IoT Threats to the Smart Grid: A Framework for Analyzing Emerging Risks

D. Jonathan Sebastian Cardenas
d.sebastiancardenas@wsu.edu
Washington State University
Pullman, WA

Adam Hahn
a.hahn@wsu.edu
Washington State University
Pullman, WA, US

ABSTRACT

Internet of Things (IoT) technologies have experienced an unprecedented growth over the last decade due to their wide applicability and low overall costs. These same factors have also allowed IoT deployments to transition into industrial environments which are expected to meet high reliability requirements. These technological-base shifts have raised operational (safety) concerns among researchers, which have been further fueled by high-profile cyber incidents that have exposed vulnerabilities in field devices. Although, multiple IoT cyber security issues are being actively researched, a compelling issue is to identify threats associated with cross-domain devices. A cross-domain vulnerability is any such vulnerability that can cause other non-IT system to experience unintended consequences.

Recent research has shown that physical systems, like the electrical grid might be exposed to abnormal conditions if a large set of load-controllable IoT devices are compromised [5]. Although risk reduction methodologies for bulk power components have been proposed these are focused towards SCADA-based systems which are owned, maintained, and operated by the utility under controlled environments. Whereas, IoT devices are owned by customers, spread across a wide service area, without supervised security policies.

In this work, a detailed analysis of such threats is performed on large-scale IoT deployments that could allow attackers to control a large amount of aggregated power. Based on our research, future-growth of large-load controllers and smart inverters could pose threats to grid operations due to their rapid load changing capabilities, these changes could exceed steady-state or transient design limits leading to unintended consequences. Therefore utilities need to methodologically analyzing these risks. This paper proposes such a methodology, which includes risk modeling and mitigation strategies.

KEYWORDS

Cybersecurity, Distributed Energy Resources, Internet of Things,

ACM Reference Format:

D. Jonathan Sebastian Cardenas and Adam Hahn. 2019. IoT Threats to the Smart Grid: A Framework for Analyzing Emerging Risks. In *Northwest*

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

NCS '19, April 8–10, 2019, Richland, WA, USA

© 2019 Association for Computing Machinery.

ACM ISBN 978-1-4503-6614-4/19/04...\$15.00

<https://doi.org/10.1145/3332448.3332452>

Cybersecurity Symposium (NCS '19), April 8–10, 2019, Richland, WA, USA.
ACM, New York, NY, USA, 8 pages. <https://doi.org/10.1145/3332448.3332452>

1 INTRODUCTION

Increased environmental awareness during the early 2000's led to multiple lobbying efforts promoting the use of sustainable energy resources. As a direct result, consumer-grade DER units became cost effective and business models such as leasing, and co-ownership became lucrative. Regions which have promoted the use of these technologies have become on-going live demonstration projects for analysing benefits and potential drawbacks. In the electrical domain DER units have lowered the overall energy cost (i.e. generation cost, reduced line losses, reduced congestion [11]), but have also created reliability and safety concerns due to its intermittent nature and lack of controllability characteristics (vs traditional generators).

These electrical concerns have been mostly addressed by standards such as IEEE 1547, and UL 1741. Additionally, regional regulations such as California's rule 21, and Hawaii's Rule No. 14H have introduced mechanisms that allow the devices to perform grid support functions, usually configurable through communication channels such as IEEE 2030.5 (SIP 2.0). Although these communication channels are designed to improve grid resilience characteristics they may be used as attack vectors by ill-intentioned entities.

The majority of consumer-grade DER units are built on top of Inverter-Based technologies (IBR) due to their high efficiency rating, and their primary generator characteristics (DC generators). When IBR devices add communication interfaces they are collectively referred as smart inverters [23]. Due to development constraints imposed by the rapidly evolving market, these devices must be briskly developed while maintaining a competitive cost. To address these challenges IoT-based platforms are often choose as the basic building block, to which power electronic components are later added [24].

During the same decade, a mixture of consumer's energy-saving awareness and the adoption of energy-efficient devices has staggered the US electricity demand. Although efficiency can be achieved by technological improvements (i.e. incandescent vs LED lighting) it can also be done through the use of building automation. In recent years smart buildings and smart homes have taken automation one step further by integrating multiple sensors to make decisions based on building occupancy, external weather, and the occupant's desired comfort levels, usually these comfort levels can be remotely configured over the internet thanks to the adoption of IoT technologies by automation controllers.

As outlined before, by building a device on top of an IoT foundation developers gain access to off-the-shelf protocols, third party's

Application Programming Interfaces (API), and a validated operating system codebase. This allows developers to focus on core product development, while a smaller set of resources are reserved for creating interfaces between the device's proprietary code, external API's (e.g. support for Alexa commands), and end-user controller interface (e.g. mobile applications). However, in some instances the main IoT codebase remains unchanged, creating a lack of diversity that can be exploited by attackers.

Internet-accessible devices are vulnerable to network-based attacks, historically, networks have been used to spread viruses, malware, and other ill-intentioned pieces of code to computer resources. IoT-based designs have not been the exception and have suffered cyber attacks. In 2016 the Mirai botnet infected millions of devices to mount the largest DDoS attack at its time [1]. The botnet exploited weak credentials, and a common codebase to replicate itself into multiple devices. Although the effects of the attack were limited to the cyber domain it provided an insight about the scaling capabilities of such attacks.

This work will begin by discussing previous research, followed by a graph-based analysis of IoT deployments to assess the risks to the grid. Section 4 will present a series of hypothetical simulation scenarios that may result from IoT-based attacks. Finally, section 5 will present a series of recommendations to mitigate risks, while section 6 presents the conclusions.

2 RELATED WORK

As mentioned in the introduction IoT-based devices are susceptible to cyber attacks, so far the attacks have remained within the cyber domain, but as demonstrated by the Stuxnet malware in 2008 it is possible to affect a physical system if real-world variables can be controlled [16]. A primitive cyber-physical attack occurred in 2016 with the Brickerbot malware which reused Mirai's infection mechanism, Brickerbot corrupted the device's firmware rendering the device useless leading to economical losses. Brickerbot's code targeted surveillance devices, which could raise privacy issues, but it could not cause physical damages outside the device. In contrast, [26] the authors propose IoT devices that are controlling large loads can be used to cause abnormal grid conditions. The authors present a series of attack scenarios that are evaluated under multiple operational metrics, they conclude that the effects will depend on the grid characteristics.

In [5] the authors propose to use Internet-enabled devices to create load "shocks" that can adversely impact the grid. In their proposal, demand variations are triggered by malicious code that alters the computational demands of PCs and peripherals. The authors propose a series of mechanisms which can be used to gain locational awareness and maximize impact. In [8] the effects of losing PV generation in high-penetration areas are analyzed. The results show that voltage oscillations occur, with machine angles deviating from their normal-operational range. The authors assume that PV-generation losses are due to their intermittent nature, or a trip due to a voltage excursion.

In [24] the authors discuss the implications of highly interconnected DER devices, dependency links are found between local area networks, vendor's cloud services and utility's networks. Authors conclude that the grid impact will depend on the hub size (the

number of devices attached to a network). The spreading characteristics of viruses inside communities (or hubs) has been discussed in [25]. The authors focus on analysing the factors that influence the infection rate, the analysis includes a network capacity model, and an epidemiological modeling of hosts. Vulnerable hosts are said to follow a Susceptible-Infected-Recovery (SIR) model.

In the regulatory context, frameworks that assess risk, protect and mitigate attacks have been developed. In the US, bulk power system components are regulated by a set of standards organized under the Critical Infrastructure Protection program [18]. Although these standards are enforced by regulatory bodies (i.e. NERC in the US) they are limited to specific grid components, as of 2019 no regulatory provisions to address IoT cyber-physical security have been enacted. NIST 8228 (draft) acknowledges the need for determining IoT risks due to interactions with the physical world, it further suggests that decentralized control operations (due to multi-hub interconnections) significantly increase potential impacts. Vulnerabilities due to multi-hub dependencies have also been identified as a significant risk in the 2017 DOE's Quadrennial report [7].

Nevertheless, certain standards, such as IIR-oriented IEEE 2030.5 are designed with security in mind. In IEEE 2030.5 communications are performed over a secure TLS channel with means to authenticate client and server interactions, additionally California Rule 21 requires random delays to be introduced before committing new settings. In NIST 8228 risk mitigation goals for IoT devices are identified, one of them is protecting device security which involves preventing the device from conducting attacks, the concept can be expanded to address issues like chain of trust, product certification, and product self-vulnerability management.

To assess these IoT risks, this paper starts by discussing the risks due large scale interactions between IoT devices, vendor clouds, third party providers and the internet. It continues with an evaluation of impacts to the electrical grid based on the number of vulnerable devices in a service area. Finally, a set of key metrics to estimate risks are given.

3 IOT RISKS

IoT devices are ubiquitous to our modern life, they are present in a multitude of devices, ranging from medical equipment, residential automation, voice assistants, appliances and passenger vehicles. Although applicability of each device is quite variable they share a common set of core features that make them appear as a homogenized entity within the cyber space. Figure 1 illustrates the main components that are involved in an IoT device, it split into four layers plus the external agent (end users). The next subsections discuss some of the risks associated with each of this layers.

3.1 External agent layer

The external agents can access the devices from any interface that connects to the internet, it is usually done through vendor provided web sites, mobile applications or even through third party devices such as Google Voice. This is the most visible layer that attackers will try to access, most cloud-service attacks have resulted in data breaches that are focused in stealing user information. However,

Figure 1: Typical components in IoT devices and their associated cyber security threats

more complex vulnerabilities could allow attackers to insert malicious web content into IoT devices without any authentication by using simple protocols like HTTP[2].

On top of these risks, an external agent environment cannot be isolated from the access mechanism. This means that local malware and other threats will be present when the user logs in, operates it, and they may impersonate his actions even after the user has changed activities. The scope of end-user environment isolation is outside the scope of this work but its existence must be acknowledged.

3.2 Cloud services and third party agents.

In this section a cloud service is a generalization of any server(s) that is used to process, transmit or store information being generated by remotely hosted IoT devices. Cloud services can be implemented under vendor-owned infrastructure or could be subleased from third parties in a service-payment model, each having its advantages or disadvantages. For small companies it might be beneficial for a specialized company to manage physical security and provide them with basic cyber security needs (firewalls, DDoS protection), while larger companies can custom build their solutions according to their needs. However, in both scenarios developers must understand the underlying services, for example in 2016 a voters registration database hosted by a cloud provider was publicly accessible after the default storage permissions were left intact [30].

Cloud services are one of the most critical assets in the IoT realm, most clouds perform off-site processing of field gathered data, they serve as intermediaries between the external agent and the field device, but they are also used to automatically push firmware updates. Due to these capabilities they serve as master agents for all the IoT devices registered within the service, which can make them prime targets for ill-intentioned entities. As an example of such threats, there was a case in 2017 where IoT-based locks were unintentionally bricked after posting an incorrect firmware. Although firmware-based attacks might be impractical due to network saturation, smaller files, such as settings files could be pushed to devices. As an example, in 2016, 800 thousand [12] IBR's settings were updated overnight.

Third party integration's also represent a security risk, weakly integrated services or stolen credentials could allow attackers to exploit otherwise secure systems. In 2015 a stolen third-party credential was used to insert a credit card skimmer into point of sale terminals by pushing an update from the company's central server

[31]. Some third party integration's minimize these risks by requiring the use of a per-client key token that allows the third party to only gain access to a specific set of devices. However, in recent years, vulnerabilities in the token creation, storage, and validation mechanisms have been disclosed [33].

3.3 Communications

In order to achieve most IoT functionalities communication paths must be established, this is often achieved by using the Internet. However, the internet is an unregulated set of networks in which traffic can be tracked, diverted, or interrupted. In this work, the internet will be referred to as a wide area network (WAN), while the term local area network (LAN) will be used to describe the private user network.

One of the simplest attacks consists in performing a Domain Name Server (DNS) resolution attack, such attacks can be done by changing the LAN DNS information, or by falsely announcing a shorter route. DNS hijacking can be used to redirect traffic towards an adversary's network, if an IoT device does not fully validate the server identity it may inadvertently send user data to a malicious data collector, depending on the attacker capabilities this mechanism can also be used to control the device. Attacks on data privacy are also possible at this level but do not pose a risk to cyber physical security. Communications also play a role in determining the propagation speed of attacks, according to [25], devices that are connected to high speed links are capable of spreading malware at a faster rate, and tend to become infected earlier on.

3.4 IoT device

IoT-based devices are a fusion of software packages designed to reduce developer burden towards creating internet-ready devices. These packages are often based on open source projects which are actively maintained and therefore are expected to offer patches against recent cyber-vulnerabilities. However, most update mechanisms are designed to offer a cumulative update that ensures product functionality, leading to delayed updates. In [29] the authors estimate that adapting the upstream Linux code to the Android code base takes 5 months to be accomplished, even though they are actively maintained. Delayed updates are only part of the problem, another issue is planned obsolescence in which companies stop publishing updates even if the device remains in service. This is particularly true for devices that are expected to be in service for a long time, for example, California requires IBRs to have a warranty of 10 years, while the typical software maintenance periods last less than 3 years.

Unpatched vulnerabilities become a problem of scale when thousands of devices are vulnerable to a common attack vector, as a result of exploiting such vulnerability the device may experience an array of consequences, including becoming unresponsive or allowing custom code execution. According to the National Vulnerability Database (NVD) more than 5% of known vulnerabilities in the last 3 years can lead to a "code execution vulnerability" [21]. If custom code execution is achieved, the attacker can 1) determine hardware type, 2) propagate the Zero-day vulnerability, 3) launch an attack based on hardware type.

3.5 Physical Layer

IoT devices have a wide applicability spectrum, each one with different types of actuators and sensors than in theory create a diverse environment that is resilient to attacks. However, there exists a set factors that reduce this diversity, for example, a single vendor can sell thousands of devices under the same model number, or offer seemingly-different devices that are functionally equivalent. Although, functionally-equivalent models are expected to compete in the market with other vendors there is a tendency to create oligopolies, under which new/smaller competitors can only subsist with either a novel or investor-backed product. These oligopolies are due to user-adoption behaviours that tends to follow a preferential attachment model (power law model) [18], under this model certain brands or products become successful due to consumer recommendations or marketing. Figure 2 presents the sales rank for the market leaders in the field of smart thermostat for a US-based store [13]. In addition NEST claims to have sold over 11 million since 2011, out of the 25 million forecasted devices by 2019 [22]. This lack of diversity could cause a large scale infections, for example a 5% infection rate in NEST devices, could rival the 600,000 infected devices observed during the Mirai Attack [1].

Figure 2: Smart thermostats sales rank tracked across a year for a particular store

As mentioned by the introduction large IoT-based load controllers could jeopardize grid operations if their cumulative load controlling capability exceed the operational limits. However effects are not limited to the electrical sector, depending on the actuator capabilities other physical consequences may occur in other domains, for example in 2016 the FDA identified vulnerabilities in pacemakers and also found faults in life-support intravenous pumps [14].

4 RISK ASSESSMENT METHODOLOGY

In this section a methodology (Fig. 3) for determining the electrical impact due to an attacker's capability of controlling a botnet of IoT devices is presented. Figure 3 presents an overview of the proposed methodology, each of the components will be discussed in the next subsections.

4.1 Cyber model

As mentioned in section 3 there are multiple threats associated with each IoT layer, although there exist a possibility of having a targeted attack towards a single user/site by attacking his LAN or access mechanism, the impact would be limited. In this work the focus will be given to attacks that target a large set of devices. It is

Figure 3: Overview of the proposed methodology

Table 1: California DER characteristics*

Data Source	Installed capacity [MVA]**	Num. of installations	Avg. site capacity [kVA]	Avg. devices per site
CSI Database	1921	143,605	29.67	8.35
NEM Database	6591	792,773	8.3127	4.52

* Includes smart and traditional DER installations

** Some datasources report this value in DC-measured MW

important to note that utilities must first estimate the amount of IoT devices within its service territory, this can be performed by using national or state information (if local information is unavailable). An example of such dataset is given in table 1, were the amount of installed DER power given on a per site basis [27][28].

4.1.1 Modeling vendors. In each IoT domain there exists a set companies that have a significant market share, this product-vendor dependencies form a hub of vulnerable devices. In the field of thermostats three companies are dominant [22], although sale numbers are not public, utilities can estimate them based on consumer's energy saving rebate history. For DER devices certain entities like [27] publish statics that can be used to determine the maximum hub size of interdependent devices, table 2 summarizes some of the available data.

It is important to note that not all devices listed in table 2 are "smart", for this particular case 35-40% are internet capable devices. Additionally not all devices are directly accessible, some of these devices could be located behind a firewall or other security mechanisms [32], a general equation to find the maximum hub size ($Hub_{size(v)}$) can be written as follows:

$$Hub_{size(v)} = M_{size} * M_{share_{LV}} * Int_c * (1 - f_{w_{effec}}) \quad (1)$$

where:

M_{size} = Num. of installed devices within the utility's region

$M_{share_{LV}}$ = Market share of largest vendor [0-1]

Int_c = Percent of internet-capable devices [0-1]

$f_{w_{effec}}$ = Firewall effectiveness (i.e. $\approx 45\%$)[0-1]

4.1.2 Modeling third party connections. In a similar way that vendors tend to have market oligopolies, certain third party operators dominate the market. In the market of smart thermostat 2 companies have dominant positions [22], while in the DER market 3 companies account for 65% of the market (see table 3). An important distinction from traditional vendors is that third party solutions depend on Internet connectivity to provide their services, therefore $\%Internet_c = 1$ must be set in 2.

Table 2: Device characteristics, per vendor

Vendor	Sites	Total devices	Devs per site	Avg. S_{site} [kVA]	Avg. S_{device} [kVA]	S_{total} [MW]	Market share %MW
Others	2731	16938	6.20	128.23	20.68	350.20	18.23
Advanced Energy	398	739	1.86	465.56	250.74	185.29	9.65
Yaskawa Solectria	1026	2258	2.20	134.03	60.90	137.52	7.16
Kaco	2854	3279	1.15	7.45	6.48	21.26	1.11
Xantrex Tech.	3256	4028	1.24	30.58	24.72	99.57	5.18
PV powered	4269	5126	1.20	23.45	19.53	100.09	5.21
SolarEdge Tech.	4341	5822	1.34	6.66	4.97	28.92	1.51
Fronius USA	18624	21147	1.14	6.40	5.63	119.15	6.20
Sun power	20650	27046	1.31	6.25	4.77	128.94	6.71
Power One	22111	28586	1.29	7.52	5.41	166.23	8.65
Enphase Energy	28139	694465	24.68	5.26	0.21	147.90	7.70
SMA America	5206	48906	1.39	12.41	8.93	436.74	22.74
Totals	143605	858337	-	-	-	1921.85	100

Table 3: California DER 3rd party dependencies, based on [28]

3rd party	Number of sites	Market share %
SolarCity/Tesla	79045	31.3%
Sunrun	46216	18.3%
Vivint	38481	15.2%
Sunpower	13240	5.2%
Lennar Homes of Cal.	10190	4.0%
Sunnova	8147	3.2%
Sungevity	5000	2.0%
Others	52231	20.7%

$$Hub_{size(3p)} = M_{size} * M_{share_{3p}} * Int_c * (1 - f_{w_{effec}}) \quad (2)$$

where:

$M_{share_{3p}}$ = Market share of largest third party operator [0-1]
(see Eq. 1 for other terms)

4.1.3 Modeling software connections. As mentioned in the introduction IoT devices are based on off-the-shelf OS's, with Linux (39%), Windows (%14) and FreeRTOS (19%) having a 71.5% percent market share. With Raspbian, Ubuntu, and Debian distributions accounting for 57% of Linux-based deployments. In this case it is possible to come up with a statistically-based equation to estimate the largest software hub size. The proposed equation is:

$$Hub_{size(s)} = M_{size} * M_{share_{LS}} * Int_c * (1 - f_{w_{effec}}) * (%Attack_{sr}) \quad (3)$$

where:

$M_{share_{LS}}$ = Market share of largest software base [0-1]
 $Attack_{sr}$ = Attacker's success rate (i.e. $\approx 5\%$) [0-1]
(see Eq. 1 for other terms)

In the field of software vulnerabilities an important factor in determining the attacker success rate depends on determining whether or not the software is patched, this number tends to be low due to developer's continuous patching efforts. As an example, when the WannaCry code was leaked an estimated 129 Million PC's where running windows XP [15], out of those 1.25M PC's where vulnerable to the attack according to a IP scan[17], this means that .96% of PCs where vulnerable. This seemingly low percentage

takes into account firewall access, and actual internet connectivity levels, PC under LAN environments are expected to have a much higher vulnerability level, which helps explain why significant parts of large organizations became infected.

4.2 Interface model

Based on the hub_{size} calculations presented in the previous section it is possible to estimate the attackers controllable power by using:

$$E(power) = Max(Hub_{size(v)} * Avg_{dev load(v)}, Hub_{size(3party)} * Avg_{dev load(3party)}, Hub_{size(s)} * Avg_{dev load(s)}) \quad (4)$$

where:

$E(power)$ = Expected attackers-controllable power
 $Hub_{size(X)}$ = Hub's X size, where $X=\{v=vendor, 3party=third\ party, s=software\}$
 $Avg_{dev load(X)}$ = Average load demand for each device in hub X, where $X=\{v=vendor, 3party=third\ party, s=software\}$

The $E(power)$ = can have an associated ramping rate, for example, electrical-based HVAC systems can switch states in an "instantaneous" manner, whereas DER devices have a ramping rate imposed by SIP v2 configuration. Also, it is important to note that hub calculation must be performed based on the number of residents / housing units in the utility's region, therefore $hub_{size} \ll devices\ in\ service\ area$. In this work we further restrict $E(power)$ = value to a $\Delta load$ value by acknowledging that not all devices can change from a no load condition to a full load in a short period of time (i.e. must thermostats have PID controllers).

Based on [5] and [8] we propose to model IoT-controlled loads under two operational domains, under static analysis an instant $\Delta load = k * E(power)$ switching action is proposed. This model is ideal for evaluating system violations, such as line limits, short term dispatchability, or for evaluating real-time energy market costs.

Figure 4: Physical modeling of $\Delta load$. note: $\Delta load > 0$ means an inverter has been turned off (masked load effect), or HVAC has increased.

The second model uses a combination of $\Delta load$ that is applied over a $\Delta time(t)$, such model is ideal for evaluating the system transient response. Under this model each load bus can have a unique $\Delta S / \Delta time$ combination to account for network or device-imposed delays in executing an attacker action.

4.3 Impact assessment

The proposed electrical model needs to be integrated into the utility's routine studies, these include scheduling day to day operations, sizing ramping rate reserves, evaluating NERC's reliability "n-1" under the stress of IoT-induced $\Delta load$ variations. [5] and [26] present a series of scenarios under which utilities must assess their cyber-physical security.

Table IV.1: Largest DER vendor-hub risk

Properties	factors	Cum. %
<i>S_{California}</i>	26049MW	100.00%
NEM+CSI supply	8512MW	32.68%
<i>Mshare_{LV}</i>	22.74%	7.43%
<i>Int_c</i>	38%	2.82%
<i>F_{w_{effect}}</i>	45%	1.55%
<i>F_{w_{effect}}</i>	5%	2.68%

Table IV.2: Largest DER software-hub risk

Properties	factors	Cum. %
<i>S_{California}</i>	26049MW	100.00%
NEM+CSI supply	8512MW	32.68%
<i>Int_c</i>	38.00%	12.42%
<i>Mshare_{LS}</i>	39.00%	4.84%
<i>F_{w_{effect}}</i>	45.00%	2.66%
<i>Attack_{sr}</i>	5%	0.13%

Table IV.3: Largest DER 3rd party-hub risk

Properties	factors	Cum. %
<i>S_{California}</i>	26049MW	100.00%
NEM+CSI supply	8512MW	32.68%
3rd party operated	31.85%	10.41%
<i>Mshare_{3p}</i>	31.30%	3.26%
<i>F_{w_{effect}}</i>	45.00%	1.79%
<i>F_{w_{effect}}</i>	5%	3.09%

Table IV.4: Largest thermostat vendor-hub risk (space heating)

Properties	factors	Cum. %
<i>S_{California}</i>	26049MW	100.00%
Energy used in heating*	27.0%	27.00%
Use of electricity in heating*	58.0%	15.66%
Customers with Prog. Thermostat**	6.9%	1.08%
<i>Mshare_v</i>	50.0%	0.54%
<i>Int_c</i>	100%	0.54%
<i>F_{w_{effect}}</i>	45.0%	0.24%
<i>F_{w_{effect}}</i>	5.0%	0.51%

Table IV.5: Largest thermostat vendor-hub risk (space and water heating)

Properties	factors	Cum. %
<i>S_{California}</i>	26049MW	100.00%
Energy used in space and water heating*	52%	52.00%
Use of electricity in heating*	58%	30.16%
Customers with Prog. Thermostat**	6.9%	2.08%
<i>Mshare_v</i>	50.00%	1.04%
<i>Int_c</i>	100%	1.04%
<i>F_{w_{effect}}</i>	45%	0.47%
<i>F_{w_{effect}}</i>	5%	0.99%

Table IV.6: Largest thermostat vendor-hub risk (cooling)

Properties	factors	Cum. %
<i>S_{California}</i>	26049MW	100.00%
Energy used in cooling*	4%	4.00%
Use of electricity in cooling*	40%	1.60%
Customers with Prog. Thermostat**	6.9%	0.11%
<i>Mshare_v</i>	50.00%	0.06%
<i>Int_c</i>	100%	0.06%
<i>F_{w_{effect}}</i>	45%	0.02%
<i>F_{w_{effect}}</i>	5%	0.05%

* Derived from 2009¹ residential energy use data[10].** Derived from 2015¹ residential energy use data (pacific)[9].

5 CASE STUDY

In this section a steady-state analysis on the effects of $\Delta load$ variations is performed. The studied case uses the market properties available for the state of California and computes $\%Load$ expressed as a percentage of the average system load experienced in the system (26,049 during 2017 [3]). Each of the tables IV.1-IV.6 computes the results of equations 1,2,3 based on the data presented in table 1, 2,3 and government sources [10],[9]. $\%Load$ is assumed to be equal to the highlighted values (for each $f_{w_{effect}}$ pair). Internet connectivity is assumed to be 100% for smart thermostats and inverters managed by 3rd parties, the possibility of having an unpatched system is assumed to be 5%. Two firewall effectiveness are assumed, 45% (industry standard), and 5% to account for user's trust due to Universal Plug and Play (UPNP) capabilities of some IoT devices, UPNP allows devices to be discoverable within the local network, and can auto-configure most residential router's firewalls.

The next part of this study uses a publicly available [20] steady-state power system model to evaluate the steady state response to load changing events. The first section of the study determines the line loadability limits to determine if there exists a risk with any of the computed $\%Loads$. The selected system is comparable to the California system, it is approximately 80% of its average load value and contains +3k nodes. The second section, determines if there exists a risk for increased market costs given the expected $\%Loads$ variations.

5.1 Line loadability

When analysing line loadability certain rules must be enforced 1) line limits are proactively enforced by scheduling appropriate amounts of power flows, 2) such scheduling is performed using an optimal power flow study, which uses cost functions to limit flows based on a congestion price, and dispatches generators such that generation and congestion prices are minimized. By using such technique and setting conservative line ratings a system operator can ensure that the system satisfies the demand while satisfying reliability requirements.

According to NERC [4] lines must be capable of short-term overloading and therefore conductors are rated in three operating modes: continuous, overload and emergency, with the overload rating being at least 115% of the normal rating, although most are rated at 130%. This overload rating is designed to give operators at least a 15-minute window to correct flows.

Table V: Line currents obtained by simulating the case in MATPOWER

	Reference	Classical	Optimal	CPF=1.0815	CPF=1.1374
Max. (I) [P.U.]	9.07	9.0874	7.7659	10.0520	16.8670
Avg. (I) [P.U.]	0.31	0.3196	.2890	.3280	.3697
Capacity Mult. of $I_{max} = Limit_{MVar}$	-	1.6522	1.0000	1.2089	1.4280
Max. Obs. Load Mult. of $I_{max} = Limit_{I Tight}$	-	1.7109	1.0731	1.3000	1.5062
Max. Obs. Load Mult. of $I_{max} = Limit_{I Loose}$	-	1.4512	0.9185	1.1126	1.3002

Additionally, secondary controllers auto-correct power imbalances within few minutes, with economic-driven adjustments performed manually by operators. Based on these concepts the results of performing a classical power flow solution is presented in column 2 of table V. In order to validate the implementation and source files the results were compared against those published in [19] (column 1).

In [19] the authors acknowledge that power systems have two ratings that are applicable to the optimal power flow problem, a MVar rating used for stability studies and a current limit that specifies the maximum current that can be transferred (and thus establishes the line trip value). Since the Polish system dataset only contains MVar ratings they suggest a method for obtaining the line current. Such method computes two current values, a tight value that shall be used in stressed systems and a loose limit that can be used in normal cases. Equation 1 shows how the compute these values based on the maximum MVar rating between nodes (n,m) given the maximum and minimum voltages observed at the ends.

$$I_{tight\ lim} = \frac{\max(S_{nm})}{\max(V)} \leq \max(I_{nm}) \leq \frac{\max(S_{nm})}{\min(V)} = I_{Loose\ lim} \quad (5)$$

Figure 5: Voltage and price increases observed during an optimal power flow simulation, using a fixed amount of generation.

Table VI: System characteristics for the 2008 Polish scenario, reported values are based on the default case

Elements	Quantity	Statics	P (MW)	Q (MVar)
Buses	3230	Total gen capacity	35585.0	-63120.3 to 79422.5
Available generators	505	On-line capacity	25406.0	-62528.7 to 73954.0
Committed generators	298	Generation (actual)	21602.0	5664.9
Loads	2314	Base load (1.0)	21181.5	8723.2

Based on these limits the classical PF (column 2) is expanded to include the maximum observed currents expressed in multiples of the rated capacities, as it can observed multiple violations occur with the base-load values. If instead we use optimal power flow (column 3) we can observe that the maximum current decreases and is maintained within the continuous rating operating margin (for economic reasons it is ideal to operate at 100% the rated capacity). This is the base case that should be used to assess the grid loading capacity. Columns 4 and 5 where obtained by running a continuation power flow, it reuses the optimal power flow results as the initial scenario. The results were obtained by fixing the generator output while increasing the system load. Column 4 assumes that the tight limit is used to set the line overload rating (assuming a 130% line overload capability), the result implies that the load can grow up to 8.15% before any violations occur. Column 5 was similarly obtained by using the loose limit (assuming a 130% line overload capability) in this case the grid can withstand a 13.74% increase (although a stability studies must be performed due to MVar violations). Based on the expected $\% \Delta Load$ variation results we can contend that no line violations will occur. However, if PV penetration continues to grow, or market shares keep increasing then it would be plausible to experience line overloads when $\% \Delta Load > 8\%$.

5.2 Market cost increases

System operators continually perform market clearing operations to pick the optimal set of generators such that the average system Local Marginal Prices (LMP) are minimized, when load varies unexpectedly these LMP values can increase disproportionately. To study the effects of $\% \Delta Load$ variations a market clearing process was simulated. The units being committed are assumed to be pre-allocated (see table VI), but the output of these generators are allowed to vary according to the system load. Optimal power solutions at increasing load levels are solved based on this restriction. Load is varied up to 10% (1.1 PU), the voltage profiles observed during this simulation are presented in Figure 5a. The Local Marginal Price (=generator cost + congestion cost) (LMPs) are plotted in Figure 5b, while normalized prices (assuming that base prices are defined at the 1.0 load factor) are shown in

Figure 5c. The results indicate that there is a significant maximal LMP in the network that starts to grow once the load increases 5%, however, the average LMP price remains relative constant, increasing to 32% once a 10% load increase occurs.

The results imply that although there is an increase in cost, it is insignificant for the given $\% \Delta Load$ variations, however if the smart DER penetration level doubles, then price increases could occur. It must be noted that the performed simulation does not include stricter bid commitments like maintaining a per generator commitment within a certain range for a determined amount of time. Such models are outside the scope of this work and are likely to increase the overall cost.

It is important to note that the presence of high LMP's can benefit certain generators, by assigning them bids that can lower the LMP price, even if that bid is significantly more expensive than other generators (far away generators are affected by congestion prices). This could in turn create a powerful incentive for bidders to use IoT bots to game the market.

6 DISCUSSION AND PROPOSED MITIGATIONS

Utilities need to understand and address the new emerging risks in both the internal and external infrastructure including those IoT devices that are attached to their infrastructure. Utilities must also acknowledge that they no control over the devices located outside their premises, but they must be able to withstand the impact of large IoT-hub that miss-behaves. Utilities can also work with governmental entities by requesting policies that 1) promote market diversity, 2) limit the number of devices controlled by a single entity, 3) establish risk-analysis frameworks that include contingency and mitigation procedures. Within this context, the Department of Homeland Security has published a set of strategic guidelines for addressing cybersecurity for IoT infrastructure [6], these guidelines could be adapted to the power-grid environment. Other solutions include, inclusion of mandatory software maintenance programs into existing warranty mandates, use of hardware enforced fail-back mechanisms that prevent instantaneous load changes.

7 CONCLUSIONS

The work presented an overview of the IoT-based risks present in the electrical grid. These risks were incorporated into a risk assessing methodology that uses a probabilistic approach to compute the amount of power ($\Delta load$) that can be controlled. The work makes use of real-world databases to compute approximate numerical threats, the numbers presented are used for demonstration purposes, and utilities should attempt to obtain the most up-to-date information.

Based on the results presented in section V it would appear that the current risk is below the required threshold for raising an urgent alarm. However, if the IoT-penetration levels keep increasing (as it would be expected) then risk mitigation strategies must be implemented. Finally, guidelines for reducing risks and mitigating them were identified. These guidelines are based on industry trends and will be generally applicable to a wide range of energy delivery participants.

ACKNOWLEDGMENT

The authors would like to thank the US DOE, India's Department of Science and Technology (DST) under UI-ASSIST partnership (DE-IA0000025). We also thank the DOE for their funding under Grid Modernization Laboratory Call (GMLC) Project GM0100, and CONACYT(Mexico).

REFERENCES

- [1] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. 2017. Understanding the mirai botnet. In *26th {USENIX} Security Symposium ({USENIX} Security 17)*. 1093–1110.
- [2] Edmund Brumaghin. 2018. Vulnerability Spotlight: Multiple Vulnerabilities in Samsung SmartThings Hub. <https://blog.talosintelligence.com/2018/07/samsung-smarthings-vulns.html>
- [3] CAISO. 2017. Annual report on market issues and performance. <http://www.caiso.com/Documents/2017AnnualReportonMarketIssuesandPerformance.pdf>
- [4] North American Electric Reliability Corporation. 2017. Determination and Application of Practical Relaying Loadability Ratings.
- [5] 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 *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017)*. ACM, New York, NY, USA, 303–314. <https://doi.org/10.1145/3134600.3134639>
- [6] Department of homeland security. 2016. Securing the Internet of Things. <https://www.dhs.gov/securingthelot>
- [7] DOE. 2017. *QUADRENNIAL ENERGY REVIEW, TRANSFORMING THE NATION'S ELECTRICITY SYSTEM: THE SECOND INSTALLMENT OF THE QER*. Technical Report. <https://goo.gl/g7gC98>
- [8] S. Eftekharnjad, V. Vittal, G. T. Heydt, B. Keel, and J. Loehr. 2013. Impact of increased penetration of photovoltaic generation on power systems. *IEEE Transactions on Power Systems* 28, 2 (May 2013), 893–901. <https://doi.org/10.1109/TPWRS.2012.2216294>
- [9] EIA. 2015. Air conditioning in homes in the South and West regions. <https://www.eia.gov/consumption/residential/data/2015/hc/php/hc7.8.php>
- [10] EIA. 2019. Household energy use in California. https://www.eia.gov/consumption/residential/reports/2009/state_briefs/pdf/ca.pdf
- [11] EPRI. 2015. *The Integrated Grid: A Benefit-Cost Framework*. Technical Report.
- [12] Peter Fairley. 2015. 800,000 Microinverters Remotely Retrofitted on Oahu in One Day. <https://spectrum.ieee.org/energywise/green-tech/solar/in-one-day-800000-microinverters-remotely-retrofitted-on-oahu>
- [13] Joshua Fruhlinger. 2018. Smart thermostats sell best in June and December according to sales-rank data. <https://media.thinknum.com/articles/smart-thermostats-seasonal-sales/>
- [14] Karen K Giuliano. 2018. Intravenous smart pumps: usability issues, intravenous medication administration error, and patient safety. *Critical care nursing clinics of North America* (2018).
- [15] Daniel Jennings. [n. d.]. Are 129 Million PCs Still Using Windows XP? - Daniel Jennings. <https://seekingalpha.com/instablog/22912651-daniel-jennings/5080343-129-million-pcs-still-using-windows-xp>
- [16] David Kushner. 2013. The Real Story of Stuxnet. <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>
- [17] Rapid7 Labs. [n. d.]. National Exposure Index. https://www.rapid7.com/globalassets/_pdfs/research/rapid7-national-exposure-index-2018.pdf
- [18] Jure Leskovec, Ajit Singh, and Jon Kleinberg. 2006. Patterns of Influence in a Recommendation Network SECT. In *Advances in Knowledge Discovery and Data Mining*, Wee-Keong Ng, Masaru Kitsuregawa, Jianzhong Li, and Kuiyu Chang (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 380–389.
- [19] Paula A. Lipka, Clay Campaigne, Mehrdad Pirnia, Richard P. O'Neill, and Shmuel S. Oren. 2017. Constructing transmission line current constraints for the IEEE and polish systems. *Energy Systems* 8, 1 (01 Feb 2017), 199–216. <https://doi.org/10.1007/s12667-016-0194-8>
- [20] MATPOWER. 2005. CASE3120SP Power flow data for Polish system - summer 2008 morning peak. <http://www.pserc.cornell.edu/matpower/docs/ref/matpower5.0/case3120sp.html>
- [21] NIST. 2019. NATIONAL VULNERABILITY DATABASE: Statics results. https://nvd.nist.gov/vuln/search/statistics?form_type=Advanced&results_type=overview&query=code+execution+vulnerability&search_type=all
- [22] U.S. Department of Energy. 2016. https://www.energy.gov/sites/prod/files/2016/12/f34/OverviewofExistingFutureResidentialUseCasesforCT_2016-12-16.pdf
- [23] B Seal. 2016. Common functions for smart inverters. In *EPRI, Knoxville, TN*.
- [24] D. J. Sebastian and A. Hahn. 2017. Exploring emerging cybersecurity risks from network-connected DER devices. In *2017 North American Power Symposium (NAPS)*. 1–6. <https://doi.org/10.1109/NAPS.2017.8107267>
- [25] Giuseppe Serazzi and Stefano Zanero. 2003. Computer virus propagation models. In *International Workshop on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems*. Springer, 26–50.
- [26] Saleh Soltan, Prateek Mittal, and H. Vincent Poor. 2018. BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. In *USENIX Security Symposium*.
- [27] DBA Energy Solutions. 2019. Distributed Generation Incentive Program Data. https://www.californiadgstats.ca.gov/downloads/#_nem_cids
- [28] DBA Energy Solutions. 2019. Distributed Generation Interconnection Program Data. <https://www.californiadgstats.ca.gov/downloads>
- [29] Daniel R Thomas, Alastair R Beresford, and Andrew Rice. 2015. Security metrics for the android ecosystem. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*. ACM, 87–98.
- [30] Chris Vickery. 2016. Massive Breach of Mexican Voter Data. <https://mackeeper.com/blog/post/217-breaking-massive-data-breach-of-mexican-voter-data/>
- [31] Yong Wang, Christen Hahn, and Kruttika Suttrave. 2016. Mobile payment security, threats, and challenges. In *2016 second international conference on mobile and secure services (MobiSecServ)*. IEEE, 1–5.
- [32] A. Wool. 2004. A quantitative study of firewall configuration errors. *Computer* 37, 6 (June 2004), 62–67. <https://doi.org/10.1109/MC.2004.2>
- [33] Ronghai Yang, Wing Cheong Lau, and Tianyu Liu. 2016. Signing into one billion mobile app accounts effortlessly with oauth2. 0. *blackhat Europe* (2016).