the PST-16 system, the required number of bots to obtain a certain success probability varies depending on the area attacked. However, a high probability of success does not necessarily mean a high impact on the system. This paper shows that the response to the high-impact MaDIoT attacks of the two models considered is very different as the initial impact of the attack on the system also differs, mainly affecting rotor angles in the PST-16 system, and the frequency in the IEEE 39-Bus.

Keywords: cyberattack; power system dynamics; MaDIoT; load altering attacks; powersystem stability

Citation: Rodríguez-Pérez, N.; Matanza Domingo, J.; Sigrist, L.; Rueda Torres, J.L.; López López, G. Confronting the Threat: Analysis of the Impact of MaDIoT Attacks in Two Power System Models. *Energies* **2023**, *16*, 7732. https://doi.org/10.3390/en16237732

Academic Editors: Mourad Debbabi, Basile L. Agba and Marthe Kassouf

Received: 10 October 2023
Revised: 14 November 2023
Accepted: 21 November 2023
Published: 23 November 2023

1. Introduction

In recent years, there has been an increasing concern over the security of power systems. With the increasing penetration of Internet of Things (IoT) devices at the consumer level, cyberattacks may not only target utilities' Supervisory Control And Data Acquisition (SCADA) systems [1] but try to exploit the vulnerabilities of these devices [2]. IoT devices generally have lower levels of security [3] and, when massively compromised, may be used to reduce the security margins of the system, cause load shedding, or cause a cascading failure that results in a wide-area blackout [4–6]. In addition to being more vulnerable than SCADA systems, the surface of attack of electricity demand is larger, and high-wattage devices such as electric vehicle charging points are not being continuously monitored by the system operator (SO) [7,8].

In [9], the authors present the concept of internet-based load altering attack, identifying direct and indirect loads that could be compromised through the internet, such as data centers, demand side management loads, and loads directly managed by customers (e.g., air conditioning, washing machines, etc.).

The term MaDIoT (Manipulation of Demand through IoT) attack is first introduced by [5] as an attack that disrupts the normal operation of the power grid by altering the power demand using IoT devices to which the attacker has access. The authors of [5] study these attacks on the Polish grid model and conclude that these can cause local outages and large blackouts in the grid. However, reference [10] suggests the possibility that the

model analysed is not N-1 secure, which would lead to an overestimation of the impact of the attacks.

Reference [10] shows that causing a wide area blackout in a large North American regional system through evenly distributed MaDIoT attacks is exceedingly challenging; even if the grid was put in a vulnerable state previously, such attacks would only lead to partial blackouts due to the disconnection of a portion of the loads (via Under-Frequency Load Shedding (UFLS) protection) and generators (via Over-Frequency Generator Rejection (OFGR) protection). After this, the system would quickly recover its stability thereafter.

In [11], the authors study scenarios in the IEEE 39-Bus system assuming that the attacker possesses advanced knowledge about the topology of the system and the estimated generation/demand for each node; this would enable the launch of more sophisticated attacks targeting the most vulnerable nodes. The results in [11] present success rates between 67 and 91% in causing widespread blackouts; however, the criteria used to consider a MaDIoT attack as successful are unclear, and the likelihood of an attacker having the required system knowledge and resources is presumably low.

This paper studies and compares the impact of MaDIoT attacks on power systems with different characteristics using DIgSILENT PowerFactory. For this purpose, the IEEE 39 test system, as well as a simplified model of the European power system (PST-16), are used. These systems mainly differ in their size (network and demand) and generation mix. For the study, simulations of attacks on three random nodes are carried out in both models when they are facing peak-demand conditions. Therefore, it is assumed that the attacker does not have advanced knowledge about the grid. Under these assumptions, this paper presents results for the IEEE 39-Bus system that are compared to those obtained in [11], to expand on and complement them.

The main contributions of this paper are the following:

- An analysis of the impact of MaDIoT attacks on the simplified model of the European power system: the PST-16 benchmark model. To the authors' knowledge, this model is used for the study of MaDIoT attacks for the first time in this paper since previous works have mainly used American system models [10–13].
- Taking the results in [11] as a base, this paper provides new results for the IEEE 39-Bus system under different assumptions, providing additional insights into the potential impact of MaDIoT attacks in that system.
- A comparison of results when simulating MaDIoT attacks in IEEE 39-Bus and PST-16 systems.

The rest of the paper is organised as follows. Section 2 describes the test systems used for the comparative analysis, how different components are configured, and the assumptions and scenarios considered. Then, Section 3 presents and discusses the simulation results obtained, and, finally, Section 4 draws the conclusions of the study and proposes future research.

2. Methodology

Similarly to [5,10,11], the study presented in this paper uses simulation results to compare the performance of MaDIoT attacks in the IEEE 39-Bus system [14], which is used in [11], and the PST-16 system [15], which is used for the first time for the analysis of MaDIoT attacks. This way, the impact on an American grid and a European grid can be compared as different power system models including different electrical topologies, demand distributions, generation structures, and exhibiting different dynamic behaviour may have an impact on the success of MaDIoT attacks. The software used for the simulations is DIgSILENT PowerFactory 2022 SP3 (22.0.6.0).

Below, a brief description of the test systems used can be found, followed by an explanation of the protection schemes implemented and the assumptions and scenarios considered for the analysis.

2.1. Test Systems

Two base systems are used for the analysis: the IEEE 39-bus system and the PST-16 benchmark system. Table 1 provides a summary of the characteristics of these models.

Table 1. Summary of the characteristics of the IEEE 39-BUS and the PST-16 models.

	IEEE 39-BUS	PST-16
Frequency (Hz)	60	50
Areas	1	3
Number of buses	39	66
Base active load (MW)	6097.1	15,565
Base reactive load (Mvar)	1408.9	2225
Generators	10	16
Generation type	hydro, thermal	hydro, thermal, and nuclear
Voltage level (kV)	345	380, 220, 110

2.1.1. IEEE 39-Bus

It represents the New England power system, consisting of 39 buses, with a total base load of 6097.1 MW of active power and 1408.9 Mvar of reactive power (default conditions of the model in PowerFactory). Since it is an American system, the electrical frequency is set to 60 Hz.

For the IEEE 39-Bus case, the default dynamic load model of the system model in PowerFactory is used.

2.1.2. PST-16 (Simplified European Model)

The PST-16 Benchmark System [15] consists of three areas (A, B, and C) and 66 buses, with a total base load of 15,565 MW of active power and 2225 Mvar of reactive power. Since it represents a European system, the electrical frequency is set to 50Hz.

For this system, the constant impedance load model is used [15]. Regarding the modelling of generators, the ones used by the base model were not altered. Details on the generator's model and the grid diagram can be found in [15].

Figure 1 shows a simplified diagram of the PST-16 system. Area A represents the north of Europe, with a high share of hydro generation, and areas B and C represent central and south Europe, respectively, with high shares of thermal and nuclear. As Figure 1 shows, area C concentrates the loads, so power has to be transferred from area A and B to area C through two long tie-lines.

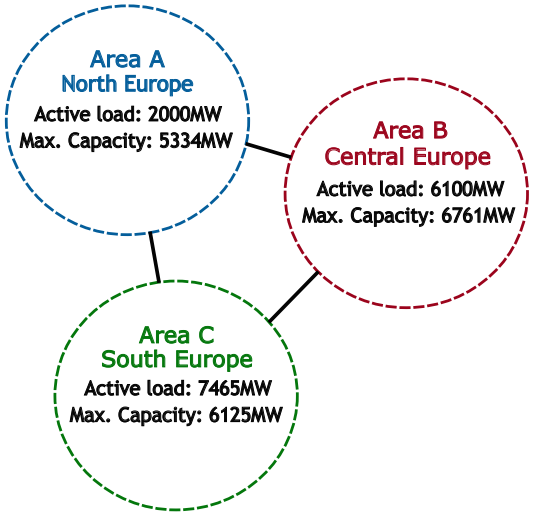

Figure 1. Simplified diagram and main characteristics of the PST-16 benchmark model.

The base conditions of the PST-16 system can be considered to correspond to peak-demand conditions as it represents 85% of the generation capacity.

2.2. Protections

Four protection types that are relevant to the study were implemented in the test systems: overvoltage protections, undervoltage protections, an Under-Frequency Load Shedding (UFLS) scheme, and an Over-Frequency Generator Rejection (OFGR) protection scheme.

2.2.1. Overvoltage and Undervoltage Protections

These protections disconnect the loads when voltage is above (F59 phase overvoltage protection) or below (F27 phase undervoltage protection) a pre-defined value. Overvoltage protections are configured to trip when voltage surpases 1.1 p.u for 10 s, whereas undervoltage protections trip when voltage is below 0.85 p.u for 10 s.

2.2.2. UFLS Protection

This protection scheme gradually disconnects loads from the system as the frequency drops below certain levels, as shown in Table 2.

Table 2. UFLS scheme applied for the 50 and 60 Hz models (frequency vs. load to be shed).

Frequency Threshold (Hz)	**49** **59**	**48.8** **58.8**	**48.6** **58.6**	**48.4** **58.4**	**48.2** **58.2**	**48** **58**
Load-shed (%)	5	5	10	10	10	10

2.2.3. OFGR Protection

To protect the generators, the protection trips when the frequency at the generation bus reaches 51.7 Hz (PST-16) or 61.7 Hz (IEEE 39), which are values similar to those used in [10]. These protections disconnect the corresponding generator from the system.

2.3. Attack Models and Simulation Scenarios

For the analysis, it is assumed that every compromised load (i.e., bot) consumes 3 kW of active power as in [11]. Trying to keep the power factors similar to those in the baseline test systems, the attack is considered to also imply a variation in the reactive power. The power factor of the demand (inductive) for the IEEE 39-bus and PST-16 systems is 0.97 and 0.99, respectively. Therefore, the reactive power of the bot is considered to be 0.69 kvar for the IEEE 39-bus system and 0.42 kvar for the PST-16 system. Only MaDIoT attacks that increase power consumption are considered, as in [11].

This paper focuses on the impact of MaDIoT attacks on power systems. As in previous works [5,10,11], we assume that the target devices can be compromised. Thus, the specific botnet architecture is out of scope. Nevertheless, it can be assummed that the devices are compromised somehow (e.g., they are accessible from the Internet and keep default passwords), and then a malware is installed on them to allow remote command and control, as in the case of the famous DDoS attack orchestrated against the DNS provider Dyn back in 2016, which used millions of IoT devices infected with the Mirai malware [16,17] and managed to put the Internet against the ropes. The attack model, following the modelling guidelines provided by [18], is summarised in Table 3. The frequency of MaDIoT attacks is considered to be iterative as multiple attemps would be needed to achieve the desired impact. The real-time detection of MaDIoT attacks by the system operator is extremely difficult to achieve [5,19] since the attacked devices are not under the control of system operators, so the attack reproducibility and discoverability can be classified as a multiple-times attack. The functional level of the attack can be considered level 1 (the manipulation of control networks) or level 2 (local networks overseeing processes), according to [18]. The attacked assets would be high-wattage devices connected via IoT, whose equivalent to the

classification in [18] would be field controllers and human–machine interfaces. The attack techniques used by the attacker would be the modification of control logic (to activate the high-wattage devices), wireless compromise, and Denial-of-Service of the power grid (final objective of the attack). Since the attacker needs to obtain unauthorised access to modify control commands, the attack premises are communications and protocols, as well as asset control commands.

Table 3. Considered MaDIoT attack model based on the modelling guidelines by [18].

	Attack Model
Attack frequency	Iterative
Attack reproducibility and discoverability	Multiple-times
Attack functional level	Level 1 or 2
Attacked asset	Field controllers, human–machine interfaces
Attack techniques	Modify control logic, wireless compromise, and Denial-of-Service to the power grid
Attack premise	Cyber: communications and protocols, and asset control commands

Regarding the attacker, in [11] it is presumed to know details of the grid, such as its topology and power flows, so that voltage stability indexes can be calculated, identifying the most vulnerable nodes. This is justified by studies that state that much information can be obtained through openly available information [20] or by using satellite images (for example, Google Maps) [21–23]. This process can be very time-consuming, and it is extremely complex to check its accuracy to perform a power flow analysis. Furthermore, the attacker would need to have access to devices in all the nodes of the system or target specific nodes and try to find devices connected to those nodes that can be compromised.

However, an attacker may already have a botnet to exploit without knowing exactly where the bots are connected electrically but with a good idea of their proximity (e.g., by mapping the IPs). For this reason, this article considers that the attacker does not have advanced knowledge of the grid, significantly reducing the amount of work the attacker would need to carry out before the attack and, therefore, increasing the possibility for the power system of suffering an attempt of MaDIoT attack.

Table 4 summarises the adversary model according to the modelling guidelines provided by [18]. As mentioned previously, the adversary knowledge would be oblivious and the attacker does not have physical access to the assets (non-possession adversary access). MaDIoT attacks are targeted attacks (the objective are high-wattage IoT devices), and the attacker is considered to have substantial resources, tools, and skills to carry out the attack (class II). It should be noted that this paper assumes that the attacker has managed to compromise the devices and install a piece of malware that allows for command and control, so the attacker can control a massive number of devices. Since this kind of attack has already been reported in the state of the art, the feasibility of the attack does not represent the matter of study of the paper, which instead focuses on the impact that maliciously controlling a massive amount of consumption may have on the power system.

Table 4. Considered MaDIoT adversary model based on the modelling guidelines by [18].

	Attack Model
Adversary knowledge	Oblivious
Adversary access	Non-possession
Adversary specificity	Targeted attack
Adversary resources	Class II

To consider that bots are close to each other and to study a worst-case-like scenario, the analysed attacks only affect three nodes. These nodes are selected randomly every time a simulation is executed, in a Monte Carlo-like way, as opposed to the approach in [11], where the most vulnerable nodes were targeted.

For the PST-16 system, the attacked nodes belong to the same area since the closer they are, the higher the expected impact on the system [11]. Attacks are carried out at t = 1 s in the simulation.

For both systems, the attack is considered successful if, at the end of the simulation, loads have been disconnected (the tripping of UFLS, overvoltage, or undervoltage protections) or if generators had to be disconnected (OFGR protections). This criterion is similar to the one in [13], which considered an attack as successful if it trips at least one over/under frequency protection relay, even if the impact is not catastrophic.

Table 5 shows the scenarios considered for the analysis for each test system. For each one, the botnet size varies in the range [50 k, 500 k], in 50 k steps, and the simulation time is 21 s to keep the computational load at acceptable levels. For the PST-16 system, a total of nearly 1500 simulations are performed, while the IEEE 39-Bus accounts for 424 simulations.

Table 5. MaDIoT attack scenarios for the IEEE 39-Bus model (New England) and the PST-16 model (Europe).

Scenario	Test System	Area	Botnet Size	# Nodes Attacked
US39	IEEE 39	-	[50 k, 500 k]	3
EU-A	PST-16	A	[50 k, 500 k]	3
EU-B		B		
EU-C		C		

3. Analysis of Results

In this section, the simulation results for the scenarios considered in Table 5 are presented and discussed.

3.1. Success Ratio

To provide an overview of the results and ease the comparison of the two models, Figure 2 shows the success ratio (the number of successful attacks divided by the total number of attacks) of the MaDIoT attacks simulated for the scenarios presented in Table 5. In this figure, the differences in the success ratios between the US39 scenario and the EU scenarios are noticeable.

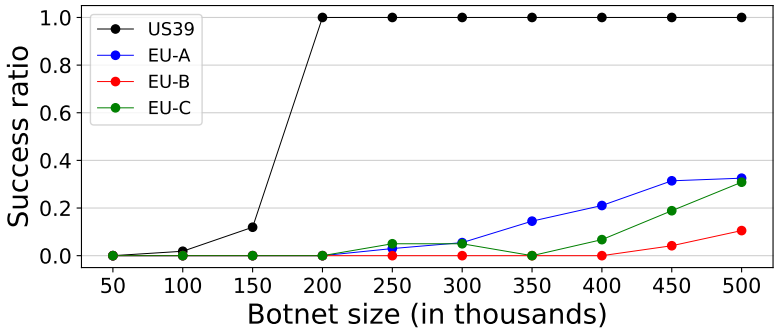

Figure 2. Success ratio for different scenarios when increasing the size of the botnet.

For the US39 scenario, it is remarkable that all the attacks simulated that compromised more than 150 k bots were successful. In fact, the difference between 150 k and 200 k is significant, going from 10% success probability to 100%. The consideration of an attack as successful if it trips at least one protection explains this difference. This means that, under the conditions assumed, it does not matter if the buses affected are close between them

when compromising more than 150 k bots: the attack will always manage to disconnect loads or generation. Therefore, the attacker does not need advanced knowledge of the grid: by performing its attack during the peak demand hour, the probability of success could be high. It may seem like this contradicts the results presented in [11]; however, it should be taken into account that the study in [11] considered a daily load pattern for the grid, so its results may aggregate the success ratio of carrying out MaDIoT attacks during valley demand hours (which could present lower success ratios) and during peak demand (which could present higher success ratios).

On the other hand, regarding the PST-16 system, MaDIoT attacks start being successful in the EU-A and EU-C scenarios for botnets $>$ 200 k bots and, for the EU-B scenario, for botnets $>$ 400 k. While EU-A and EU-C end up having a similar success ratio (≈30%) for the largest botnet size considered, the maximum success ratio for the EU-B scenario is significantly smaller (≈10%). As Figure 1 shows, areas A and C are the areas with the highest gap between generation capacity and demand: area A has more generation than demand, while area C needs to import power from outside the area.

The number of bots needed to have a successful attack is lower in the IEEE 39-Bus system than in the PST-16 as it is also a smaller system.

3.2. Impact of MaDIoT Attacks on Test Systems

Despite the fact that IEEE 39-Bus and the PST-16 grid models present different success ratios to the MaDIoT attacks, the success ratio is not tantamount to the degree of the impact (the number of loads and/or generators disconnected). Table 6 shows the average generation and demand disconnected in successful MaDIoT attacks to 500 k bots in the US39 and EU-C scenarios (EU-C is the highest impact scenario for the PST-16 model). Although the average demand affected is similar in both scenarios, in the US39 scenario generation is not disconnected. To compare them, two high-impact cases (one per model) have been selected for analysis in this paper. The results of these two cases are plotted in Figures 3–5, which are discussed below.

Table 6. Average impact on the system when successfully attacking 500 k bots in the US39 and EU-C scenarios.

Scenario	Botnet Size	Average Generation Disconnected	Average Demand Disconnected
US39	500 K	0 MW	983.64 MW
EU-C	500 K	1515.28 MW	938.84 MW

Figure 3 plots the frequency (Hz), the voltages (p.u), and the relative rotor angle of generators (with respect to the reference generator) against time when compromising a total of 500 k bots within loads 30, 31, and 34 in the PST-16 model (one high-impact EU-C scenario). The time of the attack (t = 1 s) is indicated by "*" in the *x*-axis. For the frequency and voltages, only the information for six buses is plotted, including the buses to which the attacked loads are connected, to keep the figure visually simple. Regarding the relative rotor angle, only three generators from area C are represented.

Figure 3 shows how the attack significantly destabilises the system. Figure 4 shows a zoom on the frequency and the relative rotor angle during the first 10 seconds of the case shown in Figure 3. Starting with the frequency, the attack has, at first, a reduced impact that is noticeable for a few seconds; a slight oscillation between the areas is observed, but the system manages to confine frequency variations and is apparently stable. Nevertheless, by t = 15 s, area C diverges from the other two areas. The frequency of bus C10, which has generation connected, drops suddenly to 46 Hz at around t = 18.5 s. These frequency variations about 12 s after the attack are explained by the loss of the rotor angle stability of the system.

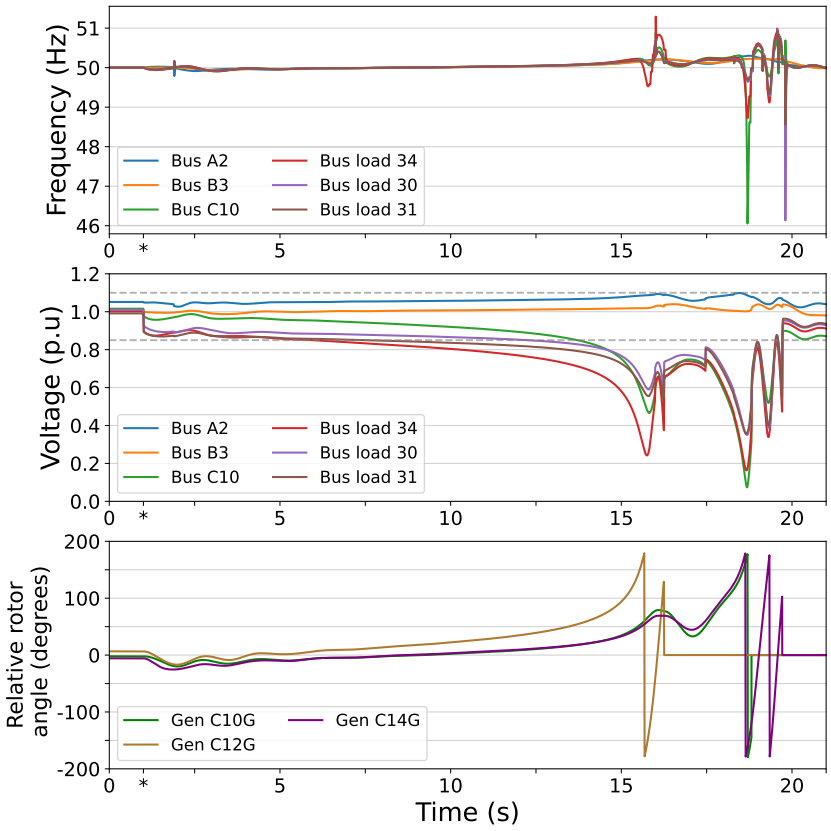

Figure 3. Frequency, voltages, and relative rotor angle of generators when attacking 500 k bots in loads 30, 31, and 34 in the PST-16 system (EU-C scenario with high impact). Attack at t = 1 s (indicated by *).

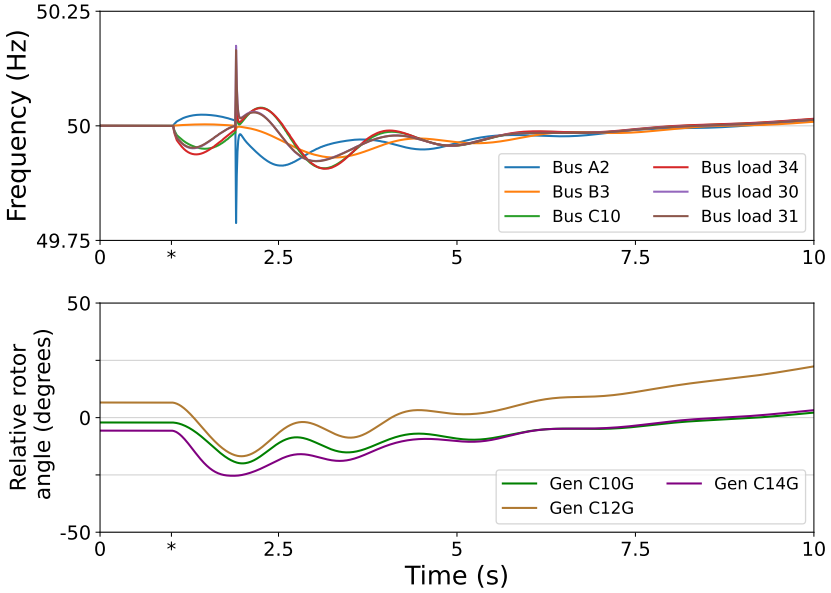

Figure 4. Zoom to the frequency and relative rotor angle shown in Figure 3 for the first 10 s. Attack at t = 1 s (indicated by *).

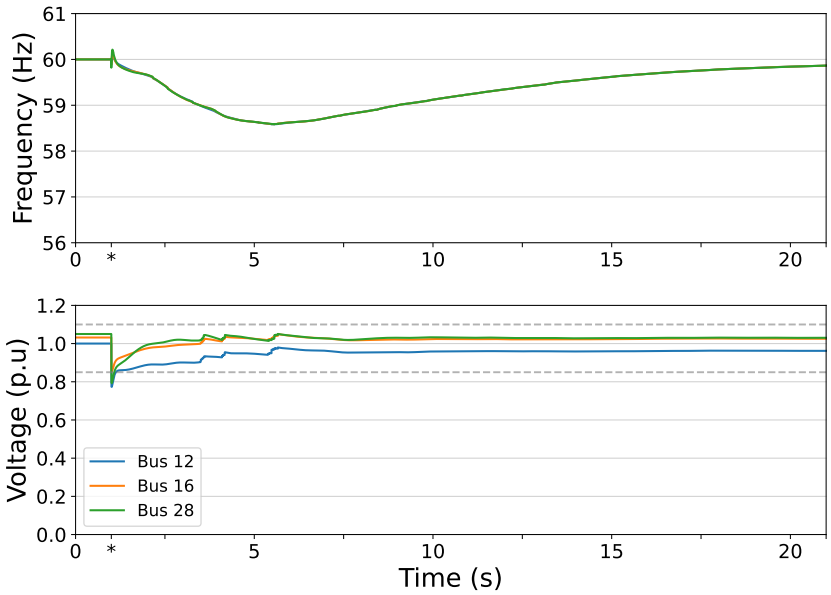

Figure 5. Frequency and voltages when attacking 500 k bots in loads 12, 16, and 28 in the IEEE 39-Bus system (US39 scenario with high impact). Attack at t = 1 s (indicated by *).

The middle plot of Figure 3 clearly shows the immediate high impact that the attack has on the voltages of area C. It is worth remembering that the system, prior to the attack, was already working under what could be considered peak-demand conditions and that, under these conditions, area C was already dependent on the power imports from the other two areas. The voltages of the buses attacked drop significantly to just above the limit configured for the tripping of the undervoltage protections. However, due to the increase in demand caused by the attack, the system loses rotor angle stability and goes into voltage collapse. The bottom plot of Figure 3 shows that the rotor angles in the generators of area C start to diverge with respect to the reference generator after some initial oscillations. Therefore, the system first experiences a rotor angle stability problem that leads to a voltage collapse.

Since voltages drop below 0.85 p.u for more than 10s (Figure 3), undervoltage protections start tripping, disconnecting loads from the system. The actuation of these protections, together with the UFLS and OFGR protections in the frequency domain, are one of the main causes for the oscillations in the 15–20 s interval. After the actuation of the protections, the system seems to recover by t = 20 s but with rather low voltage levels (e.g., at Bus C10). By that time, nearly 2.9 GW of generation has become disconnected from the system due to the OFGR scheme. However, the impact could be different if further protection features were implemented (e.g., distance protection with/without out-of-step protection). In this case, despite facing an increase in the demand due to the attack, the system ends up with around 3 GW less demand than before the attack (≈20% decrease), due to load shedding (UFLS and undervoltage protections). This means that not only the equivalent to the extraordinary demand caused by the attack had to be disconnected from the system but also that more loads had to be disconnected for the system to recover.

Similarly to Figure 3, Figure 5 plots the frequency and voltages when attacking 500 k bots in loads 12, 16, and 28 in the IEEE 39-Bus system (one high-impact US39 scenario).

In the case plotted, the immediate impact of the attack on the frequency and voltages of the system is significant. It can be observed that the frequency drops by 1 Hz in approximately two seconds. Below 59 Hz, the UFLS scheme starts actuating, as described in Table 2. This softens the drop in frequency; only when it reaches ≈58.6 Hz does the system start to increase the frequency. However, the recovery is slow. In this case, the system manages to keep all voltages within limits, so the only protections tripping are the UFLS protections. These protections shed about 1.1 GW of loads along the system.

Nevertheless, despite disconnecting loads, the total demand of the system increases by 76 MW with respect to the demand before the attack (≈1.2% increase). This means that, practically, the amount of demand disconnected is equivalent to the demand increase provoked by the attack. However, the shedding also affects legitimate loads as UFLS protections make no distinction. Compared to the EU-C case analysed in Figure 3, the relative impact is smaller because the system manages to maintain its stability.

Therefore, although any attack compromising any three buses in the IEEE 39-Bus system may be successful, its impact could be relatively low, equivalent to the magnitude of the attack. On the other hand, destabilising the PST-16 system is more difficult as it is larger and has more resources to face the attack; however, as discussed, a successful attack can significantly affect the stability of the system, causing the partial disconnection of loads and generation.

The results presented also show the different types of impact that MaDIoT attacks have on different grids. In the case presented for the PST-16 system, the attack mainly affects rotor angle instability in area C and voltages, whereas for the IEEE 39-Bus system the main impact was on the frequency, motivated by the high inertia of the generation in the model.

It should be highlighted that these results correspond to a worst-case-like scenario where demand is high, and the attack affects only three electrical nodes that are close among them. The success ratio and impact of the attack can be expected to be lower when the attack is distributed among a greater number of nodes (while keeping the same botnet size), when demand is low (as more line capacity becomes available and the relative attack size per botnet size is smaller) or when distant nodes are the ones affected (for example, when there is only one node per area in the PST-16 model). Not only the size but also the location of the attack has an impact on the survival of the system, i.e., whether or not the attack can destabilise the power system. For instance, while the distribution of the attacks among different locations affects fewer frequency-stability-induced problems, it may affect voltage-stability-induced problems.

4. Conclusions and Future Work

High-wattage IoT devices at the consumer level of electricity grids could constitute a new attack vector as they would be placed in multiple nodes of power systems. Therefore, knowing to what extent MaDIoT attacks could affect different types of systems, under different conditions, will become essential as the number of these devices increases.

This paper has analysed and compared the impact of MaDIoT attacks in the PST-16 model (simplified European model) and the IEEE 39-Bus model (New England system), expanding and complementing the studies performed by previous work. The main assumptions were that the affected loads were distributed in three random nodes and that the attacker did not have advanced knowledge about the grid. An attack was considered successful if it managed to disconnect either loads and/or generation through protections.

The results show how the success ratio of the attacks depends on the power system affected. The IEEE 39-Bus system presents success ratios of up to 100%, while the maximum success ratio obtained in this study for the PST-16 system is around 30%. However, a more detailed analysis of high-impact cases has shown that higher success ratios do not necessarily mean a higher impact. The PST-16 system is larger and has more resources to face the increase in demand caused by the attack, but a high-impact attack such as the one analysed would cause a blackout equivalent to 20% of the initial demand, experiencing an impact that is greater than the magnitude of the attack. In the IEEE 39-Bus system, the analysed high-impact case just resulted in an impact equivalent to the magnitude of the attack.

The main limitation of this work, also shared by previous work, is related to the lack of consideration of the dynamics and protection schemes of the large electricity distribution systems connected to transmission systems. This would require the development of an integrated transmission and distribution system model, which would also require

a large computational capacity. The analysis of MaDIoT attacks considering both the transmission and distribution system is an interesting research line to explore in the future. Other interesting future research work goes along the line of including automatic or manually induced operator actions, such as re-dispatches, to avoid, for instance, line overloads that could lead to subsequent line trippings and initiate a cascading outage. Such mitigation actions have not been considered in previous works. MaDIoT attacks targeting nodes from different areas in the PST-16 system may be also considered. The analysis of the impact of these attacks when increasing power transformer capacity or the capacity of the lines connecting the areas would also be interesting. Sequential attacks (increasing/decreasing demand in time during the same attack) and attacks in low-demand conditions also represent interesting future research lines. Finally, considering the wide adoption of distributed generation at consumer level, it has also become a relevant attack vector. Thus, evaluating the impact of attacks that involve massively controlling not only consumption but also generation represents a promising research line that may suppose the next evolution of MaDIoT attacks (MaDIoT 3.0).

Author Contributions: N.R.-P.: conceptualization, methodology, formal analysis, investigation, software, writing—original draft preparation, and visualization. J.M.D. and G.L.L.: writing—review and editing, supervision, project administration, and funding acquisition. L.S.: writing—review and editing, supervision, and validation. J.L.R.T.: resources, writing—review and editing, and supervision. All authors have read and agreed to the published version of the manuscript

Funding: This work was developed within the framework of the eFORT Project. This project has received funding from the European Union's Horizon Europe Research and Innovation programme under Grant Agreement No 101075665. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them. During the development of this work, the first author acknowledges that financial support was received from Comillas Pontifical University for research stays for professors and researchers in foreign research centers (in this case, TU Delft).

Data Availability Statement: Data are contained within the article.

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

Abbreviations

The following abbreviations are used in this manuscript:

DER	Distributed Energy Resources
DSO	Distribution System Operator
IoT	Internet of Things
MaDIoT	Manipulation of Demand through IoT
OFGR	Over-Frequency Generator Rejection
SCADA	Supervisory Control And Data Acquisition
UFLS	Under-Frequency Load Shedding

References

1. Bruno, C.; Guidi, L.; Lorite-Espejo, A.; Pestonesi, D. Assessing a Potential Cyberattack on the Italian Electric System. *IEEE Secur. Priv.* **2015**, *13*, 42–51. [CrossRef]
2. Xenofontos, C.; Zografopoulos, I.; Konstantinou, C.; Jolfaei, A.; Khan, M.K.; Choo, K.K.R. Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies. *IEEE Internet Things J.* **2022**, *9*, 199–221. [CrossRef]
3. Alrawi, O.; Lever, C.; Antonakakis, M.; Monrose, F. SoK: Security Evaluation of Home-Based IoT Deployments. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 1362–1380. [CrossRef]
4. Dabrowski, A.; Ullrich, J.; Weippl, E.R. Grid Shock: Coordinated Load-Changing Attacks on Power Grids: The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well. In Proceedings of the 33rd Annual Computer Security Applications Conference, Orlando, FL, USA, 9–13 December 2017; pp. 303–314. [CrossRef]
5. 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.

6. Goodridge, M.P.; Zocca, A.; Lakshminarayana, S. Analysis of Cascading Failures Due to Dynamic Load-Altering Attacks. In Proceedings of the 14th IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (IEEE SmartGridComm 2023), Glasgow, UK, 31 October–3 November 2023.
7. 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. [CrossRef]
8. Mokarim, A.; Gaggero, G.B.; Marchese, M. Evaluation of the Impact of Cyber-Attacks Against Electric Vehicle Charging Stations in a Low Voltage Distribution Grid. In Proceedings of the 14th IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (IEEE SmartGridComm 2023), Glasgow, UK, 31 October–3 November 2023.
9. Mohsenian-Rad, A.H.; Leon-Garcia, A. Distributed Internet-Based Load Altering Attacks Against Smart Power Grids. *IEEE Trans. Smart Grid* **2011**, *2*, 667–674. [CrossRef]
10. Huang, B.; Cardenas, A.A.; Baldick, R. Not everything is dark and gloomy: Power grid protections against IoT demand attacks. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, 14–16 August 2019; pp. 1115–1132.
11. Shekari, T.; Cardenas, A.A.; Beyah, R. MaDIoT 2.0: Modern High-Wattage IoT Botnet Attacks and Defenses. In Proceedings of the 31st USENIX Security Symposium (USENIX Security 22), Boston, MA, USA, 10–12 August 2022; pp. 3539–3556.
12. Goodridge, M.P.; Lakshminarayana, S.; Few, C. Analysis of Load-Altering Attacks Against Power Grids: A Rare-Event Sampling Approach. In Proceedings of the 2022 17th International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Online, 12–15 June 2022; pp. 1–6.
13. 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]
14. Athay, T.; Podmore, R.; Virmani, S. A practical method for the direct analysis of transient stability. *IEEE Trans. Power Appar. Syst.* **1979**, *PAS-98*, 573–584. [CrossRef]
15. Rueda, J.L.; Cepeda, J.C.; Erlich, I.; Korai, A.W.; Gonzalez-Longatt, F.M. Probabilistic Approach for Risk Evaluation of Oscillatory Stability in Power Systems. In *PowerFactory Applications for Power System Analysis*; Gonzalez-Longatt, F.M., Luis Rueda, J., Eds.; Power Systems; Springer International Publishing: Berlin/Heidelberg, Germany, 2014; pp. 249–266. [CrossRef]
16. Borys, A.; Kamruzzaman, A.; Thakur, H.N.; Brickley, J.C.; Ali, M.L.; Thakur, K. An Evaluation of IoT DDoS Cryptojacking Malware and Mirai Botnet. In Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT), Online, 6–9 June 2022; pp. 725–729. [CrossRef]
17. Antonakakis, M.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z.; Halderman, J.A.; Invernizzi, L.; Kallitsis, M.; et al. Understanding the Mirai Botnet. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, Canada, 16–18 August 2017; USENIX Association: Berkeley, CA, USA, 2017; pp. 1093–1110.
18. 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]
19. Martel, E.; Kariger, R.; Graf, P. *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*; Center for Cybersecurity and Electricity Industry Community, World Economic Forum: Geneva, Switzerland, 2019.
20. Keliris, A.; Konstantinou, C.; Sazos, M.; Maniatakos, M. Open Source Intelligence for Energy Sector Cyberattacks. In *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*; Gritzalis, D., Theocharidou, M., Stergiopoulos, G., Eds.; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; pp. 261–281. ._14. [CrossRef]
21. Arderne, C.; Zorn, C.; Nicolas, C.; Koks, E.E. Predictive mapping of the global power system using open data. *Sci. Data* **2020**, *7*, 19. [CrossRef]
22. Kim, H.; Olave-Rojas, D.; Álvarez Miranda, E.; Son, S.W. In-depth data on the network structure and hourly activity of the Central Chilean power grid. *Sci. Data* **2018**, *5*, 180209. [CrossRef] [PubMed]
23. Medjroubi, W.; Müller, U.P.; Scharf, M.; Matke, C.; Kleinhans, D. Open Data in Power Grid Modelling: New Approaches Towards Transparent Grid Models. *Energy Rep.* **2017**, *3*, 14–21. [CrossRef]