Preprint: to appear at ACSAC 2017, December 4-8 2017

Grid Shock: Coordinated Load-Changing Attacks on Power Grids

The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well

Adrian Dabrowski
SBA Research
Wien, Austria
adabrowski@sba-research.org

Johanna Ullrich
SBA Research
Wien, Austria
jullrich@sba-research.org

Edgar R. Weippl
SBA Research
Wien, Austria
eweippl@sba-research.org

ABSTRACT

Electric power grids are among the largest human-made control structures and are considered as critical infrastructure due to their importance for daily life. When operating a power grid, providers have to continuously maintain a balance between supply (i.e., production in power plants) and demand (i.e., power consumption) to keep the power grid's nominal frequency of 50 Hz or alternatively 60 Hz. Power consumption is forecast by elaborated models including multiple parameters like weather, season, and time of the day; they are based on the premise of many small consumers averaging out their energy consumption spikes.

In this paper, we develop attacks violating this assumption, investigate their impact on power grid operation, and assess their feasibility for today's adversaries. In our scenario, an adversary builds (or rents) a botnet of zombie computers and modulates their power consumption, e.g., by utilizing CPU, GPU, hard disks, screen brightness, and laser printers in a coordinated way over the Internet. Outperforming the grid's countervailing mechanisms in time, the grid is pushed into unstable states triggering automated load shedding or tie-line tripping. We show that an adversary does not have to rely on smart grid features to modulate power consumption given that an adequate communication infrastructure for striking the (legacy) power grid is currently nearly omnipresent: the Internet to whom more and more power-consuming devices are connected.

Our simulations estimate that between 2.5 and 9.8 million infections are sufficient to attack the European synchronous grid – depending on the mix of infected devices, the current mix of active power plant types, and the current overall produced power. However, the herein described attack mechanisms are not limited to the European grid.

ACM Reference Format:
Adrian Dabrowski, Johanna Ullrich, and Edgar R. Weippl. 2017. Grid Shock: Coordinated Load-Changing Attacks on Power Grids: The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well. In *2017 Annual Computer Security Applications Conference.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3134600.3134639

ACSAC 2017, December 4–8, 2017, San Juan, PR, USA

ACM ISBN 978-1-4503-5345-8/17/12…$15.00
https://doi.org/10.1145/3134600.3134639

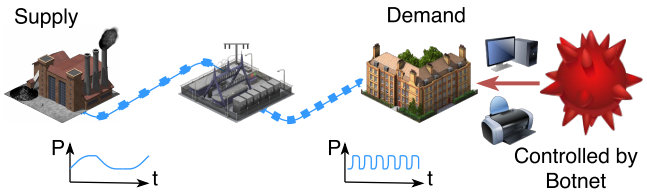


Figure 1: Visualization of Attacks 1 and 2: The botnet can modulate the power demand much faster than power plants can react.

1 INTRODUCTION

Electric power grids are among the largest human-made structures and by far the most important for technology-dependent societies. Without electricity, life as we know it would not function; there would be breakdowns in water and food supply, transport, medical aid, and communication infrastructures. For this reason, power grids are considered critical infrastructures, and operated with a high level of care to provide qualitative service, i.e., constant voltage and frequency. At the same time, power grids are legacy systems pre-dating modern telecommunication networks — such as the Internet — by decades, as is reflected in its structure: Electricity consumers are predominantly uncontrolled, i.e., consuming electric power whenever they need thereby causing fluctuations in consumption. However, on a macro scale fluctuations average out: for each consumer turning a light bulb off there is most likely another one turning the light on. Energy suppliers have developed sophisticated models that reliably forecast power demand in dependence of time of the day, week day, season and many other parameters allowing (centralized) power plants to trace actual consumption best possible in order to keep the equilibrium of production and consumption; the remaining gap is placed at disposal by so called *control reserves* (*spinning reserve* in the U.S.), i.e., the activation of power plants in stand-by.

Power grids around the globe currently undergo substantial modifications commonly summarized under the term *smart grid*, and the included concepts put an end to the strict separation of controlled production and uncontrolled consumption. On the one hand, renewables like wind turbines and photovoltaics provide electric energy in dependence of weather conditions and are thus only to a certain extent predictable, not to mention arbitrarily controllable. On the other hand, demand-side management aims to shift certain types of consumption, e.g., heating or cooling, in time. Synchronized over a communication channel, energy should then be consumed at the time of production by renewables. Due to such remote control of high amounts of power consumption, the smart grid is considered to be vulnerable to direct cyber attacks aiming to destabilize the system [28, 64].

In this paper, we show that an adversary does not have to rely on explicit (or future) smart grid features to modulate power consumptions, as the communication infrastructure to attack the *legacy grid* is already available: the Internet. An adversary might compromise a large number of Internet-facing power-drawing devices, e.g., computers, TVs, or thermostats controlling heating systems, and modulate their power consumption in a coordinated way (Figure 1). As these fluctuations are at a large scale, fast and unpredictable, power plants are not able to trace power consumption any more causing an imbalance of production and consumption and eventually load-shedding, disconnection of power plants, disconnection of transmission lines, or a split of one synchronous power grid into multiple areas. Our attack benefits from the fact that the power grid is substantially slower in reaction than information technology, and will become even more vulnerable in the future, as controllable power consumption (with a potentially low level of security protection) increases due to the spread of the Internet-of-Things (IoT).

In this paper, we focus primarily on the synchronous grid of Continental Europe (also known as UCTE grid) as it is the largest of its kind spanning over 23 countries, including large parts of Europe, North Africa as well as Turkey, and cite the respective UCTE/ENTSO-E policies. While terminology and details might differ in other synchronous grids, e.g., in the United States, we want to stress that the general principles, attacks, and conclusions apply to AC power grids all over the world.

The paper is structured as follows: Section 2 provides background on today's power grids from an engineering perspective. Section 3 describes our attack scenarios and the anatomy of the adversary's botnet for these attacks. It goes without saying that such an attack can ethically never be tested on a real power grid. Thus, we measure the capabilities for load modulation of a zombie and its peripherals in Section 4 and use simulations to predict the impact of large load changes on the power grid in Section 5. In Section 6, we combine the gained results into multiple scenarios and assess the number of infections needed considering parameters like time of the day, season, etc. Section 7 discusses related work, and Section 8 concludes the paper.

2 BACKGROUND

This section provides background on the power grid from an engineering perspective and an introduction into control theory, discussing feedback loops and resonance frequencies.

2.1 Producer-Consumer Equilibrium

Electric power cannot be stored at large scale, i.e., must be generated and consumed at the same time. In consequence, the challenge when operating a power grid is to maintain an equilibrium of electric power supplied by power plants and power consumed by electric loads. Apart from a few consumers with extraordinary high consumption — e.g., aluminum foundries and steel mills — are uncontrolled, i.e., they turn their power consumption on and off whenever they need or feel to. Thus, keeping a balance between supply and demand has become the suppliers' tasks – their power plants' production has to trace current consumption.

Table 1: Emergency routines in case of under-frequency in Germany [60, p65] similar to the ENTSO-E policies [55, p26]

	Frequency	*Action*
1	49.8 Hz	Alerting, activation of plants, shedding of pumps
2	49.0 Hz	Load-shedding of 10-15% of total load
3	48.7 Hz	Load-shedding of further 10-15% of total load
4	48.4 Hz	Load-shedding of further 15-25% of total load
5	47.5 Hz	Disconnection of all power plants

Scheduling power plants in order to deliver enough electric power at all times is a non-trivial task, which is fulfilled by applying a two-fold approach: elaborated models were developed describing overall power consumption in dependence of type of load (commercial or residential), time of the day, week day, season, weather and many parameters more allowing a quite accurate prediction of power consumption. Secondly, the remaining gap is handled by control reserve, i.e., additional power production capacities that are kept in stand-by and activated if needed [55, 56].

If production and consumption are imbalanced, frequency deviates from its nominal value f_0 (in Europe $f_0 = 50\,Hz$, in the US $f_0 = 60\,Hz$): If there is more supply than demand, the frequency increases; if there is less supply than demand, the frequency decreases. This happens, because large spinning turbines produce the vast majority of electricity in today's power grids and store rotational energy, i.e., kinetic energy due to rotation. In case of over-supply, conservation of energy produces additional torque on the generator's spinning axis and accelerates the turbine, i.e., energy supplied to the turbine is converted into mechanical energy instead of electric energy. As the turbine speed and the grid frequency are rigidly coupled, the grid frequency increases as well. Vice versa, higher power consumption slows down the generator due to a counter-torque on the spinning axis and lowers the output frequency. In fact, a grid's frequency deviation $\Delta f = f - f_0$ with f being the current value is used as the primary indicator for an imbalance in demand and supply and triggers the control reserve, bringing the power grid back into equilibrium.

Due to minor imbalances, frequency is fluctuating around the nominal value even under normal operational conditions due to minor imbalances. If deviations are larger than a pre-defined threshold, emergency routines are performed to bring the power grid back into balance. For example, German regulations define a five-step plan for load-shedding in case frequency drops under certain values [20], see Table 1. These routines protect turbines and other physical devices from damage, e.g., due to resonant frequencies.

2.2 Continental Synchronous Grid Area

Historically, power grids were "islands" with a single power generator which were then stepwise integrated into larger grids for reasons of reliability and costs. Also, consumption spikes are likely to be handled better by multiple power plants. Cheaper (but typically less controllable) power plants are able to produce the base load, more expensive (and dynamic and more controllable) plants handle peak loads. Nowadays, networks are operated on a national, even continental level.

A parallel operation of generators requires coherence, i.e., operation at exactly the same frequency and in phase, leading to *synchronous grid areas*. Misalignment, e.g., in extreme case, one generator is at the positive peak of a sine, while another is at the negative peak, will result in major short-circuit like currents potentially leading to fire or physical destruction. The biggest synchronous area is the *continental synchronous grid area*, also called *synchronous grid of continental Europe*, comprising most of the European Union, Switzerland, many Balkan countries as well as three North African states; there are also plans for further expansion. This implies that the sine at a power plug in Athens, Greece is the same as another one obtained in Lisbon, Portugal or Tunis, Tunisia. It has a total production capacity of more than 600 GW and a nominal frequency of 50 Hz.

The continental synchronous grid is organizationally split into control zones which are led by a transmission system operator (TSO) [57]. Control zones are the size of a smaller European country like Austria or Switzerland and mostly follow national borders or geographical landmarks. Larger countries are split into multiple control zones, e.g., Germany has four. Control zones have connections with adjacent zones via transmission lines. However, their capacity covers only a fraction of the power consumption and is mostly meant for the compensation of power imbalances.

TSOs are unified in the *European Network of Transmission System Operators for Electricity (ENTSO-E)* which defines regulations on how to jointly operate the grid. Among these regulations, ENTSO-E specifies the provision and application of control reserve in three steps to balance production and consumption, namely *primary*, *secondary* and *tertiary control* as described in the following paragraphs [55, 56].

On the physical level, before any control system kicks in, the rotational energy stored in the spinning turbines stabilizes the frequency to a certain extent.

Primary control is activated within seconds after an incident – i.e., frequency deviation is exceeding a certain threshold – and the first to actively react to a power imbalance. Primary control is applied in proportion to the frequency deviation, i.e., $K \cdot (f - f_0)$, and does not bring the frequency back to nominal, it rather stabilizes the frequency at a stationary value. In practice, a control system (governor) within the power plant observes the grid frequency and decides whether to increase or decrease power output. In primary control, all generators in the synchronous area participate simultaneously.

Secondary control is activated after 30 seconds and takes some minutes until full activation. Its task is to replace primary control and return the frequency to its nominal value. This type of control reserve has to be carried out by the TSO whose control zone is imbalanced. The respective zone is recognized by the *Area Control Error (ACE)* which is calculated for each zone according to Equation 1.

$$ACE = P_{measured} - P_{planned} + K \cdot (f - f_0) \quad (1)$$

$P_{measured}$ is the sum of measured power transfers on transmission lines, $P_{planned}$ the sum of planned power exchanges with adjacent zones, and K is the network power frequency characteristic of the primary control. If all produced primary control is exported into other control zones, ACE is zero and secondary control remains inactive in the respective area. If the imbalance occurred in its own zone, a TSO's ACE differs from zero and secondary control is initiated.

Tertiary control frees up resources from primary and secondary control after their sustained activation. In contrast to the prior two control mechanisms, tertiary control also allows for manual intervention by the TSO.

2.3 Feedback Loops and Resonance Frequencies

Control theory distinguishes open-loop systems from closed-looped systems. In an open-loop system, the controller aims to achieve the output reaching a set point without monitoring the output; in consequence, accurate system models are necessary while still not being able to adapt in case of unexpected disturbances. Meanwhile, closed-looped systems are measuring the system's output y (e.g., via a sensor), comparing it with the set point w and reacting upon the control deviation $e = w - y$. The output counteracts the deviation from the set point; this behavior is also known as *negative feedback*. This way, a disturbance influencing the output is measured, and counteracted.

Closed-loop controls frequently incorporate delays, as it takes time to measure, calculate and physically react, e.g., when accelerating physical masses. This implies that feedback is not instantaneous and the system might swing when excited at certain frequencies. A signal's phase shift is dependent on the delay, and a shift of 180 degrees changes negative feedback into positive. The feedback does not counteract the deviation anymore, but rather reinforces it, leading to self excitation and an increasing amplitude. Such a situation is potentially damaging and thus to be avoided; as a rule of thumb, the control should be faster than the monitored physical system.

Linear controllers exhibit proportional (P), integral (I) or derivate (D) behavior as well as respective combinations: Proportional control amplifies the control deviation e by a constant factor, integral control integrates the control deviation e over time, and derivate control differentiates. Proportional control shows permanent control offset, i.e., the output differs from its intended value by some offset. If the latter is undesired, proportional control has to be combined with integral behavior, forming a PI controller.

Power imbalance influences a grid's frequency; there are multiple controls reacting on frequency shifts, i.e, closed-loop controls [55, 56]. Load, in particular from induction engines, increases/decreases with frequency and thereby automatically reduces power imbalance. This effect is known as *self regulation of loads*, and is assumed to be 1%/Hz in the continental synchronous grid. In addition, there are the operational measures of primary, secondary and tertiary control, rescheduling power production facilities. Primary control is specified to show proportional behavior, i.e., it cannot return frequency to its nominal value of 50 Hz, whereas, secondary is a combined proportional, integral (PI) controller returning the frequency to its nominal value. Both show delays, i.e., primary control reacts typically within a few seconds and secondary control within 30 seconds, replacing primary control, vulnerable to self-excitation. Since tertiary control can be manually scheduled, its behavior cannot be specified in a similar manner.

3 THREAT SCENARIO

For our attacks, we assume a botnet controlling a high amount of computers and their peripherals. Each bot can trivially modulate the power consumption of the CPU, the GPU (Graphics Processing Unit), hard drives, and the screen backlight. Laser printers — an peripheral common — are also large power consumers due to the high temperatures used in their fusion units. In some cases, the botnet might find other locally accessible Internet-of-Things (IoT) devices on the network, which often incorporate less security protection or default passwords, for load modulation.

While each of the devices only contributes several hundred to thousands Watt, their effect multiplies by the botnet producing a large leverage on power consumption within the grid. It can modulate this power consumption in a coordinated fashion and in a sub-second range. This way, the adversary aims to negatively affect the power grid.

In the first part of this section, we introduce different kinds of load modulation attacks. In the second part, we specify the botnet in detail.

3.1 Attack Types

We consider an attack successful if of the following effects occurs:

- Customers or power plants become disconnected from the grid, e.g., by automatic load shedding due to under-frequency or frequency protection protocols for power plants.
- Transmission lines (tie lines) become disconnected, e.g., by overload-protections, or adjacent control zones become disconnected.

Attack 1: Static Load Attack. The attacker increases the power consumption of all bots to the maximum; this action shifts power generation and consumption out of the equilibrium by increasing the consumption faster than the producers can react. Just a brief violation of the frequency thresholds, triggers load shedding (see Table 1), i.e., the automatic disconnection of parts of the grid. To enlarge the amplitude of load changes, the adversary might piggyback their attack on power spikes and oscillations that usually happen in the grid [23, 26]. This attack targets the *primary control*.

Attack 2: Dynamic Load Attack. Closed-loop control systems with negative feedback and non-zero latency tend to over- and undershoot when reacting to changes. This effect can be used to increase the amplitude of Attack 1 by measuring the reaction times and modulate the power consumption so that the highest production peak is met with a low modulated demand and vice versa. Since the attacker is reacting on the grid, s/he needs a return channel to measure the state of the grid,i.e., the current frequency. In particular, the adversary increases the load to the maximum and waits for the full primary control to be activated; then, decrease the load to the minimum wait for the primary control to deactivate, and so on. This attack targets the behavior of the primary control.

Eventually, the attacker might find a resonant frequency that leads to a much larger frequency swing than appropriate for the load change. The ENTSO-E synchronous area is known to have eigenfrequencies that manifest in several post-incident reports [18],[54, p.77],[26, p.3].

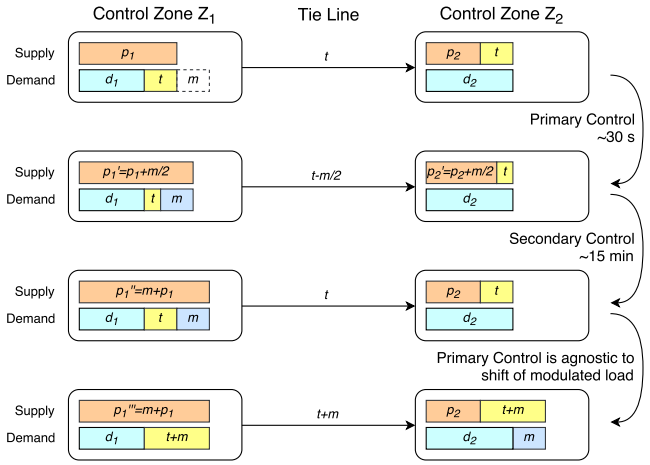


Figure 2: Simplified schematic of attack 3

Attack 3: Inter-Zone Attacks. This attack aims to trip tie lines that are connecting areas by putting large loads on them. A naïve way to increase the load on a tie line is to find a line that is operating near the maximum and increase power consumption in the target area of that transfer. Some TSO's publish their line state on the web [1]. Even though they are delayed in time, it gives an attacker a good insight on when the line is usually loaded the most. However, since primary control detects the increase in load, a part of the additional load will be produced in the targeted area (control zone), leaving only the rest to the tie line.

Reducing power consumption in one area while simultaneously increasing it in the target area would further increase the burden on the line, but decreasing load (of mostly idle electronic appliances) is only possible in rare cases. However, the attacker can wait for the automatic secondary control to equalize for changes between both zones to meet scheduled transfers; then change the load modulation between zones to achieve the same effect.

Figure 2 depicts the scheme step by step. First, load is added to Zone Z_1, effectively lowering the transmission on the line (in- and outgoing transmissions cancel each other out). However, secondary control will compensate for the overproduction in one zone and the underproduction in another and adjust output power accordingly to meet the scheduled transfer on the line. The attacker waits until this happens and inverts the modulation between the zones, recreating the imbalance with reversed sign, again triggering substantial compensation currents over transmission lines. For simplicity, we assume $m_1 \approx m_2 = m$, so that an extra of m is added to the transmission line. Since the total load of the grid does not change, the primary control will not kick in.

3.2 Anatomy of a Grid-Attacking Botnet

A botnet is a set of hijacked computers (called *bots* or *zombies*) on the Internet that is set up to to perform tasks on behalf of the botnet owner [46]. Among other, botnets gained infamous popularity by traffic-based denial-of-service attacks, mass-hacking, sending spam, spying on the computer owners, online fraud, mining cryptocurrencies, stealing secrets from presidential candidates, and infecting other computers. Some botnets operate for years until they

are detected. The following paragraphs provide details on how an adversary is able to built an adequate botnet for power-load attacks.

Acquisition. Prices of botnets vary depending on the country the zombies are placed in. A 2013 report [16], named USD 1,000 for 10,000 U.S.-based bots, and between USD 400 and USD 600 for European-based bots. Large botnets contain up to tens of million devices [43].

Synchronization. For power grid attacks, a timely communication structure is in order to coordinate precise load manipulations. Modern protocols such as NTP [33, 66] compensate for round-trip time, delivering sub-millisecond performance if allowed to run for extended periods of time [34].

Geographical Estimation. For our attacks, the botnet has to coarsely estimate the position of the zombie machines. For attacks 1 and 2 the granularity can be as low as the continent as central Europe is an interconnected supergrid. For attacks on the US grid, the granularity should be at least on state level as there are multiple synchronous grids. There are various ways to identify the geographical position of a bot:

- *GeoIP lookup:* Maxmind [32] and other databases provide at least a state/country level localization – even in the free version.
- *Wi-Fi localization:* Coarse location by BSSIDs of Wi-Fi access points is now a standard technique for mobile phones. Some stand-alone PCs certainly almost all notebooks come with a Wi-Fi receiver. Some databases are available free of charge [61].
- *Keyboard layout:* Malware such as the Conficker worm [10, 43] uses the keyboard layout to determine the country of the computer to avoid targeting the own country. This works on language-fragmented continents like Europe, but not in North America.

Frequency Measurement. Attack 2 and 3 (Section 3.1) benefit from the frequency feedback channel. In case the attacker and bot-master is sitting anywhere within the attacked grid, s/he can invest into a low-cost power grid frequency measurement unit, such as from open-source projects [11, 14], measuring the frequency at an ordinary power outlet. Since the frequency is identical in all parts of the network (until it breaks up), one measurement station is sufficient. Attacks on remote grids might approximate measurements by analyzing audio/microphone hum, or Webcam light flickering on target machines — similar to its use in multimedia forensics [12, 25]. Furthermore, some websites [15, 17, 21, 23, 38] offer live data for certain grids.

4 EVALUATION: POWER-MODULATION

To understand the attack and estimate the effects we have to answer two questions. First, to which amount can a bot zombie influence its power consumption and at which pace. Secondly, use simulations to predict the outcome of such a load attack on the power grid. The former is described in this section, the latter in Section 5.

In a lab experiment, we measured a bot's capability for software-driven load modulation. In a first step, we analyzed the dynamics of a PC's load increase/decrease in order to determine their capabilities

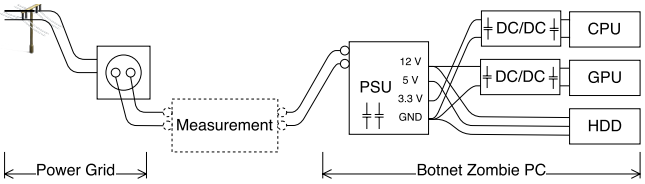


Figure 3: Model of botnet zombie and method of measurement

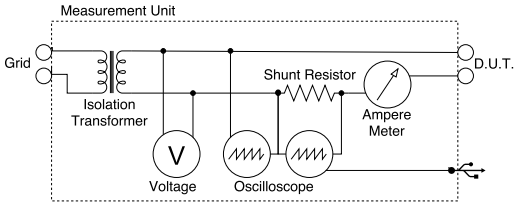


Figure 4: Measurement setup in detail

for fast load changes. Then, we categorized different types of devices that might become part of our attack and investigated the increase of load from an idle to a fully utilized state.

4.1 Electric Model of a Load-Altering PC

Since PCs and servers appear to have great potential for load control, we took a closer look and asked how fast they can modulate their power consumption.

The components of a PC (or Server) do not directly draw power from the mains. Instead, a series of power conversions takes place before reaching the relevant components, i.e., CPU, GPU and hard drive. Our model is depicted in Figure 3: We must assume that each conversion step through the power supply unit (PSU) and subsequent DC/DC converters incorporates power-stabilizing capacitors which will dampen the artificially produced load spikes. To measure the effective load amplitudes and times as dispensed to the grid, we had to measure at the power socket (Figure 4).

As a conservative assumption of an office PC, we chose an Intel Core2 Duo (Figure 5). For a high-end gaming PC we tested an Intel i7-6700 with an NVIDIA Geforce GTX 1070 graphics card (Figure 7). Both were connected with an LG 24" TFT screen which was measured separately (Figure 6). On Linux, we used command line tools `hdparm -t` for inducing stress to hard disks, `stress -c` for the CPU, and `glmemperf` for the GPU. On Windows, we used ZCPU for CPU stress and 3D Mark to measure the GPU.

As expected according to our model, the capacitors soften the steep current edges, especially in the low-end range. Thus, the PSU in the old office PC ramped up the consumption within 2-3 AC cycles, i.e., 40-60 ms. In contrast, the gaming PC can multiply its power consumption and the PSU ramps up the usage within a single AC cycle. Hard disk consumption turned out to be negligible: most of the power is used for the disk rotation which is independent from head movements.

Laser printers are without question the heaviest power consumers of all computer peripherals due to the high temperatures involved when fixating the toner to the paper. The fuser's surge current is a multiple of its already high power consumption (Figure

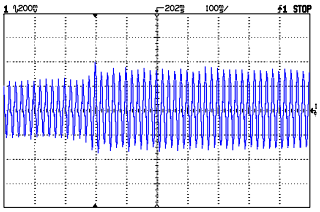


Figure 5: Example: low-end office PC. PSU ramps up power within 2-3 AC cycles

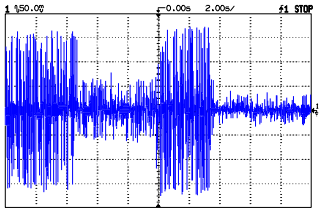


Figure 6: LG 24" TFT screen needs 8 s before going to sleep mode.

8a). In our setup with a small office/home office (SOHO) printer, the heat-up process started within a second when printing via USB, and several seconds when printing over the network. The high power usage continues for 8 seconds for the first page and 5 seconds for all following pages. On stand-by, the printer reheats the fuser every 35 seconds, until it goes to sleep mode after several minutes.

Screens can easily be turned on and off via software as operating systems offer power saving controls and appropriate APIs. As seen in Figure 6, the screen first displays a goodbye message (3 seconds), then goes into time-out mode (5 seconds) and finally to sleep.

These measurements (Table 2) give us a preliminary insight regarding the achievable dynamics of load changing attacks performed by a botnet. As expected, capacitors in the power conversion units smear the hard edges of artificially produced power spikes. However, even in the worst case (60 ms per slope) an attacker can achieve modulation frequencies up to 8 Hz.

4.2 Categorization of Load-Altering Appliances

The second part of this Section looks at the question on the amount of controllable load by PC components and commonly found IoT devices and their usage.

The last column of Table 2 compromises data from our own measurements, data sheets and PC power tutorials [9].

Since such an overview cannot depict the countless different models of hardware sold and installed around a world, its purpose is to estimate the impact of the attacks described above.

The Δ *Load* column denotes the margin of controllable power consumption, e.g., the difference between idle state and full utilization. For example, desktop hard disks (typ. 5,400 RPM) have a lower base power consumption than server hard disks (typ. 7,200 - 10,000 RPM), but the difference between access and non-access is small.

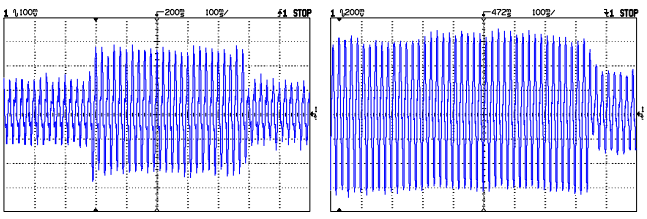
Table 2: Modulated load by device

Device	Type	Pwr Control Inc.	Pwr Control Dec.	Latency on	Latency off	Δ Load
CPU	Core2 Duo	●	○	20-60 ms	20-60 ms	35 W
	i3	●	○	20-60 ms	20-60 ms	55-73 W [9]
	i5	●	○	20-60 ms	20-60 ms	73-95 W [9]
	i7	●	○	20-60 ms	20-60 ms	77-95 W [9]
	i7-E	●	○	20-60 ms	20-60 ms	130-150 W [9]
GPU	Low-end	●	○	20-60 ms	20-60 ms	20-76 W [9]
	Mid-end	●	○	20-60 ms	20-60 ms	102-151 W [9]
	High-end	●	○	20-60 ms	20-60 ms	150-238 W [9]
	Top-end	●	○	20-60 ms	20-60 ms	201-297 W [9]
HDD		●	○	20-60 ms	20-60 ms	3-7 W [9]
Screen TFT	size dep.	●	●	1-5 s	5-10 s	60-100 W
Laser Printer	SOHO	●	○	1-3 s	5-10 s	800-1300 W
Smart Air Cond.		●	○	1-10 s		600-1000 W
Smart Thermostat	elec. Heating	●	○	1-10 s		1-15 kW
Smart Oven		●	○	1-10 s		2-3 kW
Smart Refrigerator		●	○	1-10 s		300-500 W
Smart Kettle		●	○	1-10 s		1000-1500 W

In contrast to other appliances, screens can easily reduce power without much side effects by going to sleep. Major operating systems offer unprivileged API or command line calls to accomplish that. Hard-disks can be sent to sleep as well (spin-down) but this typically needs administrator privileges. Furthermore regular background file system activity (book-keeping) will not make the effect lasting without putting the whole OS into sleep. Such a step withdraws the PC from the control of the botnet and is therefore not included.

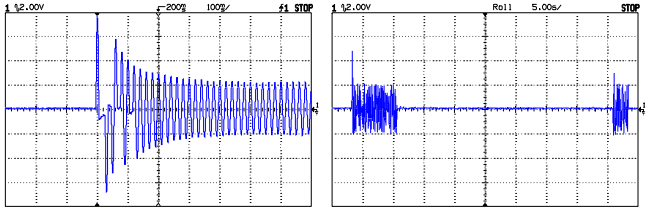
As for printers, we did not considered office printers as they are usually shared by multiple users. Thus, print jobs are sequentialized and power consumption would not multiply with the number of infections, as it is spread over time.

Internet-of-Things devices are included in our list although they are still rare. The exception are smart thermostats [2, 39, 50] being sold in the U.S since 2015 are increasingly[52], in total 20 million devices since 2013 (U.S. has 126 Mio. Households [49]). Such air conditioners [2, 7, 27]) and smart refrigerators [48] can be manipulated by changing the set-point temperature. Kitchen appliances such as smart ovens [47] and Wi-Fi-controlled water kettles [42] can also substantially draw power.



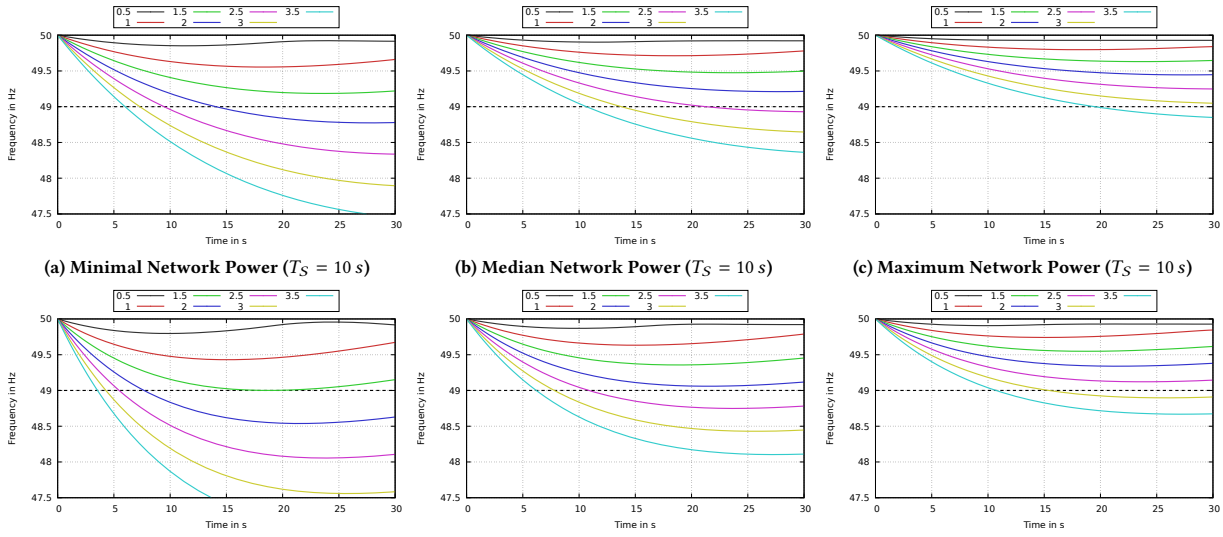
(a) Intel i7 ZCPU stress test **(b) 3D mark benchmark ending**

Figure 7: Gaming PC; the PSU ramps up the current within a single AC cycle to a multiple compared to idle usage.



(a) Heating the fuse unit peaks power at 20 A, before settling at 4.8 A = 1100 W **(b) One page consumes 1100W for 8 s (idle) or 5 s (standby). In standby reheating occurs about every 35 s**

Figure 8: Brother HL2150 SOHO printer



(a) Minimal Network Power ($T_S = 10\,s$) (b) Median Network Power ($T_S = 10\,s$) (c) Maximum Network Power ($T_S = 10\,s$)

(d) Minimal Network Power ($T_S = 6\,s$) (e) Median Network Power ($T_S = 6\,s$) (f) Maximum Network Power ($T_S = 6\,s$)

Figure 9: Impact of static load attack on frequency in a grid with high rotational inertia (a-c), i.e., predominantly fed by conventional power plants, and low rotational inertia (d-f), i.e., fed by a high share of renewables, at different levels of total network power. Static load attacks are in multiples of the ENTSO-E reference incident (3000 MW).

5 EVALUATION: GRID EFFECTS

We investigated the effects of a botnet's load change on the continental synchronous grid. In particular, seek to answer in which way and to what extent load has to be modulated by an adversary using the botnet. Furthermore, we studied whether the grid's state, i.e., total load or the mix of feeding power plants, influences the success ofan attack. Such attacks against critical infrastructure can never be tested on a real system, specifically for a grid like the continental synchronous grid area providing power to more than 500 million people. Therefore, we developed a model in *Matlab/Simulink* that is based on the model of Ulbig et al. [53] and the ENTSO-E policies [55, 56]. In the remainder of this section, we describe in detail the model, the dependencies of grid parameters, and the success of each attack as presented in Section 3.

Attack 1: Static Load Attack. The adversary suddenly increases a high amount of load; the raised demand leads to an imbalance of production and consumption, thus shifting the frequency from its nominal value to lower values. If the adversary's amount of load is high enough, the frequency decreases rapidly without the primary control being able to counteract in time. If the frequency goes down to 49 Hz, load is shed due to emergency protocol, i.e., numerous consumers become disconnected from the power grid.

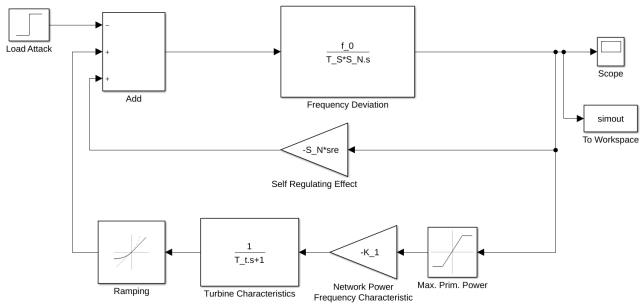


Figure 10: Model for static load attack (primary control)

For a simulation, we developed a model as depicted in Figure 10. The model contains the grid's response to a production-consumption imbalance with $f_0 = 50\,Hz$ (nominal frequency), start time constant T_S and the network power S_N. Further, it contains two feedback loops: The first considers the the self-regulation of load in case of frequency changes; the load typically changes 1%/Hz. The other feedback represents primary control, containing a saturation when reaching 200 mHz (at this point the full primary reserve is activated), a proportional element with a gain of 15,000 MW/s (full primary reserve of 3,000 MW should be activated at 200 mHz), a PT1-element representing turbine characteristics with $T_N = 2\,s$ (fast gas turbines) and a maximum slew rate of 500 MW/s as specified by ENTSO-E policies. With $T_S = 10$ and $S_N = 150\,GW$, the system's response to the reference incident (RI) of 3,000 MW corresponds with the design hypothesis of the policies [55] and emphasizes our model's accordance with the continental synchronous grid. Secondary control is not included into this model as it would not be activated at such an early phase of imbalance.

In a first step, we investigated the impact of the power grid's network power S_N on the amount of load that has to be modified by the adversary. S_N represents the amount of currently produced power and differs in the course of days, weeks and seasons. Generally, it is lower during night, summer and on national holidays, as consumers request less power than during daytime, winter and on work days. Values for network power P_N are taken from ENTSO-E statistics of the year 2016 [41]: The highest load was 583,711 MW on January 19th 2016, 5-6 a.m., the lowest load of 263,591 MW whereas

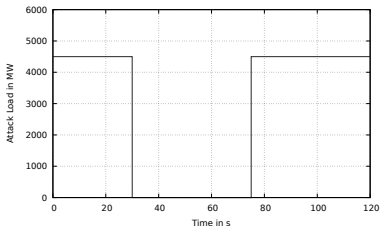


Figure 12: Dynamic load attack (1.5 reference incidents)

on May 29th 2016, 6-7 p.m, occurred the median load of 2016 was 409,823 MW.

We measure the static load attack in multiples of a ENTSO-E's *reference incident* of 3,000 MW. The impact of these attacks on grid frequency with a start time constant of $T_S = 10\,s$ is shown in Figures 9a-9c. Reaching the threshold of 49 Hz causes load shedding, and, thus, a successful attack. At minimal network power twice the reference incident, i.e., 6,000 MW is enough, whereas median network power requires 2.5 times the reference incident, i.e., 7,500 MW, and maximum network power 3.5 times, i.e., 10,500 MW. In conclusion, it is easier to reach the threshold for load shedding at times of an overall low power level in the network, i.e., at night, during summer and on national holidays.

Finally, the start time constant T_S is dependent on the type of power plants supplying the grid and is historically getting lower due to the increased use of renewables (wind turbines, PV)[1]. T_S might get as low as 6 s [53]. Figures 9d-9f highlight the consequences: more renewables make the frequency shifting faster, and reaching the threshold for load shedding becomes easier. Low start time constants are typically encountered during times of low power generation, e.g., on national holidays with lots of wind, as renewables sources are preferred for supply in Europe.

Attack 2: Dynamic Load Attack. Dynamic attacks promise to be more successful than static ones, i.e., reach higher frequency shifts while modulating the same amount of load. In our case, the adversary drives all load to full power, waits until primary control is initiated and reaches its maximum; then, the adversary withdraws all power consumption. Since the primary control's full activation takes 30 seconds, the attack load is modulated as depicted in Figure 12 (Our simulation relies on the model as shown in Figure 10).

The results of an attack via modulating 1.5 times the reference incident are shown in Figure 11: the absolute frequency shift at

[1]Photovoltaics and many wind-turbines are connected to the grid by solid-state inverters. In consequence, they can not stabilize the grid's frequency by means of rotational inertia.

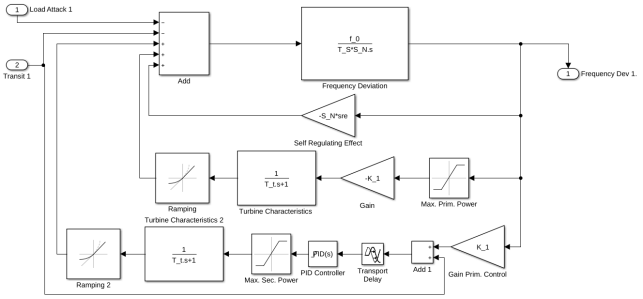
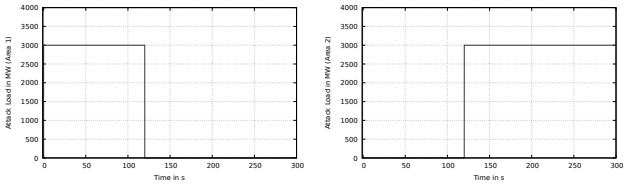


Figure 13: Model for control area including primary and secondary control



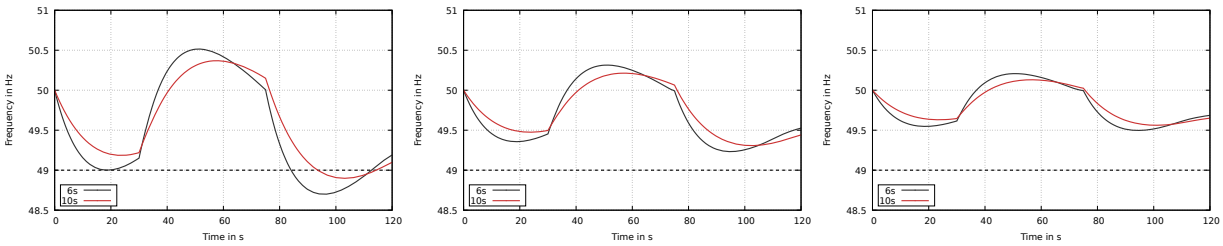
(a) Attack load in area 1 **(b) Attack load in area 2**

Figure 14: Inter-zone attack (reference incident)

the second swing after 80 seconds is typically higher than at the first one; in addition, the frequency is becoming larger than the nominal value of 50 Hz for a period of roughly 30 seconds, i.e., frequency overshoots despite an adversary that is solely able to modulate additional load in a grid[2]. Again, the less network power, e.g., during summer and nights, and the smaller the start time constant (more renewables), the easier it is to reach the threshold of 49 Hz for load shedding; the higher the attack load, the higher the frequency shift.

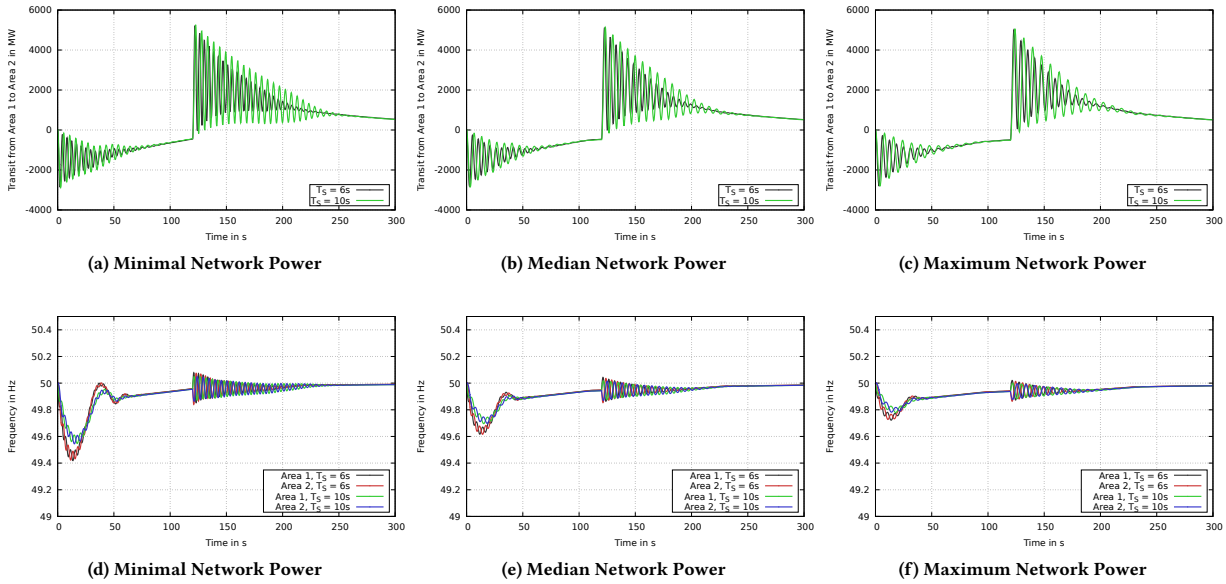
Attack 3: Inter-Zone Attacks. This attack relies on a synchronous grid containing multiple zones which are interconnected by transmission lines. In a first step, the adversary increases the load in one zone. Secondary control is eventually activated, and compensates for this additional consumption. As soon as this happens, the adversary reduces the load, while increasing it in the other zone, waiting for secondary control to compensate again. Finally, this leads to high amounts of transmission on the tie lines, which might eventually trip them.

[2]In the past, wind turbines were disconnected from the grid at a frequency of 50.5 Hz.



(a) Minimal Network Power **(b) Median Network Power** **(c) Maximum Network Power**

Figure 11: Dynamic load attack at different levels of total network power and rotational inertia



(a) Minimal Network Power (b) Median Network Power (c) Maximum Network Power

(d) Minimal Network Power (e) Median Network Power (f) Maximum Network Power

Figure 15: Transit power and frequency deviation in inter-zone attack at different levels of total network power and rotational inertia

For the simulation, we extended our model by another feedback loop representing secondary control, see Figure 13. Secondary control calculates the Area Control Error (ACE) as described in Section 2.2. $P_{measured}$, i.e., the transit to other areas, is fed into the model via input 2, $P_{planned}$ is assumed to be zero. The ACE is then forwarded to a delay (which might be up to 5 seconds [56]), and eventually to a PID controller representing the secondary controller with anti-wind-up functionality ($C_p = 0.17$,$T_N = 120$), a saturation when reaching the maximum amount of secondary control, again a PT1-element representing turbine characteristics $t_N = 2\,s$ (fast gas turbine), and a ramping as power plants cannot increase/decrease with arbitrary dynamics. Then, we took two such areas and connected them to a 2-area model by subtracting one area's frequency from the other and feeding the result into the transfer function $\frac{2\pi P_{Tie}}{s}$ to finally gain the power in transmission. Their frequencies are feed into the tie line's transfer function and further to both areas but with opposite sign.

Figure 14 shows the load that is modulated by the adversary in areas 1 and 2; Figure 15 shows the result in dependence of total network power load and rotational inertia. Figures 15a-15c show that the maximum amount of power in transit over the tie line is to a great extent independent from these parameters. They rather have an impact on the frequency deviation as shown in Figures 15d-15f, but inter-zone attacks aim to trip power lines. Thus, the adversary has to aim for a maximal power spike between area 1 and area 2 and fast changes, as line-tripping is done based on the total amount of load in transit as well as its time derivative [53].

Table 3: Prototypical computer hardware configurations with expected modulatable load

Components	Δ *Watt*	*Office*	*Home*	*Game*	*Server*
Core2	35	5%	5%	0%	0%
i3	64	40%	30%	5%	30%
i5	84	30%	40%	30%	80%
i7	86	15%	20%	40%	90%
i7E	140	10%	5%	25%	50%
GPU-Low	49	50%	50%	5%	0%
GPU-Mid	126.5	30%	30%	40%	0%
GPU-High	194	15%	15%	40%	0%
GPU-Top	249	5%	5%	15%	0%
TFT	80	125%	110%	150%	0%
Laser Printer	1,100	5%	30%	30%	0%
Expected Δ Load		**338.45**	**600.75**	**715.8**	**233.8**

6 DISCUSSION

In Section 3.2 we outlined the botnet and in Sections 4 and 5 we measured and simulated the components and attacks. In Section 6 we put the pieces together and sketch different distributions of infections to estimate the botnet size needed for an successful attack.

Based on the hardware listed in Table 2 we created four prototypical desktop computer configurations as presented in Table 3 which reads as follows: We assumed that home computers have a CPU-class distribution of 5% Core2, 30% i3, 40% i5, 20% i7, and 5% i7E or equivalents, totaling 100%. GPU values read accordingly, again summing up to 100%. For servers we assumed a higher probability for real multi-processor systems, effectively summing up to more than 100%. Likewise, gaming PCs (and to some degree others as well) have a higher probability of being connected to more than one screen [59]. The lowest row lists the expected controllable load per infected PC.

For IoT devices (Table 4) we created two different scenarios: A conservative one with just smart thermostats and another one with

Table 4: IoT scenarios

IoT	Δ Watt	*Mix 1*	*Mix 2*
AC	800	0%	4%
Thermostat	8,000	4%	8%
Oven	2,500	0%	1%
Refrigerator	400	0%	1%
Kettle	1,250	0%	1%
Expected Δ Load		**320**	**692.75**

Table 5: Infections needed

	Distribution 1	*Distribution 2*	*Distribution 3*
Office PC	40%	40%	30%
Home PC	30%	30%	40%
Gameing PC	15%	15%	20%
Server	15%	15%	10%
+ IoT-Mix (Table 4)	-	Mix 1	Mix 2
Avg. Δ Load p. Infection	458.045 W	778.045 W	1,201.125 W
Infections 3000 MW (1 RI)	6,549,575	3,855,819	**2,497,659**
Infections 4500 MW (1.5 RI)	**9,824,363**	5,783,728	3,746,488

additional devices. The former reflects the fact that est. 20 Million devices [52] have been sold in the last 4 years in the U.S. to their 126 Mio. housholds [49]. We reduced the factor by 1/3 to account for to the distribution of electric heating systems [40] in the U.S.

Table 5 combines the different computer types from Table 3 as well as the IoT scenarios into three possible infection distributions, whereas the first — most conservative estimation — excludes IoT devices completely. The second distribution corresponds with the first, with the addition of thermostats and the third adds all classes of IoT devices.

The following row computes the expected controllable load on average per installation of a botnet client, based on the distribution of infected computers. The last two rows display the botnet size necessary for 1 and 1.5 reference incidents (3,000 MW or 4,500 MW respectively).

Depending on the mix of infected devices, a successful attack can be achieved with 2.5 to 9.8 million devices — depending on other conditions described in Section 5 are met, such as day of time and mix of energy sources. For attacks 1 and 2 the infections can be located anywhere within the synchronous grid.

While this can only be considered a rough estimate, it is well within reach of real-world botnets. More accurate estimates are difficult [6, 44], but go up to 50 Mio. infected computers at the peaks times of certain botnets [51]. These figures cover infections globally, but Europe's estimated 17% share of Internet users in 2017 [35] and high technological level let these numbers appear feasible. Furthermore, we anticipate an increase of connected computers and Internet-enabled devices in the next years.

6.1 Limitations

The used simulation models are based on Ulbig et al. [53] and have to estimate some properties of the grid such as the mix of generator characteristics. A more precise simulation is possible with data from TSOs or ENTSO-E which include the exact mix of connected power plants and their scheduled (or actual) availability.

6.2 Future work

The simulation model for attack 2 uses resonance mainly caused by activation delay and generator characteristics of the primary control. However, additional grid-inherent resonances are known for the ENTSO-E synchronous area [18],[54, p.77],[26, p.3]. An attacker could piggyback on top of them and try to amplify them to gain more leverage. Grid-inherent resonant frequencies could also amplify the effects of attack 3.

We did not look at cascading effects which were almost always involved in large scale power outages [19, 54, 58]. These simulations are only possible with grid wide topology data including all tie lines characteristics.

In this paper we only targeted severe power disruptions of the grid e.g., by load shedding. However, an attacker could also just aim for economic damage invisible to the end-customer. Immediate costs arise by the additional deployment of reserves and increased unplanned international transfers. Long-term costs are associated with the permanent allocation of reserves as preparation for such attacks.

7 RELATED WORK

Irregular behavior in power grids happens from time to time, mostly due to unexpected incidents and not as a consequence of malicious behavior. ENTSO-E investigates and publishes such incidents to advance the knowledge for proper incident response. Thereby, ENTSO-E reported on inter-area oscillations [18], the impact of solar eclipses on power production [45], a blackout in larger parts of central Europe caused by a cascade of tripping lines [54], and a similar one in Turkey [19]. The first action against a power grid known to have been malicious happened in the Ukraine in 2015. The adversaries used malware delivered via e-mails, stole credentials and finally got access to the power providers' SCADA systems [8]. The adversaries used attack vectors well-known in traditional IT, whereas our attacks strike the power grid – a cyber-physical system – in its physical part.

Numerous works considered false data injection attacks, i.e., an adversary compromising meters and sending wrong data to the provider, and their detection [29–31, 63, 65]. Mishra et al. [36] investigated rate alteration attacks, i.e., fabrication of price messages, in smart grids. Mohsenian et al. [37] introduced the notion of Internet-based load attacks on smart grids, for example by manipulating computational load, exploiting capabilities of demand-side management or (apparently) manipulating spot-market electricity prices, e.g., so that programmable smart meters start charging electric cars all at once. Furthermore, the remote kill switch found in some smart-meters to disconnect subscribers from the grid has been suggested for similar destabilizing attacks on power grids as in our paper [5, 13]. However, as of 2017, meters with demand-side management are rolled out only to a limited extent. Smart meters that are rolled out at large-scale under various national and EU programs [24] often are metering-only and do not include a power control switch as they are more expensive and some nations completely opt out from such functionality [22].

Amini et al. [3, 4] claim that dynamic load attacks are more successful with respect to their impact on grid frequency. Their

model requires, however, huge power-shocks, effectively doubling the power consumption. We considered attacks with a load up to 3.5 times the continental synchronous grid's reference incident, i.e., 10,500 MW in total. This is lower than 4 % of the grid's total load, even at times of lower network power, thus making our attacks more practicable.

Xu et al. [62] aimed to increase loads in IaaS, PaaS and SaaS clouds to trip data centers' circuit breakers. The load increase is caused by the adversary renting cloud services or by using external web services to trigger computationally expensive operations. The authors sought to unplug a cloud provider's data center, but did not negatively impact the power grid itself, whereas our attacks aim to directly shut down the power grid or at least parts of it. Beyond that, our attack load might consist of any kind of controllable load and is not limited to cloud-based loads.

8 CONCLUSION

Power grids are among the largest human-made control structures and pre-date large communication networks like the Internet by decades. Their successful, i.e., synchronized, operation requires constant balance of power supply and demand; therefore, power providers maintain elaborated models to forecast demand in dependence of parameters like time of the day, season and weather conditions. However, these models rely on the assumption that fluctuations caused by single consumers are averaged out on a macro scale, i.e., for each consumer turning a light bulb off there is another one turning the light on. In our scenario, an adversary builds (or rents) a botnet of zombie computers and modulates their power consumption, e.g., by utilizing CPU, GPU, screen brightness, and laser printers in a coordinated way. Outperforming the grid's countervailing mechanisms in time, the grid is pushed into an unstable state triggering automated load shedding or tie line tripping due to under-frequency.

We developed three different attacks against the power grid and analyzed their feasibility. Therefore, we first investigated the dynamics and increase of different loads, in particular regarding PCs and IoT devices. We found CPUs, GPUs, and screens with a controllable load increase of 100 W and more; printers and IoT devices with even 1,000 W and more. In a second step, we simulated the impact of load attacks on grid stability, given that testing our attacks on a real power grid is infeasible for a variety of reasons.

Under favorable conditions, i.e., low total network power and a high share of inverter-connected renewables feeding power into the grid, 4,500 MW of additional load is sufficient to destabilize the system and trigger load shedding. In the European continental synchronous grid area, these conditions are typically prevalent at night or on public holidays with high wind power supply. According to our computations, an adversary requires a botnet of 2.5 to 9.8 million bots (Table 5). While this is not feasible in all cases, it might be worthwhile for entire nation attacks.

While terminology and details differ between synchronous grids worldwide, we want to stress that the general principles and conclusions are applicable to all AC power grids and our attacks work in every of these grids, though minor adaptions likely be necessary.

9 ACKNOWLEDGMENTS

We like to thank the reviewers for their constructive comments and additional insights.

This work was partially sponsored with the *CyPhySec* project by the *Bridge Frühphase* program and the *COMET K1* program, both by the Austrian Research Promoting Agency (FFG). Isometric icons from the *Lincity-ng* project in Figure 1 distributed under CC-BY-SA-v2.

REFERENCES

[1] 50Hertz Transmission GmbH. 2017. Grid load in the 50Hertz control area. (2017). http://www.50hertz.com/en/Grid-Data/Grid-load

[2] Airpatrol. 2017. Smart Air Conditioner Controllers. (2017). http://www.airpatrol.eu/ accessed 2017-06-04.

[3] S. Amini, H. Mohsenian-Rad, and F. Pasqualetti. 2015. Dynamic load altering attacks in smart grid. In *2015 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. 1–5. https://doi.org/10.1109/ISGT.2015.7131791

[4] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad. 2017. Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes. *IEEE Transactions on Smart Grid* (2017), 1–1.

[5] R. Anderson and S. Fuloria. 2010. Who Controls the off Switch?. In *2010 First IEEE International Conference on Smart Grid Communications*. 96–101. https://doi.org/10.1109/SMARTGRID.2010.5622026

[6] 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. 2017. Understanding the Mirai Botnet. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, BC, 1093–1110. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[7] General Electric Appliances. 2017. GE WiFi Connect - Air Conditioners. (2017). http://www.geappliances.com/ge/connected-appliances/air-conditioners.htm accessed 2017-06-04.

[8] Brian Harrell. 2017. Why the Ukraine power grid attacks should raise alarm. (2017). http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html

[9] buildcomputers.net. 2017. Power Consumption of PC Components in Watts. (2017). http://www.buildcomputers.net/power-consumption-of-pc-components.html accessed 2017-05-06.

[10] Pierre-Marc Bureau. 2009. Malware Trying to Avoid Some Countries. (2009). https://www.welivesecurity.com/2009/01/15/malware-trying-to-avoid-some-countries/ accessed 2017-05-30.

[11] Michael Ciuffo. 2012. Transistor Clock Part 1: Power and Time Base. (2012). http://ch00ftech.com/2012/06/20/2279/ accessed 2017-06-05.

[12] Alan J. Cooper. 2008. The Electric Network Frequency (ENF) as an Aid to Authenticating Forensic Digital Audio Recordings – an Automated Approach. In *Audio Engineering Society Conference: 33rd International Conference: Audio Forensics-Theory and Practice*. http://www.aes.org/e-lib/browse.cfm?elib=14411

[13] M. Costache, V. Tudor, M. Almgren, M. Papatriantafilou, and C. Saunders. 2011. Remote Control of Smart Meters: Friend or Foe?. In *2011 Seventh European Conference on Computer Network Defense*. 49–56. https://doi.org/10.1109/EC2ND.2011.14

[14] Mathias Dalheimer. 2016. An open-source infrastructure for power grid monitoring. (2016). https://github.com/netzsinus Github repository.

[15] Mathias Dalheimer. 2017. Momentane Frequenzabweichung im Stromnetzes. (2017). https://netzsin.us/ in German, accessed 2017-06-05.

[16] Dancho Danchev. 2013. How much does it cost to buy 10,000 U.S.-based malware-infected hosts? (2013). https://www.webroot.com/blog/2013/02/28/how-much-does-it-cost-to-buy-10000-u-s-based-malware-infected-hosts/ accessed 2017-05-30.

[17] Dynamic Demand. 2017. Dynamic Demand. (2017). http://www.dynamicdemand.co.uk/grid.htm accessed 2017-06-05.

[18] European Network of Transmission System Operators for Electricity. 2011. Analysis of CE Inter-Area Osciallations Of 19 and 24 February 2014. (2011). https://www.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/RG_SOC_CE/Top7_110913_CE_inter-area-oscil_feb_19th_24th_final.pdf

[19] European Network of Transmission System Operators for Electricity. 2015. Report on Blackout in Tureky on 31st March 2015. (2015).

[20] Forum Netztechnik. 2012. Technische Anforderungen an die automatische Frequenzentlastung. (2012). In German.

[21] Thomas Gobmaier. 2017. Measurement of the mains frequency. (2017). http://www.mainsfrequency.com/ accessed 2017-06-05.

[22] Nicolas Höning. 2013. Remote "shut-off" option cancelled for Dutch smart meters. (2013). https://www.nicolashoening.de/?energy&nr=238 accessed 2017-09-24.

[23] Markus Jaschinsky. 2017. altuelle Netzfrequenz (47,5-52,5 Hz) - Netzfrequenz.info. (2017). https://www.netzfrequenz.info/aktuelle-netzfrequenz-full accessed 2017-06-05.

[24] Joint Research Centre of the Eurpean Comission. 2017. Smart Metering deployment in the European Union. (2017). http://ses.jrc.ec.europa.eu/smart-metering-deployment-european-union

[25] Mateusz Kajstura, Agata Trawinska, and Jacek Hebenstreit. 2005. Application of the Electrical Network Frequency (ENF) Criterion. *Forensic Science International* 155, 2 (2005), 165–171. https://doi.org/10.1016/j.forsciint.2004.11.015

[26] Mats Larsson, Walter Sattinger, Luis-Fabiano Santos, and Roland Notter. 2013. *2013 IEEE Power & Energy Society General Meeting*. Institute of Electrical and Electronics Engineers, Chapter Practical Experience with Modal Estimation Tools at Swissgrid. https://library.e.abb.com/public/503f299a520c490c972def08598f6d7b/Practical%20Experience%20with%20Modal%20Estimation.pdf

[27] LG. 2017. LG Smart AC with mobile app. (2017). http://www.lg-dfs.com/smartac.aspx accessed 2017-06-04.

[28] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu. 2012. Securing smart grid: cyber attacks, countermeasures, and challenges. *IEEE Communications Magazine* 50, 8 (August 2012), 38–45. https://doi.org/10.1109/MCOM.2012.6257525

[29] X. Liu and Z. Li. 2014. Local Load Redistribution Attacks in Power Systems With Incomplete Network Information. *IEEE Transactions on Smart Grid* 5, 4 (2014), 1665–1676.

[30] X. Liu, Z. Li, and Z. Li. 2016. Optimal Protection Strategy Against False Data Injection Attacks in Power Systems. *IEEE Transactions on Smart Grid* (2016), 1–9.

[31] K. Manandhar, X. Cao, F. Hu, and Y. Liu. 2014. Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter. *IEEE Transactions on Control of Network Systems* 1, 4 (2014), 370–379.

[32] MaxMind Inc. 2017. GeoIP Products. (2017). http://dev.maxmind.com/geoip/ accessed 2017-05-30.

[33] D. Mills. 1992. Network Time Protocol (Version 3) Specification, Implementation and Analysis. RFC 1305 (Draft Standard). (March 1992), 109 pages. https://doi.org/10.17487/RFC1305 Obsoleted by RFC 5905.

[34] David L. Mills. 2014. Clock Discipline Algorithm. (2014). https://www.eecis.udel.edu/~mills/ntp/html/discipline.html accessed 2017-05-30.

[35] Miniwatts Marketing Group. 2017. World Internet Users Statistics and 2017 World Population Stats. (2017). http://www.internetworldstats.com/stats.htm accessed 2017-09-22.

[36] S. Mishra, X. Li, A. Kuhnle, M. T. Thai, and J. Seo. 2015. Rate alteration attacks in smart grid. In *2015 IEEE Conference on Computer Communications (INFOCOM)*. 2353–2361.

[37] A. H. Mohsenian-Rad and A. Leon-Garcia. 2011. Distributed Internet-Based Load Altering Attacks Against Smart Power Grids. *IEEE Transactions on Smart Grid* 2, 4 (Dec 2011), 667–674. https://doi.org/10.1109/TSG.2011.2160297

[38] NationalGridUSA Service Company, Inc. 2017. Electricity Transmission Operational Data. (2017). http://www2.nationalgrid.com/uk/industry-information/electricity-transmission-operational-data/

[39] Nest Labs, Inc. 2017. Meet the Nest Learning Thermostat. (2017). https://nest.com/thermostat/meet-nest-thermostat/ accessed 2017-06-04.

[40] Department of Energy. 2017. Home Heating Systems. (2017). https://energy.gov/energysaver/home-heating-systems accessed 2017-06-08.

[41] European Network of Transmission System Operators For Electricity. 2017. Power Statistics. (2017). https://www.entsoe.eu/data/statistics/Pages/default.aspx accessed 2017-06-06.

[42] Darren Pauli. 2015. Connected kettles boil over, spill Wi-Fi passwords over London. (2015). https://www.theregister.co.uk/2015/10/19/bods_brew_ikettle_20_hack_plot_vulnerable_london_pots/ accessed 2017-05-04.

[43] Phillip Porras, Hassen Saidi, and Vinod Yegneswaran. 2009. *An Analysis of Conficker's Logic and Rendezvous Points*. Technical Report. SRI International. http://www.csl.sri.com/users/vinod/papers/Conficker/ accessed 2017-05-30.

[44] Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose, and Andreas Terzis. 2007. My Botnet is Bigger Than Yours (Maybe, Better Than Yours): Why Size Estimates Remain Challenging. In *Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets (HotBots'07)*. USENIX Association, Berkeley, CA, USA, 5–5.

[45] Regional Group Contitental Europe and Synchronous Area Great Britain. 2015. Solar Eclipse 2015 - Impact Analysis. (2015).

[46] Rafael A. Rodríguez-Gómez, Gabriel Maciá-Fernández, and Pedro García-Teodoro. 2013. Survey and Taxonomy of Botnet Research Through Life-cycle. *ACM Comput. Surv.* 45, 4, Article 45 (Aug. 2013), 33 pages.

[47] Samsung. 2016. NE58K9850WG/AA - 5.8 cu. ft. Slide-In Electric Flex Duo Range with Dual Door. (2016). http://www.samsung.com/us/home-appliances/ranges/slide-in/ne58k9850wg-slide-in-electric-flex-duo-range-with-dual-door-black-stainless-steel-ne58k9850wg-aa/

[48] Samsung. 2017. Family Hub Refrigirator. (2017). http://www.samsung.com/us/explore/family-hub-refrigerator/ accessed 2017-06-04.

[49] Inc. Statista. 2016. Number of households in the U.S. from 1960 to 2016 (in millions). (2016). https://www.statista.com/statistics/183635/number-of-households-in-the-us/ accessed 2017-06-07.

[50] tado GmbH. 2017. Smart heating control. (2017). https://www.tado.com/ accessed 2017-06-04.

[51] Karl Thomas. 2015. Nine bad botnets and the damage they did. (2015). https://www.welivesecurity.com/2015/02/25/nine-bad-botnets-damage/ accessed 2017-06-08.

[52] Katherine Tweed. 2015. Smart Thermostats Begin to Dominate the Market in 2015. (2015). https://www.greentechmedia.com/articles/read/smart-thermostats-start-to-dominate-the-market-in-2015 accessed 2017-06-07.

[53] Andreas Ulbig, Theodor S. Borsche, and Göran Andersson. 2014. Impact of Low Rotational Inertia on Power System Stability and Operation. *arXiv* 1312.6435 (2014). https://arxiv.org/abs/1312.6435.

[54] Union for the Co-Ordination of Transmission of Electricity. 2007. Final Report: System Disturbance on 4 November 2006. (2007). https://www.entsoe.eu/fileadmin/user_upload/_library/publications/ce/otherreports/Final-Report-20070130.pdf

[55] Union for the Coordination of the Transmission of Electricity (UCTE). 2004. *Continental Europe Operation Handbook*. European Network of Transmission System Operators for Electricity, Chapter Appendix 1 - Load-Frequency Control and Performance. https://www.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/Operation_Handbook/Policy_1_Appendix%20_final.pdf

[56] Union for the Coordination of the Transmission of Electricity (UCTE). 2004. *Continental Europe Operation Handbook*. European Network of Transmission System Operators for Electricity, Chapter Policy 1 - Load-Frequency Control and Performance. https://www.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/Operation_Handbook/Policy1_final.pdf

[57] Union for the Coordination of the Transmission of Electricity (UCTE). 2004. *Continental Europe Operation Handbook*. European Network of Transmission System Operators for Electricity, Chapter Introduction. https://www.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/Operation_Handbook/introduction_v25.pdf

[58] U.S.-Canada Power System Outage Task Force. 2004. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. (2004). https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

[59] Valve Corporation. 2017. Steam Hardware & Software Survey. (2017). http://store.steampowered.com/hwsurvey/ accessed 2017-06-07.

[60] Verband der Netzbetreiber (VDN). 2007. TransmissionCode 2007 - Netz- und Systemregeln der deutschen Übertragungsnetzbetreiber. (2007). https://www.bdew.de/internet.nsf/id/A2A0475F2FAE8F44C12578300047C92F/$file/TransmissionCode2007.pdf In German.

[61] Wiggle Project. 2017. Wiggle: Wireless Network Mapping. (2017). https://wigle.net/ accessed 2017-05-30.

[62] Zhang Xu, Haining Wang, Zichen Xu, and Xiaorui Wang. 2014. Power Attack: An Increasing Threat to Data Centers. In *Network and Distributed System Security Symposium 2014, Proceedings of*. Internet Society.

[63] J. Yan, Y. Tang, Bo Tang, H. He, and Y. Sun. 2016. Power grid resilience against false data injection attacks. In *2016 IEEE Power and Energy Society General Meeting (PESGM)*. 1–5.

[64] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. 2012. A Survey on Cyber Security for Smart Grid Communications. *IEEE Communications Surveys Tutorials* 14, 4 (2012), 998–1010.

[65] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao. 2014. On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures. *IEEE Transactions on Parallel and Distributed Systems* 25, 3 (2014), 717–729.

[66] G. Zorn. 2010. RADIUS Attributes for IEEE 802.16 Privacy Key Management Version 1 (PKMv1) Protocol Support. RFC 5904 (Informational). (June 2010), 15 pages. https://doi.org/10.17487/RFC5904