Analysing the Impact of Compromising IoT Consumer Devices in Power Systems

Néstor Rodríguez-Pérez, Javier Matanza Domingo, Lukas Sigrist, Jose Luis Rueda Torres, and Gregorio López López

Abstract This chapter explores the potential risk in power systems due to the increasing penetration of Internet of Things (IoT) devices at the consumer level. It focuses on the potential for Manipulation of Demand through IoT (MaDIoT) attacks, where attackers exploit these devices to disrupt power system operations. For this, a comparative analysis of the impact of MaDIoT attacks on two distinct power system models is provided: the IEEE 39-Bus (New England) system and the PST-16 system (a simplified European model). By assuming that attackers lack advanced knowledge of the grid, the analysis highlights significant differences in the success probability and impact of attacks between these systems, providing insights into the varying responses of different power systems to MaDIoT attacks, and emphasising the need for system operators to consider these in their cybersecurity risk assessment in the future.

Keywords Cyberattack · MaDIoT · Load altering attacks · Power system dynamics · Power system stability

Abbreviations

DSO	Distribution System Operator
EUCC	European Cybersecurity Certification scheme
IoT	Internet of Things
MaDIoT	Manipulation of Demand through Internet of Things
OFGR	Over-Frequency Generator Rejection
SCADA	Supervisory Control and Data Acquisition
TSO	Transmission System Operator

N. Rodríguez-Pérez (✉) · J. Matanza Domingo · L. Sigrist · G. López López
Institute for Research in Technology, Comillas Pontifical University, Madrid, Spain
e-mail: nestor.rodriguez@iit.comillas.edu

J. L. Rueda Torres
Faculty of EEMCS, Delft University of Technology, Delft, The Netherlands

J. Soldatos and H. Abie (eds.), *Technology-Enabled Resilience: Innovations in Critical Infrastructure Protection*, https://doi.org/10.1007/978-3-032-25917-2_5

UFLS Under-Frequency Load Shedding

1 Introduction

In recent years, the cybersecurity of power systems has become a growing concern among countries. Usually, when we think about cyberattacks to power systems, it comes to our mind cyberattacks to Supervisory Control And Data Acquisition (SCADA) systems [8] that may take over the control centre of system operators or that may compromise the employed communication protocols to open circuit breakers and switchgears, such as in the case of the Industroyer attack in Ukraine [22]. However, there are other elements connected to electricity systems that may be vectors of attacks. The increasing penetration of Internet of Things (IoT) devices at the consumer level (such as home assistants, energy management systems, etc.) introduces new vulnerabilities that can be exploited [40].

Most IoT devices have low security levels [2] and, if an attacker manages to compromise a large amount of high-wattage IoT devices, the power system may see its security margins reduce or even experience load shedding and cascading failures leading to wide-area blackouts [12, 17, 37]. Furthermore, it must be considered that the attack surface of electricity demand is larger than that of SCADA systems, the standard user does not have an advanced level of cybersecurity awareness, and high-wattage devices like electric vehicle charging points are not continuously monitored by system operators (SO) [1, 31].

The idea of compromising demand taking advantage of its growing internet connectivity was first introduced in [30], which identified loads that could be compromised such as data centres, demand side management loads and customer-managed loads (e.g., air conditioning, washing machines). This type of attack received the generic name of Load Altering Attack (LAA) [30] and since then has attracted the attention of the research community with different studies [12, 15, 16, 23–26, 32].

Since the term "load" is very generic, Soltan et al. [37] developed the concept of Manipulation of Demand through Internet of Things (MaDIoT) to describe an attack that disrupts normal operation of the power grid by altering the power demand using compromised IoT devices. Soltan et al. studied the Polish grid model and showed that MaDIoT attacks could cause local outages and large-scale blackouts. However, Huang et al. [19] suggested that the Polish grid model analysed might not be N-1 secure, potentially leading to an overestimation of the impact of the attack.

Huang et al. [19] showed that instigating a widespread blackout in a major North American regional system through widespread MaDIoT attacks is quite difficult. Even if the system is initially susceptible, these attacks are likely to cause only partial blackouts, as some loads and generators would be disconnected, allowing the system to stabilise.

Later research by Shekari et al. [35] developed and studied the concept of MaDIoT 2.0 attacks in the IEEE 39-Bus system. MaDIoT 2.0 is a version of MaDIoT where it

is assumed that the attacker had advanced knowledge of the system's topology and the estimated generation/demand for each node. This would enable more sophisticated attacks targeting the most vulnerable nodes. The results obtained by Shekari et al. [35] showed elevated success rates in causing widespread blackouts. However, the criteria for considering a MaDIoT attack successful were unclear, and the likelihood that an attacker possessing the necessary knowledge and system resources is presumably low.

This chapter examines and compares the impact of MaDIoT attacks on two different power systems: the IEEE 39 test system (as in [35]), and the PST-16 system, which is a simplified model of the European power system [34]. These systems differ mainly in size (network and demand) and generation mix, so the PowerFactory simulation results provide insight into the different consequences of MaDIoT attacks in different systems. The results in this chapter have been obtained within the framework of the eFORT project [13], funded by the European Union's Horizon Europe Research and Innovation programme.

2 Methodology

In line with the literature of MaDIoT attacks [19, 35, 37] and given the impossibility of conducting MaDIoT experiments in actual power systems for obvious reasons, a simulation-based approach with DIgSILENT PowerFactory 2022 SP3 (22.0.6.0) was used to evaluate the impact of MaDIoT attacks on two different power systems: the IEEE 39-Bus system, also used in [35], and the PST-16 system. These two system models allow for the evaluation of the impact of MaDIoT attacks on both an American and a European grid, considering differences in electrical topologies, demand distributions, generation structures and dynamic behaviours. The simulations were carried out calling a Python script from PowerFactory, as shown in Fig. 1.

The following sections provide a brief overview of these test systems, detail the protection schemes and outline the assumptions and scenarios considered for the analysis.

2.1 Test Systems

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

2.1.1 IEEE 39-Bus

The New England power system, consisting of 39 buses, has a total base load of 6097.1 MW of active power and 1408.9 Mvar of reactive power, which are the

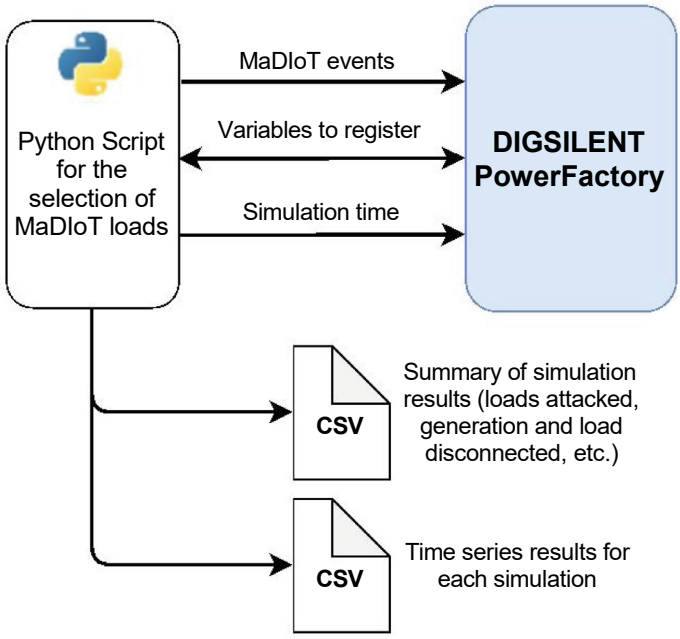

Fig. 1 Diagram showing the interaction between PowerFactory and the python script used to simulate the MaDIoT attacks

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
Max. active power generation (MW)	14,535	18,220
Line capacity (MVA)	With USA/Canada: 1231	Areas A-C: 1572; Areas B-C: 2476; Areas A-B: 2585
Voltage level (kV)	345	380, 220, 110

default initial conditions of the system before the attacks. The electrical frequency is 60 Hz. The system's maximum active power generation capacity is 14,535 MW, with 8500 MW provided by the generator at bus 39, which represents the interconnection USA/Canada. However, the support from this interconnection is fixed at 1000 MW. Consequently, the actual maximum active power capacity of the IEEE-39 system is 6035 MW, with an available reserve of 938 MW, since 1000 MW of demand are supplied by the USA/Canada interconnection. The interconnection bus (bus 39) connects to the rest of the system through two power lines with a total capacity of 1231 MVA. Initially, the load connected to bus 39 consumes 1104 MW, utilising only 19% of the interconnection lines' capacity.

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

2.1.2 PST-16 (Simplified European Model)

The PST-16 Benchmark System [34] comprises 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. These values serve as initial conditions for the system before the simulated MaDIoT attacks. The maximum active power generation capacity of the PST-16 system is 18,220 MW. As it represents a European system, the electrical frequency is set to 50 Hz.

For this system, the load model is constant impedance [34]. The generator models from the base model remain unchanged. Detailed information on the generator model, the grid diagram and the complete PowerFactory model can be found in [34].

Figure 2 presents a simplified diagram of the PST-16 system. Area A represents northern Europe, characterised by a high share of hydro generation, while areas B and C represent central and southern Europe, respectively, with significant shares of thermal and nuclear generation. As shown in Fig. 2, area C requires power transfer from areas A and B through two long links to satisfy its demand. The capacity of the line connecting areas A-C is 1572 MVA, for B-C it is 2476 MVA and for A-B it is 2585 MVA. Under the initial conditions (before the MaDIoT attacks), the loading of these interconnection lines is 110.1%, 17.3% and 37.2%, respectively. These initial conditions for the PST-16 system correspond to peak demand conditions, since it is 85% of the generation capacity.

2.2 Protections

Performing MaDIoT attacks on power systems would trigger electrical protections. For the study presented in this chapter, four types of protection were implemented in PowerFactory: overvoltage protections, undervoltage protections, an Under-Frequency Load Shedding (UFLS) scheme and an Over-Frequency Generator Rejection (OFGR) protection scheme.

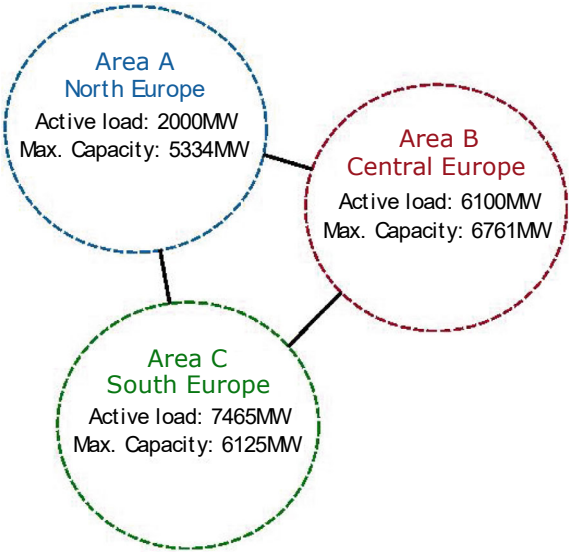

Fig. 2 Simplified diagram of the PST-16 benchmark model [33]

2.2.1 Voltage Protections

These protections disconnect loads when the voltage exceeds (phase overvoltage protection) or falls below (phase undervoltage protection) a predefined threshold.

The overvoltage protections were set to trip when the voltage exceeds 1.1 p.u. for 10 s, while the undervoltage protections trip when the voltage drops below 0.85 p.u. for 10 s.

2.2.2 Frequency Protections

Two type of protections are included in the power system models to be activated when frequency drops or goes above certain thresholds. The UFLS protection scheme gradually disconnects loads from the system as the frequency drops below the levels shown in Table 2.

However, OFGR protections are activated when the frequency of the generation bus reaches 51.7 Hz (PST-16) or 61.7 Hz (IEEE 39), similar to the values used in [19]. When activated, the corresponding generator is disconnected from the system, to safeguard it.

Table 2 UFLS scheme applied for the 50 and 60 Hz models. Based on [18]

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

2.3 Attack Models and Simulation Scenarios

For the study, it is assumed that each compromised load (i.e. bot) consumes 3 kW of active power, which is a common assumption in previous research [35]. To maintain similar power factors to those in the baseline test systems, the attack is also considered to alter the reactive power of the load. 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 a bot is 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 in the demand are considered.

The study in this chapter focusses on the impact of MaDIoT attacks on power systems. As in previous works [19, 35, 37], it is assumed that target devices can be successfully compromised in some manner (e.g., they are accessible from the Internet and retain default passwords), and malware can enable remote command and control. This is similar to the famous DDoS attack against the Dyn DNS provider in 2016, which used millions of IoT devices infected with Mirai malware [4, 7].

The attack model is described by Table 3 following the guidelines provided by [41].

Regarding the attacker, previous studies such as [35] assume that the attacker has advanced knowledge of the details of the grid, such as its topology and power flows, allowing the calculation of voltage stability indices to identify the most vulnerable nodes to attack. This assumption is supported by studies indicating that much information can be obtained from open sources [20] or by satellite images (for example, Google Maps) [5, 21, 29]. This process can be very time-consuming and extremely complex, making it difficult to verify its accuracy to perform a power flow analysis. Additionally, the attacker would need to have access to devices at all nodes of the system or target specific nodes and find devices connected to those nodes that can be compromised.

However, an attacker may already possess a botnet to exploit without knowing the exact electrical connections of the bots but having a good idea of their proximity (e.g., by mapping the IPs). Therefore, the study in this chapter assumes that the attacker does not have advanced knowledge of the grid, significantly reducing the

Table 3 Considered MaDIoT attack model based on the modelling guidelines by [41]

	Attack model
Frequency	Iterative
Reproducibility and discoverability	Multiple-times
Functional level	Level 1 or 2
Compromised asset	Field controllers, human–machine interfaces
Potential techniques	Modify control logic, wireless compromise and Denial-of-Service to the power grid
Attack premise	Cyber: communications and protocols and asset control commands

preparatory work required for the attack and, consequently, increasing the likelihood of a MaDIoT attack attempt on the power system.

Table 4 describes the adversary model following the guidelines provided by [41]. As previously mentioned, it is assumed that the adversary's knowledge is limited, and the attacker does not have physical access to the assets (non-possession adversary access). MaDIoT attacks are targeted attacks (the objective is to compromise high-wattage IoT devices), and the attacker is considered to have substantial resources, tools and skills to successfully execute the attack (class II). It is assumed that the attacker has successfully compromised the devices and installed malware that enables command and control, allowing the control of a large number of devices (botnet).

To ensure that bots are in close proximity and to study a worst-case-like scenario, the simulated attacks only affect three nodes. These nodes are selected randomly for each simulation, following a Monte Carlo-like approach. For the PST-16 system, the attacked nodes are within the same area, as closer proximity is expected to have a higher impact on the system. Attacks are initiated at $t = 1$ s in the simulation.

An attack is deemed successful in both systems when, by the conclusion of the simulation, loads are disconnected due to any activated protection mechanisms, or if generators are disconnected (OFGR protections). This same standard was applied by [3], which classified an attack as successful if it triggered at least one over/under frequency protection relay, irrespective of whether this resulted in a full system blackout.

Table 5 outlines the scenarios considered for the analysis of each test system. For each scenario, the botnet size varies from 50,000 to 500,000 in increments of 50,000, and the simulation time is set to 21 seconds to maintain acceptable computational load. For the PST-16 system, nearly 1500 simulations are performed, while the IEEE 39-Bus system accounts for 424 simulations.

Table 4 Considered MaDIoT adversary model based on the modelling guidelines by [41]

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

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

Scenario	Model	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 MaDIoT Attacks Simulation Results

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

3.1 How Successful Are the MaDIoT Attacks in Activating Protections?

Before analysing the impact of MaDIoT on the two power systems analysed, it is interesting to first inspect how successful these attacks are in each system. For this, the success ratio is defined as in Eq. 1.

$$\text{Success ratio} = \frac{\#\text{Successful MaDIoT attacks}}{\#\text{Attacks}} \tag{1}$$

It is good to remember that, following the criteria of previous research, an attack is considered successful if it manages to activate at least one of the electrical protections installed in the system.

To facilitate the comparison between the two power system models, Fig. 3 illustrates the success ratio of the MaDIoT attacks simulated for the scenarios outlined in Table 5. This figure highlights the noticeable differences in success ratios between the US39 scenario and the EU scenarios.

In the US39 scenario, it should be noted that all simulated attacks compromising more than 150 k bots were successful. The difference between 150 k and 200 k bots (theoretically increasing from 450 MW to 600 MW) is significant, with the success ratio increasing from 10% to 100%. The IEEE-39 system, without interconnection with the USA/Canada, theoretically has a margin of 938 MW before reaching its generation limit, which should be sufficient to withstand attacks of up to 300 k bots from a frequency perspective. However, simulations for 300 k bots revealed that

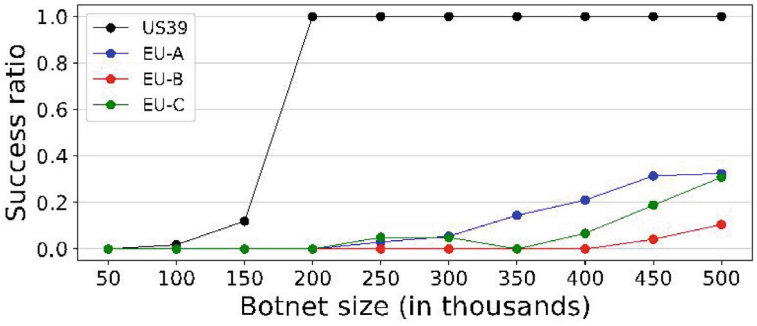

Fig. 3 Success ratio for different scenarios when increasing the size of the botnet

generation does not ramp up quickly enough post-attack to prevent the activation of first-step UFLS protections in some loads, as the attack compromises the loads simultaneously. The high success ratios that are observed are mainly due to the fact that an attack is considered successful if it trips at least one protection. Thus, under the assumed conditions, the proximity of affected buses is irrelevant when more than 150 k bots are compromised; the attack will always trigger UFLS protections in the IEEE-39 system. Consequently, the attacker does not require advanced grid knowledge; performing the attack during peak demand hours, when the system's generation margin is minimal, could result in a high success ratio. Although this may appear to contradict the findings of previous research [35], it is important to note that [35] considered a daily load pattern for the grid, potentially aggregating the success ratios of MaDIoT attacks during valley and peak demand hours.

In contrast, within the PST-16 system, MaDIoT attacks start to succeed in the EUA and EU-C scenarios when botnets surpass 200 k bots, and in the EU-B scenario for botnets larger than 400 k bots. Although EU-A and EU-C eventually show comparable success rates (around 30%) at the largest considered botnet size, the peak success rate for the EU-B scenario is notably lower, at roughly 10%. As illustrated in Fig. 2, areas A and C have the greatest imbalance between generation capacity and demand: area A experiences a generation surplus, while region C depends on power imports from outside the area.

Therefore, Fig. 3 shows that the number of bots required for a successful attack is lower in the IEEE 39-Bus system compared to the PST-16, as it is a smaller system with less generation capacity.

3.2 Beyond Success: Impact of MaDIoT Attacks on Test Systems

Although the IEEE 39-Bus and PST-16 grid models exhibit different success ratios for MaDIoT attacks, the success ratio does not equate to the degree of impact, which can be measured as the amount of loads and/or generation disconnected from the system. Table 6 presents the average generation and demand disconnected in successful MaDIoT attacks involving 500 k bots in the US39 and EU-C scenarios (with EU-C being the highest impact scenario for the PST-16 model). While the average demand affected is similar in both scenarios, generation is not disconnected in the US39 scenario. For comparison, two high-impact cases (one per model) have been selected for a more detailed analysis. The results of these cases are illustrated in Figs. 4 and 5.

Figure 4 shows the frequency (Hz), voltages (p.u) and the relative rotor angle of generators (relative to the reference generator) over time when 500 k bots are compromised, in total, in loads 30, 31 and 34 of the PST-16 model (a high-impact EU-C scenario). The attack time ($t = 1$ s) is marked by an asterisk (*) on the x-axis. For visual clarity, the frequency and voltage data for only six buses are plotted,

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

Scenario	Botnet size (K)	Average generation disconnected (MW)	Average load loss (MW)
US39	500	0	983.64
EU-C	500	1515.28	938.84

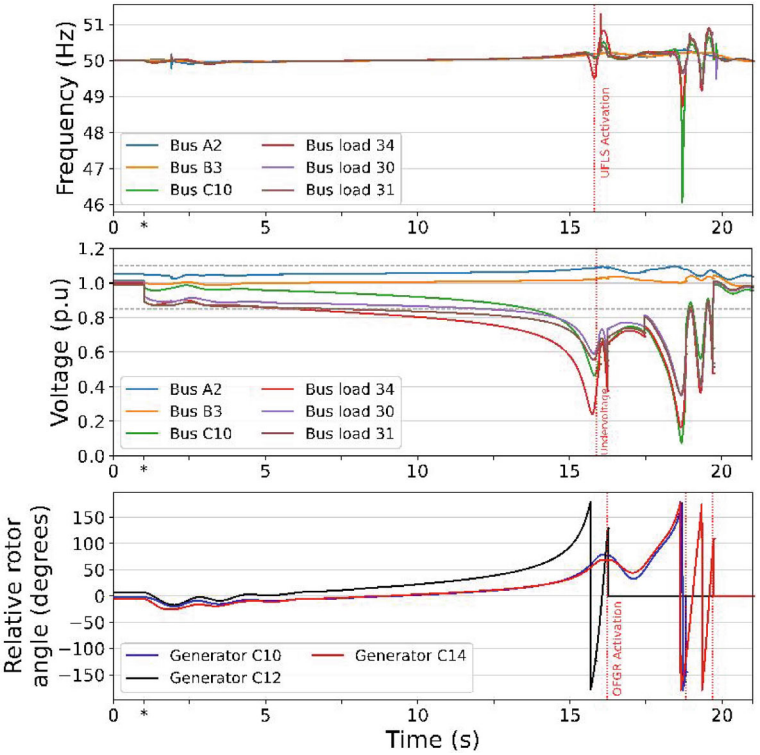

Fig. 4 Frequency, voltages and relative rotor angle of generators when attacking 500 k bots in loads 30, 31 and 34 in the PST-16 system (high-impact case)

including those to which the compromised loads are connected. For the relative rotor angle, only three generators from area C are depicted.

Figure 4 shows the significant destabilisation of the system caused by the attack. Initially, the attack has a minimal impact, noticeable only for a few seconds; a slight oscillation between the areas is observed, but the system manages to confine frequency variations and appears stable. However, by $t = 15$ s, area C begins to diverge from the other two areas. The frequency at bus C10, with generation connected,

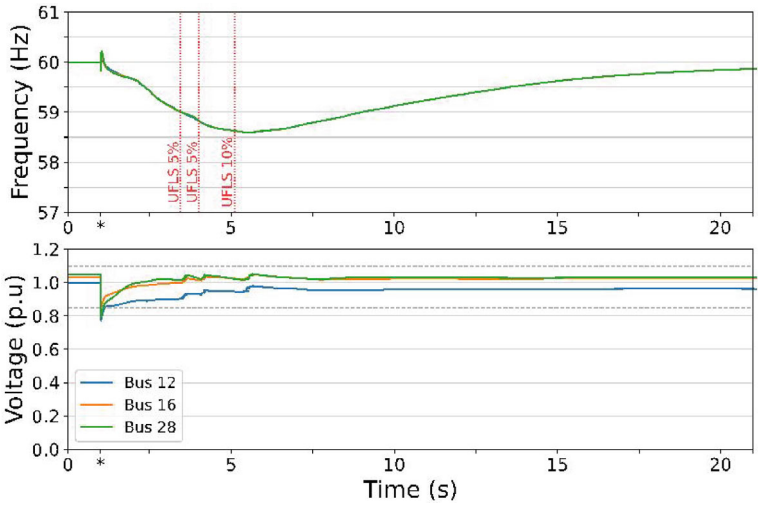

Fig. 5 Frequency and voltages when attacking 500 k bots in loads 12, 16 and 28 in the IEEE 39-Bus system (high-impact case)

suddenly drops to 46 Hz around $t = 18.5$ s. These frequency variations approximately 12 seconds after the attack are attributed to the loss of rotor angle stability in the system.

The middle plot in Fig. 4 clearly illustrates the immediate and significant impact of the attack on the voltages in area C. It is important to note that, before the attack, the system was already operating under peak demand conditions, with area C reliant on power imports from the other two areas. The voltages at the attacked buses drop significantly, nearing the threshold set for the tripping of undervoltage protections. However, due to the increased demand caused by the attack, the system loses rotor angle stability and subsequently experiences voltage collapse. The bottom plot of Fig. 4 shows that the rotor angles of the generators in area C begin to diverge from the reference generator after some initial oscillations. Thus, the system first encounters a rotor angle stability issue, which then leads to voltage collapse.

As voltages drop below 0.85 p.u for more than 10 s (Fig. 4), undervoltage protections begin to trip, disconnecting loads from the system. The activation of these protections, along with Under-Frequency Load Shedding (UFLS) and Over-Frequency Generator Rejection (OFGR) protections, are the primary causes of the oscillations observed in the 15–20 s interval. Following the activation of these protections, the system appears to recover by t = 20 s, albeit with rather low voltage levels (e.g., at Bus C10). By this time, nearly 2.9 GW of generation has been disconnected from the system due to the OFGR scheme. The impact could vary if additional protections were implemented (e.g., distance protection with or without out-of-step protection). Despite the increased demand caused by the attack, the system eventually ends up with approximately 3 GW less demand than before the attack (around a 20% decrease) due to load disconnections (UFLS and undervoltage protections).

This indicates that not only the extraordinary demand caused by the attack had to be disconnected, but additional loads also had to be shed to recover the system.

Similar to Fig. 4, Fig. 5 plots the frequency and voltages when 500 k bots are compromised in loads 12, 16 and 28 in the IEEE 39-Bus system, which constitutes a high-impact US39 scenario.

In this case, the immediate impact of the attack on the system's frequency and voltages is significant. The frequency drops by 1 Hz in approximately two seconds. Below 59 Hz, the UFLS scheme begins to actuate, as detailed in Table 2. This mitigates the frequency drop; only when it reaches approximately 58.6 Hz does the system start to increase the frequency. However, the recovery is slow. The system manages to keep all voltages within limits, so the UFLS protections are the only ones activated. These protections shed about 1.1 GW of loads across the system. Despite this, by the end of the simulation, the total system demand increases by 76 MW compared to the demand before the attack (approximately a 1.2% increase). This means that the amount of demand disconnected is roughly equivalent to the demand increase caused by the MaDIoT attack. However, it must be noted that the shedding would also affect legitimate loads, as UFLS protections do not differentiate between legitimate and compromised loads. Compared to the EU-C case analysed in Fig. 4, the relative impact is smaller, as the system manages to maintain its stability.

Therefore, although success ratios suggest that any attack compromising any three buses in the IEEE 39-Bus system may be successful, system dynamics results suggest its impact could be relatively low, proportional to the magnitude of the attack. In contrast, destabilising the PST-16 system is more challenging due to its larger size and greater generation resources to counter the effects of the attack; however, as discussed, a successful attack can significantly impact system stability, leading to partial disconnection of loads and generation which would also have economic effects.

The simulation results also highlight the different types of impact that MaDIoT attacks can have on grids that differ significantly. In the PST-16 system, the attack mainly affects rotor angle instability in area C and voltages, whereas in the IEEE 39-Bus system, the main impact is on frequency, driven by the inertia of generation in the model.

It is important to note that these results correspond to a worst-case scenario where demand is high and the attack targets only three closely located electrical nodes. The success ratio and impact of the attack are expected to be lower when the attack is distributed across a greater number of nodes (while maintaining the same botnet size), when demand is low (as more line capacity is available and the relative attack size per botnet is smaller), or when distant nodes are affected (e.g., one node per area in the PST-16 model). Both the size and location of the attack influence the system's survival, determining whether the attack can destabilise or not the power system. For instance, while distributing the attacks across different locations may reduce frequency-stability issues, it could exacerbate voltage-stability problems.

4 Potential Countermeasures

While completely eradicating the risk of a MaDIoT-type attack is unfeasible, implementing certain measures might substantially reduce its likelihood or, at least, mitigate its negative effects.

Enhancing the security of IoT devices fundamentally starts with their design. Consumer-level IoT products often lack substantial security features, a problem exacerbated by the general users' insufficient understanding of effective cybersecurity practices necessary for device protection [2].

In 2024, the European Cybersecurity Certification scheme (EUCC) [14] in Europe introduced baseline criteria for certifying devices from a cybersecurity perspective. This encompasses adherence to global standards like the Common Criteria for Information Technology Security Evaluation (ISO 15408), appointing an independent accreditation entity, ensuring that certification holders can identify and report security vulnerabilities, having well-defined procedures for managing and disclosing vulnerabilities, and establishing a system of penalties for noncompliance with security requirements.

To reduce the likelihood of being targeted in a MaDIoT attack, software and firmware updates on IoT devices must be verifiable through cryptographic means and allow for roll-back updates if needed. Implementing user authentication and role-based access control is essential for IoT devices, alongside data encryption whenever feasible.

Since Distribution System Operator (DSO)s manage the systems in which high-wattage IoT devices are predominantly connected, they should aim to develop and deploy intrusion detection and prevention systems that utilise cutting-edge techniques and technologies [28]. These may include deep learning [39], data-driven algorithms [25], edge computing [36] or preventive algorithms designed to prevent line failures [38]. Previous research has also recommended mitigation strategies such as cyber-resilient economic dispatch [9], the use of Stackelberg games for system reconfiguration [27], or implementing adaptive protections capable of identifying and counteracting attacks [6].

Moreover, it is crucial for DSOs, TSOs and other stakeholders, such as DER operators, to collaborate to enhance systemic resilience and reduce the impact of attacks. This collaboration relies on comprehensive real-time data sharing and a coordinated response to foster collective situational awareness and mitigate the risk of cascading failures. In this context, European regulations are progressively adapting to promote initiatives for information exchange and communication of cyber incidents, notably through the Network and Information Security 2 (NIS2) Directive [10]. Specifically addressing the electricity sector, the Network Code on Cybersecurity [11] (adopted in 2024) outlines baseline cybersecurity requirements, cross-border risk management strategies, cybersecurity controls, a system for sharing cybersecurity information, and sets out roles and responsibilities for involved parties, among other provisions.

5 Conclusions

The proliferation of high-wattage IoT devices at the consumer level introduces a novel attack vector, as these devices are distributed across numerous nodes within power systems. Understanding the potential impact of MaDIoT attacks on various systems under different conditions is crucial as the prevalence of these devices increases.

This chapter has examined and compared the effects of MaDIoT attacks on two models: the PST-16, which is a simplified European model, and the IEEE 39-Bus model, representing New England's power system. The study found that attack success rates vary widely depending on the targeted model. For the IEEE 39-Bus system, success rates reached up to 100%, while for the PST-16 system, the maximum success rate was around 30%. Nevertheless, further analysis of scenarios with high impact revealed that a higher success rate does not necessarily equate to a greater impact. The PST-16 system, which is larger and has more resources, can better accommodate the increased load from an attack. Still, a severe attack on this system could culminate in a blackout affecting 20% of the initial demand, having an impact exceeding the attack itself. On the other hand, in the IEEE 39-Bus system, the high-impact scenario assessed showed an impact matching the magnitude of the attack.

One significant limitation of this type of studies is the omission of the dynamics and protection mechanisms of large electricity distribution systems linked to transmission networks. To overcome this, it would be essential to create a combined model of transmission and distribution systems, which would demand considerable computational power. Future studies should explore MaDIoT attacks while taking into account both the transmission and distribution systems. Furthermore, integrating automatic or manually prompted operator actions, like re-dispatching to avert line overloads and the resulting cascading failures, offers another promising research line.

Acknowledgements 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 those of the author(s) only and do not necessarily reflect those of the European Union or CINEA.

References

1. Samrat Acharya, Yury Dvorkin, and Ramesh Karri. Public plug-in electric vehicles+ grid data: Is a new cyberattack vector viable? *IEEE Transactions on Smart Grid*, 11(6):5099–5113, 2020.
2. Omar Alrawi, Chaz Lever, Manos Antonakakis, and Fabian Monrose. SoK: Security evaluation of home-based IoT deployments. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1362–1380, 2019.
3. Sajjad Amini, Fabio Pasqualetti, and Hamed Mohsenian-Rad. Dynamic load altering attacks against power system stability: Attack models and protection schemes. *IEEE Transactions on Smart Grid*, 9(4):2862–2872, 2018.

4. Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. Understanding the mirai botnet. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 1093–1110, Vancouver, BC, August 2017. USENIX Association.
5. C. Arderne, C. Zorn, C. Nicolas, and E. E. Koks. Predictive mapping of the global power system using open data. *Scientific Data*, 7(1):19, 2020.
6. Anjana Balabhaskara, Sunandan Adhikary, Ipsita Koley, Soumyajit Dey, and Ashish R Hota. Adaptive protection of power grids against stealthy load alterations. *2024 ACM/IEEE 15th International Conference on Cyber-Physical Systems (ICCPS)*, 00:285–286, 2024.
7. Adam Borys, Abu Kamruzzaman, Hasnain Nizam Thakur, Joseph C. Brickley, Md L. Ali, and Kutub Thakur. An evaluation of iot ddos cryptojacking malware and mirai botnet. In *2022 IEEE World AI IoT Congress (AIIoT)*, pages 725–729, 2022.
8. Clementina Bruno, Luca Guidi, Azahara Lorite-Espejo, and Daniela Pestonesi. Assessing a potential cyberattack on the Italian electric system. *IEEE Security & Privacy*, 13(5):42–51, 2015.
9. Zhongda Chu, Subhash Lakshminarayana, Balarko Chaudhuri, and Fei Teng. Mitigating load-altering attacks against power grids using cyber-resilient economic dispatch. *IEEE Transactions on Smart Grid*, 14(4):3164–3175, 2023.
10. European Commission. Eu directive 2022/2555 (nis 2 directive), December 2022.
11. European Commission. Eu electricity supply—sector-specific rules on cybersecurity (network code), October 2023.
12. Adrian Dabrowski, Johanna Ullrich, and Edgar R. Weippl. 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*, pages 303–314. ACM, 2017.
13. eFORT Project. D2.2 Cascading effects analysis and related actions to increase resilience, August 2025.
14. European Union Agency for Cybersecurity (ENISA). Cybersecurity—security requirements for ICT product certification, October 2023.
15. Maldon Patrice Goodridge, Subhash Lakshminarayana, and Christopher Few. Analysis of load-altering attacks against power grids: A rare-event sampling approach. In *2022 17th International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, pages 1–6. IEEE, 2022.
16. Maldon Patrice Goodridge, Subhash Lakshminarayana, and Alessandro Zocca. Uncovering Load-Altering Attacks Against N-1 Secure Power Grids: A Rare-Event Sampling Approach. *IEEE Transactions on Power Systems*, pages 1–13, 2024.
17. Maldon Patrice Goodridge, Alessandro Zocca, and Subhash Lakshminarayana. Analysis of cascading failures due to dynamic load-altering attacks. In *14th IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (IEEE SmartGridComm 2023)*, 2023.
18. Hassan Haes Alhelou, Mohamad Esmail Hamedani Golshan, Takawira Cuthbert Njenda, and Nikos D. Hatziargyriou. An Overview of UFLS in Conventional, Modern, and Future Smart Power Systems: Challenges and Opportunities. *Electric Power Systems Research*, 179:106054, 2020.
19. Bing Huang, Alvaro A Cardenas, and Ross Baldick. Not everything is dark and gloomy: Power grid protections against iot demand attacks. In *28th USENIX security symposium (USENIX Security 19)*, pages 1115–1132, 2019.
20. Anastasis Keliris, Charalambos Konstantinou, Marios Sazos, and Michail Maniatakos. Open source intelligence for energy sector cyberattacks. In Dimitris Gritzalis, Marianthi Theocharidou, and George Stergiopoulos, editors, *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*, pages 261–281. Springer International Publishing, 2019.

21. Heetae Kim, David Olave-Rojas, Eduardo Alvarez Miranda, and Seung-Woo Son. In-depth data on the network structure and hourly activity of the central chilean power grid. *Scientific Data*, 5(1):180209, 2018.
22. Pavel Kozak, Ivo Klaban, and Tomáš Slajs. Industroyer cyber-attacks on Ukraine's critical infrastructure. In *2023 International Conference on Military Technologies (ICMT)*, pages 1–6, 2023.
23. Subhash Lakshminarayana, Sondipon Adhikari, and Carsten Maple. Analysis of IoT-Based Load Altering Attacks Against Power Grids Using the Theory of Second-Order Dynamical Systems. *IEEE Transactions on Smart Grid*, 12(5):4415–4425, September 2021.
24. Subhash Lakshminarayana, Yexiang Chen, Carsten Maple, Andrew Larkins, Daryl Flack, Christopher Few, Kenny Awuson-David, and Anurag K. Srivastava. Threats to power grid operations from the demand-side response ecosystem: A comprehensive overview. *IEEE Industrial Electronics Magazine*, PP(99):2–12, 2025.
25. Subhash Lakshminarayana, Juan Ospina, and Charalambos Konstantinou. Load-Altering Attacks Against Power Grids Under COVID-19 Low-Inertia Conditions. *IEEE Open Access Journal of Power and Energy*, 9:226–240, 2022.
26. Mahrukh Mahrukh and Mini Shaji Thomas. Load Altering Attacks- a Review of Impact and Mitigation Strategies. In *2023 International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON)*, pages 397–402, May 2023.
27. Sajjad Maleki, Subhash Lakshminarayana, Charalambos Konstantinou, and E Veronica Belmaga. Distribution system reconfiguration to mitigate load altering attacks via stackelberg games. *arXiv*, 2024.
28. Sajjad Maleki, Shijie Pan, Subhash Lakshminarayana, and Charalambos Konstantinou. Survey of load-altering attacks against power grids: Attack impact, detection and mitigation. *arXiv*, 2024.
29. Wided Medjroubi, Ulf Philipp Müller, Malte Scharf, Carsten Matke, and David Kleinhans. Open data in power grid modelling: New approaches towards transparent grid models. *Energy Reports*, 3:14–21, 2017.
30. Amir-Hamed Mohsenian-Rad and Alberto Leon-Garcia. Distributed internet-based load altering attacks against smart power grids. *IEEE Transactions on Smart Grid*, 2(4):667–674, 2011.
31. Afroz Mokarim, Giovanni Battista Gaggero, and Mario Marchese. Evaluation of the impact of cyber-attacks against electric vehicle charging stations in a low voltage distribution grid. In *14th IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (IEEE SmartGridComm 2023)*, 2023.
32. Juan Ospina, Xiaorui Liu, Charalambos Konstantinou, and Yury Dvorkin. On the Feasibility of Load-Changing Attacks in Power Systems During the COVID-19 Pandemic. *IEEE Access*, 9:2545–2563, 2021.
33. Néstor Rodríguez-Pérez, Javier Matanza Domingo, Lukas Sigrist, Jose Luis Rueda Torres, and Gregorio López López. Confronting the threat: Analysis of the impact of madiot attacks in two power system models. *Energies*, 16(23):7732, 2023.
34. José Luis Rueda, Jaime C. Cepeda, István Erlich, Abdul W. Korai, and Francisco M. Gonzalez-Longatt. Probabilistic approach for risk evaluation of oscillatory stability in power systems. In Francisco M. Gonzalez-Longatt and José Luis Rueda, editors, *PowerFactory Applications for Power System Analysis, Power Systems*, pages 249–266. Springer International Publishing, 2014.
35. Tohid Shekari, Alvaro A Cardenas, and Raheem Beyah. Madiot 2.0: Modern high-wattage iot botnet attacks and defenses. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 3539–3556, 2022.
36. Bibek Shrestha and Hui Lin. Data-centric edge computing to defend power grids against iot-based attacks. *Computer*, 53(5):35–43, 2020.
37. Saleh Soltan, Prateek Mittal, and H Vincent Poor. Blackiot: Iot botnet of high wattage devices can disrupt the power grid. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 15–32, 2018.

38. Saleh Soltan, Prateek Mittal, and H. Vincent Poor. Protecting the grid against MAD attacks. *IEEE Transactions on Network Science and Engineering*, 7(3):1310–1326, 2020.
39. Lizhi Wang, Lynn Pepin, Yan Li, Fei Miao, Amir Herzberg, and Peng Zhang. Securing power distribution grid against power botnet attacks. In *2019 IEEE Power & Energy Society General Meeting (PESGM)*, pages 1–5, 2019.
40. Christos Xenofontos, Ioannis Zografopoulos, Charalambos Konstantinou, Alireza Jolfaei, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo. Consumer, commercial, and industrial IoT (in)security: Attack taxonomy and case studies. *IEEE Internet of Things Journal*, 9(1):199–221, 2022.
41. Ioannis Zografopoulos, Juan Ospina, Xiaorui Liu, and Charalambos Konstantinou. Cyberphysical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access*, 9:29775–29818, 2021.