On Performance and Robustness of Internet-Based Smart Grid Communication: A Case Study for Germany

Sebastian Meiling, Thomas C. Schmidt, and Till Steinbach
{smeiling, t.schmidt, steinbach}@ieee.org
iNET RG, HAW Hamburg – Berliner Tor 7, 20099 Hamburg, Germany

***Abstract*—Emerging Smart Grid solutions require an out-of-band communication channel to enable services such as advanced metering, demand side management, and virtual power plants. The Internet is able to host these highly distributed communication demands, leading the Smart Grid to become an Internet-dependent critical national infrastructure. In this work, we introduce a nation-centric perspective and methodology to shed light on performance and robustness of Internet-based Smart Grid communication. By presenting a case study for Germany, our contributions are: (a) we apply new methods to identify all stakeholders of the energy sector within a national Internet topology, (b) we analyze vulnerabilities of the corresponding communication (sub-)system as part of the current Internet, and (c) we extend our analysis to include Internet access networks of consumer households, where most Smart Grid applications will be implemented. Our findings indicate that the energy-related Internet subsystems are up to 2 times more robust to network failures than the national average. Further, Internet connectivity of consumers households achieves availability of >99 % and is therefore suitable for most Smart Grid applications.**

I. Introduction

Smart Grid applications like *advanced metering infrastructure* (AMI), *demand side management* (DSM), and *virtual power plants* (VPP) rely on a dedicated communication infrastructure, for example to collect sensor data or dispatch device schedules. This out-of-band machine-to-machine communication must be scalable and cost-efficient especially for extensive Smart Grid deployments. Many Smart Grid approaches assign these communication tasks to the Internet [1], using Internet Service Provider (ISP) backbones and home gateways [2]. The decentralized, redundant nature of the Internet bares the potential of providing a communication infrastructure of the desired robustness and resilience to Smart Grids.

But, Internet-based Smart Grid communication raises complexity and vulnerability over traditional power grids which are managed by in-band control, i.e., monitoring of utility frequency, current, and voltage levels. Cascading failures as occurrent in the blackouts of 2003 in Italy and the US/Canada [3], [4] have shown that power grid outages affect Internet communication even outside the blackout areas. Such network failures can lead to a cascade of isolating other networks from the Internet that again lead to further power outages [5]. Other vulnerabilities are prevalent in the Internet routing and can lead to powerful attacks on the communication infrastructure [6]. Smart Grids must be able to detect and mitigate such incidents, and ensure availability and security of the electric utility. Today, power grids and the Internet are considered as critical national infrastructures by most countries. For a better understanding of performance, robustness, and security in Internet-based Smart Grid communication it is vital to analyze the network infrastructure between stakeholders of the energy sector.

For several years, Germany is advancing the proliferation of renewable energy resources, green technologies, and Smart Grids; which motivated our work and its focus on the German energy sector. In this paper, we contribute a methodology to expose the Internet topology of a national energy sector. This provides a unique high-level perspective on the critical infrastructure of Smart Grid communication, which allows us to quantify robustness and resilience to network failures using control plane information. Further, we conducted a measurement study at Internet access networks of consumer households, where most Smart Grid application will be located and implemented. We evaluate performance of household Internet connectivity in terms of availability and latency from a low-level perspective. Briefly said, the presented analysis combines results from control plane and data plane considering the core and edge network infrastructure of the energy sector.

The contributions of our work are structured as follows. In Section III, we introduce a methodology to infer the Internet topology of the German energy sector and discuss our findings. The measurement study and results on Internet connectivity of consumer households are presented in Section IV.

II. Problem Statement and Related Work

Large scale Smart Grid deployments require a communication infrastructure inter-connecting end-devices and stakeholders of the energy sector. While a dedicated infrastructure, e.g., power-line communication (PLC), or cellular networks (GSM/GPRS), for last mile connectivity of energy devices could be necessary, it is too expensive on larger scale. In industrialized countries most households are connected to the Internet, offering easy access to residential and industrial domain to extend (and enhance) smart power grids. Using the public Internet for Smart Grid applications, e.g., AMI, DSM, and VPP, has a huge cost saving potential. Most Internet Service Providers are even present with their own hardware at consumer households, i.e., access routers or Internet modems.

TABLE I
OVERVIEW ON REQUIREMENTS FOR SMART GRID APPLICATIONS, PROPOSED BY U.S. DEPARTMENT OF ENERGY IN [8].

Smart Grid application	ideal latency [ms]		
real-time metering	12	to	20
real-time monitoring	20	to	200
demand response	500	to	2000
in-home applications	2000	to	15000

Extending such devices with Smart Grid functionality can be done with reasonable effort [1], [2], [7] – making the Internet a logical choice to enable Smart Grids.

However, coupling power grids with the Internet introduces new threats with potentially severe impact. Berizzi [3] reports on the Italien power outage of 2003, where insufficient communication results in a failure cascade. Cowie et al. [4] analyze impacts of power outages on Internet communication during the year 2003. They found, that a power outage may lead to subsequent network outages, which cause further power failures – finally resulting in a cascade. Buldyrev et al. [5] describe an analytical model to analyze cascading failures in interdependent networks, e.g., a Smart Grid. A Smart Grid also has to comply with performance requirements on the communication infrastructure. In [8] the U.S. Department of Energy (U.S. DoE) summarizes requirements on latency and availability for Smart Grid applications (see also Tab. I). Finally, privacy and security of Smart Grid communication have to be considered critical as well.

It is therefore important to analyze Internet-based Smart Grid communication assessing characteristics such as availability, latency, and robustness. Luckie et al. [9] presented an analysis of global AS relationships, by monitoring the BGP (*Border Gateway Protocol*) control plane of the Internet routing. Wählisch et al. [10] described an approach to expose a nation-centric perspective on the Internet topology, and analyzed characteristics of commercial and industrial branches. To the best of our knowledge, our work is the first evaluation of Internet-based communication in a national energy sector.

III. THE INTERNET TOPOLOGY OF THE GERMAN ENERGY SECTOR

The goal of our topological analysis is to quantify resilience and robustness of Internet-based Smart Grid communication. Although, there are trans-national power grids, like the UCTE in continental Europe, most power grids are developed along national borders of a country. Power grids and communication networks are considered critical infrastructure by most countries, justifying the nation-centric perspective of our analysis. For this case study, we choose Germany, one of the dominant countries in proliferation of Smart Grid technologies.

A. Methodology

Following the workflow depicted in Fig. 1, we begin by retrieving the list of stakeholders on a national energy sector. This list contains electric utility companies, consumer, transmission and distribution (grid) system operators (TSOs, DSOs), and other distinct key players such as the European Energy eXchange (EEX). In Germany, these companies are registered by the *Federal Network Agency of Germany* [11]. Next, we search for IP address ranges assigned to any of these companies in the RIPE Database. This is individually done for each company by a semi-automatic approach, using keywords and manual corrections to retrieve all IP ranges with high confidence. An automatic algorithm using keywords only did not yield comparable results with the same accuracy, but rather introduced false-positives and missing entries. For faster (off-line) lookups we use split files of the daily RIPE database snapshot, namely `ripe.db.inetnum` [12]. We then determine the corresponding autonomous systems (AS) for each company IP block using public mapping services RIPE whois [13], and UCLA origin data [14].

To infer the AS Internet topology of the German energy sector we use the AS relationship dataset from CAIDA [9], [16]. This dataset enables us to construct a *Type of Relationship* (ToR) AS level graph of the energy-related subsystems within the Internet. The ToR graph consists of directed edges with customer-to-provider (C2P) and peer-to-peer (P2P) AS

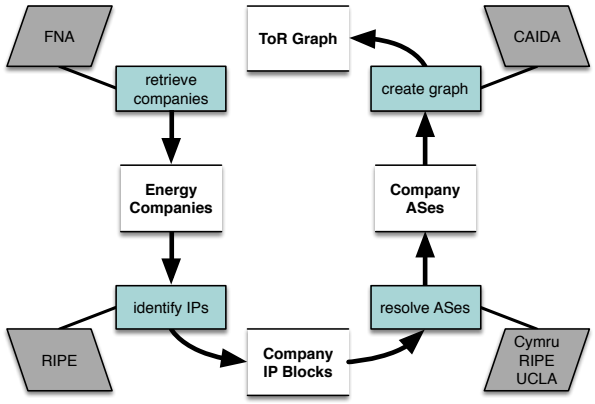


Fig. 1. Workflow to create a high-level view on the Internet topology of the German energy sector. Color legend: grey = input from public data source, green = operation, white = dataset.

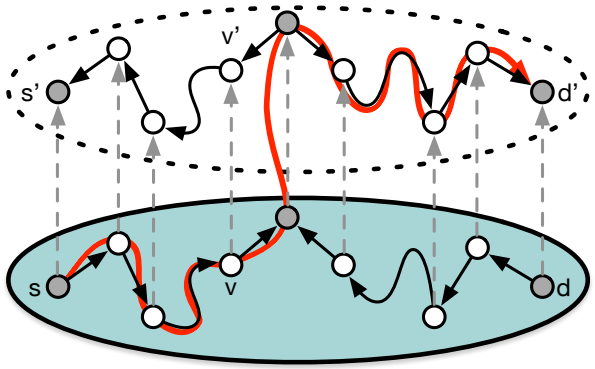


Fig. 2. Transforming a ToR graph using [15] to evaluate the number of disjoint paths between autonomous systems of the German energy sector. First, replace all P2P edge between u, v with corresponding C2P edges. Second, add virtual (upper) layer with reversed edges and connecting edges between layers. As an example, a path between s and d' is highlighted in red.

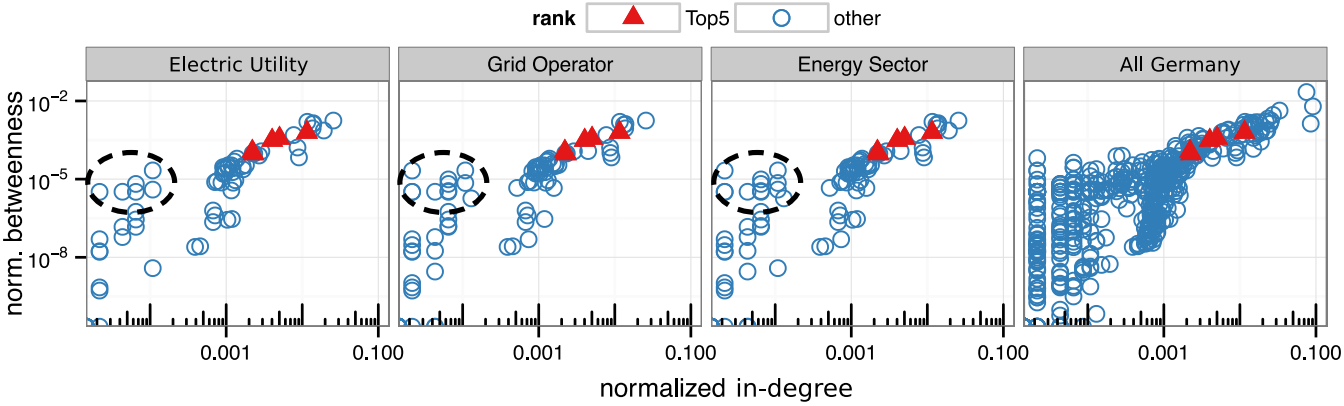


Fig. 3. Correlation of normalized betweenness and in-degree for energy branches and all German AS, verifying significance of AS hosting many energy sector companies. Triangle: Top5 energy sector AS, see Tab. III. Circle: group of notable AS with high betweenness and low degree. Axis are log10-scaled.

TABLE II
OVERVIEW ON NUMBER OF COMPANIES, WITH IP ADDRESSES, DISTINCT IP ADDRESS RANGES, AND ORIGINATING AUTONOMOUS SYSTEMS.

	# companies	# with IPs	# IP blocks	# AS
Electric Utility	463	218	459	88
Grid Operators	889	432	762	112
Energy Sector	1354	652	1050	128

relationships observed by monitoring the global BGP routing.

Base on the ToR graph, we can evaluate classic graph metrics, i.e, betweenness and (in-)degree, to assess the importance of an AS in the Internet topology. The *Betweenness* $B(x)$ of a node (= AS) x is defined as follows: let $|P(u,v)|$ be the number of all paths between AS u and v and $|P(u,x,v)|$ the number of paths between u and v passing through AS x, then betweenness of x is the ratio:

$$B(x) = \sum_{\substack{u \neq x \neq v \\ u \neq v}} \frac{|P(u,x,v)|}{|P(u,v)|}$$

normalized by $(|V|-1)(|V|-2)$, where $|V|$ is the number of nodes in the graph. From a security point of view, AS with high betweenness are potential, high value targets for an aimed attack on the communication infrastructure. The number of one-hop neighbors of an AS is described by the degree of the corresponding node in the routing graph. Specifically, we evaluate incoming (C2P) edges from one-hop neighbors in the ToR graph denoted by in-degree (normalized by $(|V|-1)$). High degree of an AS implies: a) possibly more disjoint paths, and, b) alternative routing paths in case of a link failure.

Further, we analyze robustness, i.e., number of disjoint paths, of the communication network between AS of electric utility companies. This is not directly possible on the plain ToR graph as described above. To solve this, we utilize an approach developed by Erlebach et al. described in [15] to construct a two-layer ToR graph (see Fig. 2). The result is an relationship equivalent representation of the original ToR graph with an additional layer and C2P edges only – all P2P are replaced. This helper construction enables us to retrieve the

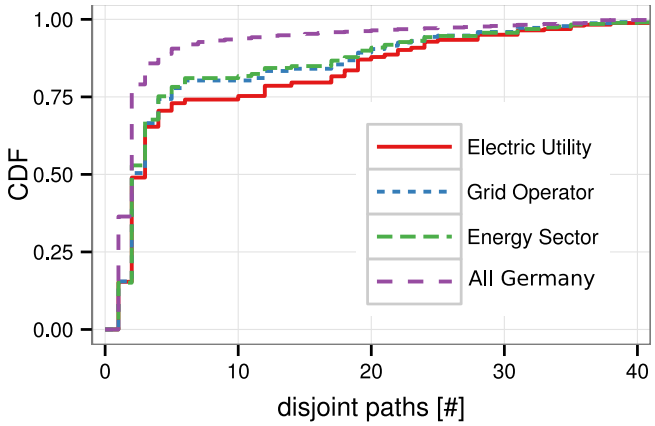


Fig. 4. Comparing CDFs of the average number of disjoint path for AS of the German energy sector and over all German AS.

number of disjoint paths between distinct pairs of company AS in the German energy sector.

B. Results

We retrieved a list of 463 electric utility companies for Germany. Of these, 218 companies have at least one IP address range registered, in total we identified 459 IP ranges mapping to 88 distinct autonomous systems (AS). This method was also applied to identify IPs and AS of grid operators, and combined for the German energy sector. We found that overall roughly 50 % of all companies in the German energy sector have IP addresses registered and, thus are *visible* to our approach. Table II gives a detailed overview on our numerical findings.

Fig. 3 shows the correlation of betweenness and in-degree for AS of electric utility companies, grid operators, the energy sector, and all German AS using the described type-of-relationship graph (ToR graph). We ranked all AS according to the number of hosted companies per energy branch and particularly marked the top 5 ranking AS (see Table III). We found that high ranking AS, also exhibit high values for graph metrics betweenness and in-degree underlining their importance from a graph topological viewpoint. That also

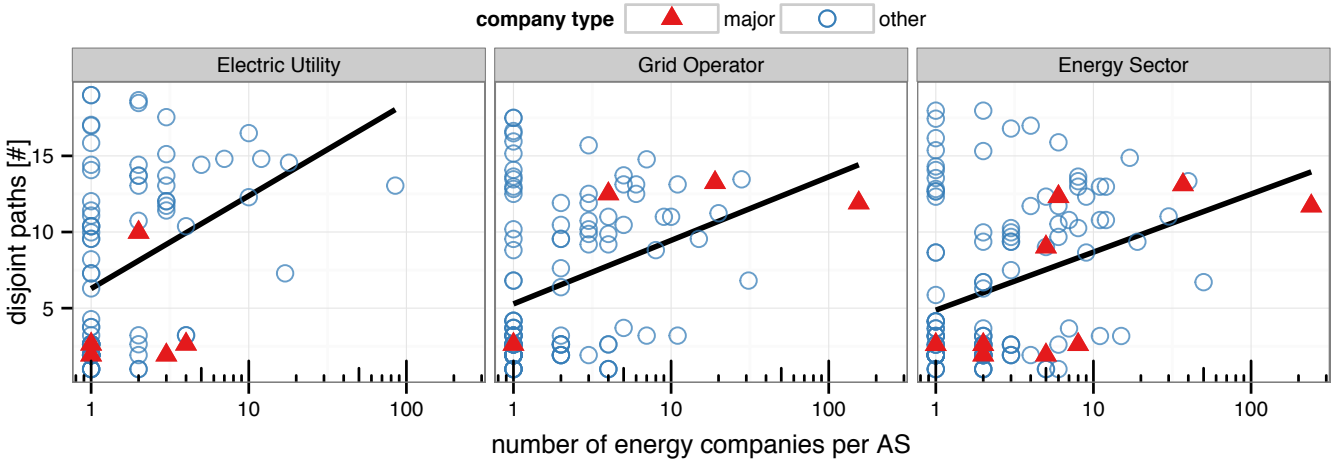


Fig. 5. Correlation of number of companies and average number of disjoint paths per AS, comparing German utility companies, grid operators, and the German energy sector. Triangle: major utilities and grid operators, circle: other energy companies, line: overall trend (linear regression). Log10-scaled x-axis.

TABLE III
OVERVIEW ON TOP 5 AS RANKED ACCORDING TO NUMBER OF COMPANIES HOSTED PER BRANCH.

Autonomous Systems		**# companies**		
Name	Number	Electric Utility	Grid Operator	Energy Sector
DTAG	3320	85	155	241
M-Net	8767	10	20	30
QSC	20676	18	19	37
Versatel	8881	12	28	40
Vodafone	3209	17	31	50

means, these AS are able to mitigate attacks and link failures, e.g., by rerouting. Apart from these top 5 AS, we also discovered a group of AS with high betweenness but low in-degree in comparison (see Fig. 3, marked with circle). This is rather interesting, as betweenness is typically proportional to degree. Our further investigation revealed that these AS belong to regional ISPs and IT service companies with strong business relations to the energy sector.

Next, we quantified robustness by evaluating the number of disjoint paths in the (2-layer) ToR graph between AS pairs of electric utility companies. Fig. 4 compares CDFs over the number of disjoint paths for the energy sectors and all German AS. The results show that the energy sector exhibits significantly more disjoint paths than overall Germany. While only less than 10 % of all German AS pairs have 10 disjoint paths or more, roughly 25 % of the energy sector AS pairs have 10 or more disjoint paths. Moreover, for Germany roughly 30 % have only a single path, but for the energy sector its less than 20 %. We summarize our findings as follows:

1) denser connectivity within the energy sector
2) higher robustness against failure and attacks

Fig. 5 compares number of companies and average disjoint paths per AS for electric utility, grid operators, and the energy sector. AS hosting major electric utility companies (EnBW, E.ON, RWE, and Vattenfall) and transmission system (grid) operators (50Hertz, Amprion, TenneT TSO, and TransnetBW) of Germany are highlighted by red triangles. *Note*: all major utility companies operate their own AS which may include subsidiary companies; while for grid operators only 50Hertz has its own AS. The results show that AS hosting many companies exhibit more disjoint paths on average, resulting in an overall higher failure robustness. However, there are some AS with few disjoint paths that host multiple energy companies, but lack redundant communication paths reducing their robustness to network failures – even AS of major utility companies are within this group.

IV. MEASUREMENT STUDY OF CUSTOMER ACCESS NETWORKS

In our measurement study we evaluate characteristics of the Internet connectivity at consumer households where many Smart Grid applications will be implemented. We deployed 30 measurement probes at households in the metropolitan area of the city of Hamburg (Germany). For the probes we used COTS hardware typical for home gateways, and customized OS software (OpenWrt) to accommodate the measurements. To ensure diversity, we had 9 different Internet Service Providers (ISPs) and several connection tariffs with DSL bandwidths of 6 - 100 MBits downstream and 0.5 - 25 MBits upstream.

A. Methodology

To evaluate availability and reliability of the Internet connection for consumer households we monitored reachability of each probe (gateway) for 2 months. All gateways were configured to contact a server at our university every 5 minutes, sending 8 UDP messages at most – if no response to any of these messages was received, the gateway was assumed to be unreachable (down) for the corresponding 5 min time interval. This represents a typical Smart Grid scenario, where energy devices are controlled by or report to a central instance, such as SCADA system, for electric utility operations.

Further, we evaluated responsiveness (latency, jitter) of the gateways by measuring *one-way delays* (OWD) from and to a reference server at our university, see [17]. In contrast to *round*

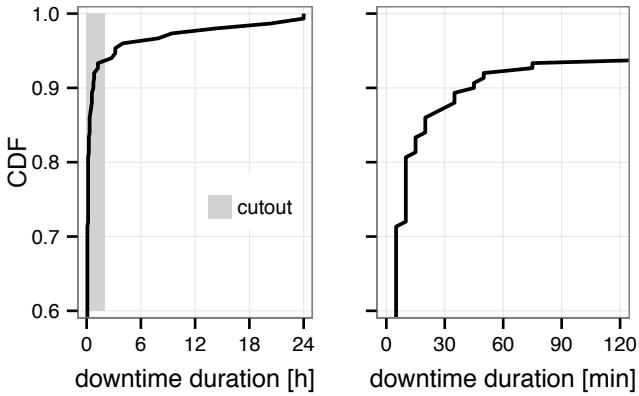


Fig. 6. Distribution of gateway downtime durations. Left: overall downtimes with 1 h precision. Right: cutout for downtimes < 2 h, with 5 min precision.

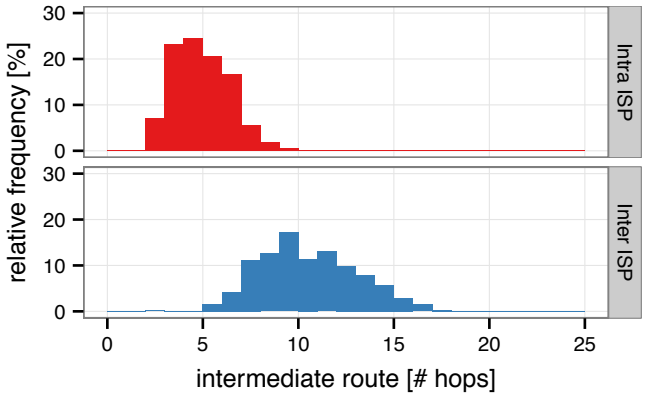


Fig. 7. Distribution of intermediate route length (IP hops) for intra and inter provider (ISP) routes between gateways.

trip time (RTT) measurements, OWD allows to assess latency for send and receive operations separately. Thereby, eliminating artifacts from asymmetries on the routing layer as they can occur for RTT measurements. In a Smart Grid it is mandatory to address characteristics of the communication infrastructure to ensure grid stability, e.g., monitoring and control of the utility frequency has sub-second timing requirements.

To assess privacy and security of Smart Grid communication it is mandatory to understand how and where the data flows through the Internet. Therefore, we analyzed routing paths between all gateway pairs using Scamper [18], an enhanced traceroute-like tool. We retrieved IP addresses of all hops (routers) along each path and derived the path length. Traces were captured 4 times daily (every 6 hours) over 3 months, we distinguish between intra and inter ISP paths.

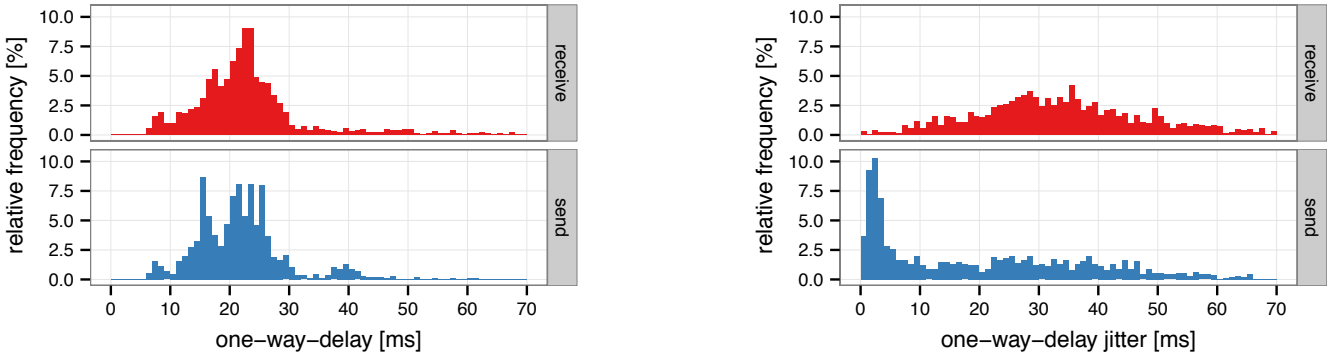
B. Results

Fig. 6 shows the evaluation of gateway availability in terms of downtime duration. We found that downtimes of gateways are highly random and unrelated to each other. Most of the time only a single gateway was affected and never all gateways at once. While downtimes range from 5 minutes up to 24 hours, approximately 90 % of all downtimes are of less than 1 h (see Fig. 6, left). In most cases gateways are unavailable for only a few minutes as shown in the cutout (Fig. 6, right). These short downtimes are likely a result of scheduled reconnects by the ISP (typically every 24 h) or resynchronization of the DSL link; which may happen several times a day. Longer, continuous downtimes are often related to power failures or (intentional) disconnects at the consumer household. Actual downtime may result from a variety of causes unknown to our external observation, e.g., hardware failure, power/network outage at household or ISP. These downtimes have negligible impact on Smart Grid applications, as they are randomly distributed over the day and rarely affect multiple households at the same time. We observed an mean downtime of < 1 % per day, equivalent to less than 15 minutes, which complies to the requirements on reliability by the U.S. DoE [8].

The results of the One-Way-Delay (OWD) measurement are shown in Fig. 8. We compare OWD distribution (Fig. 8(a)) and OWD jitter distribution (Fig. 8(b)) for receiving and sending data separately. While we found that delays differ only slightly, the jitter is significantly lower and more stable when sending. On the sender side average delay is 20 ms and more than 50 % of jitter is below 10 ms. On the receiver side average delay is 22 ms, but jitter range is very broad with 50 % between 20 and 40 ms. Timing sensitive operations or (near) realtime applications, e.g., monitoring and control, could be affected by this jitter asymmetry. Moreover, the OWD measurements revealed a lower bound, limiting the delay at approximately 6 ms on sender and receiver side. According to our results a typical Smart Grid communication scheme using request-response (or offer-answer) takes at least 12 ms, and 42 ms on average to be completed.

While these delays are well below requirements for in-home Smart Grid applications, demand response, and outage management [8] (see Tab. I); real time monitoring or metering cannot be guaranteed at all times. Due to Internet routing policies average delays are nearly equal on a regional (Hamburg), national (Germany), and continental (Europe) scale [7]. Thus, communication delays are independent of size and geographical distribution of Smart Grid deployments.

Fig. 7 shows the intra and inter ISP routing path length evaluation. As expected, intra ISP paths are significantly shorter than inter ISP paths – with average intra ISP path length of 4.5 hops and inter ISP path length of 10.0 hops. However, some gateway pairs exhibit short inter ISP paths, similar to intra ISP paths; and others exhibiting exceptionally long inter ISP paths, respectively. This is due to different peering-relationships between certain ISPs, as our further analysis confirmed: Despite the geographic closeness of all measurement probes (gateways), most inter ISP paths are routed via the DE-CIX (Frankfurt, Germany) – the most prominent Internet eXchange Point (IXP) of Germany, where many ISPs peer with each other. But we also found, that some ISPs have peering relationships using IXPs in Hamburg (ECIX) or Berlin (BCIX), resulting in shorter inter ISP routing paths. While, smaller ISPs even tend to use foreign IXPs, i.e., AMS-IX (Amsterdam, NL), to route data from and to larger ISPs, resulting in longer routes. We conclude that ISPs have



(a) One-way-delay of all gateways sending (receiving) to (from) a server.

(b) One-way-delay jitter of all gateways while sending and receiving.

Fig. 8. Comparing OWD between reference server acting as source and destination respectively and all gateway probes at consumer households.

significant impacts on Smart Grid communication in terms of performance (e.g. latency, jitter), security, and even privacy – for example when data is routed through foreign countries with different legislation.

V. Conclusion and Outlook

In this work, we presented a case study on performance and robustness of Internet-based Smart Grid communication in the German energy sector. Using our methodology to expose and analyze the national Internet topology, we found that the Internet subsystem of the German energy sector exhibits significantly more disjoint (redundant) network paths. This means that the energy-related infrastructure is up to 2 times more robust against network failures than the national Internet infrastructure in general. Further, we presented a measurement study on Internet connectivity of consumer households to evaluate reliability and performance for Smart Grid applications. The results revealed a high reliability (>99 %) of the Internet connection with average downtimes of less than 1 % per day. These downtimes are randomly distributed, not affecting multiple households at once, and are thus negligible for most Smart Grid applications. The latency measurements showed that requirements of in-home Smart Grid applications and demand response are met, while real time metering and monitoring can be challenging. We also found that some (smaller) ISPs tend to route data via foreign countries, which threatens privacy and security of Smart Grid communication.

In our future work, we will extend our analysis to other countries of the European Union to cover the continental UCTE power grid. This will contribute to a better understanding of future Smart Grid communication and interdependencies of critical infrastructures across countries.

Acknowledgement

This work is funded by the Federal Ministry of Economics and Technology of Germany (BMWi) within the project Smart Power Hamburg and by the Federal Ministry of Education and Research of Germany (BMBF) within the project Peeroskop.

References

[1] T. Sauter and M. Lobashov, "End-to-End Communication Architecture for Smart Grids," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 4, pp. 1218–1228, Apr. 2011.

[2] S. Meiling, T. Steinbach, T. C. Schmidt, and M. Wählisch, "A Scalable Communication Infrastructure for Smart Grid Applications using Multicast over Public Networks," in *Proc. of ACM Symposium on Applied Computing (SAC'13), Poster Session*. March 2013.

[3] A. Berizzi, "The Italian 2003 Blackout," in *IEEE Power Engineering Society General Meeting*, vol. 2, 2004, pp. 1673–1679.

[4] J. H.Cowie, A. T. Ogielski, B. Premore, E. A. Smith, and T. Underwood, "Impact of the 2003 Blackouts on Internet Communications," http://www.renesys.com/wp-content/uploads/2013/05/Renesys_BlackoutReport.pdf, Renesys Corporation, Tech. Rep., Nov. 2003.

[5] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[6] D. M. Slane, C. Bartholomew *et al.*, "2010 Report to Congress," U.S.–China Economic and Security Review Commission, Annual Report, November 2010. [Online]. Available: http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf

[7] S. Meiling, T. Steinbach, M. Duge, and T. C. Schmidt, "Consumer-Oriented Integration of Smart Homes and Smart Grids: A Case for Multicast-Enabled Home Gateways?" in *3rd IEEE Int. Conf. on Consumer Electronics - Berlin (ICCE-Berlin'13)*. Sep. 2013, pp. 279–283.

[8] U.S. Department of Energy, "Communication Requirements of Smart Grid Technologies," http://energy.gov/gc/downloads/communications-requirements-smart-grid-technologies, Oct. 2010.

[9] M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, and k. claffy, "AS Relationships, Customer Cones, and Validation," in *Conference on Internet Measurement Conference (IMC'13)*. 2013, pp. 243–256.

[10] M. Wählisch, T. C. Schmidt, M. de Brün, and T. Häberlen, "Exposing a Nation-Centric View on the German Internet – A Change in Perspective on the AS Level," in *13th Passive and Active Measurement Conference (PAM)*, ser. LNCS, vol. 7192. 2012, pp. 200–210.

[11] "Federal Network Agency of Germany (Bundesnetzagentur)," http://www.bundesnetzagentur.de/cln_1911/EN/Home/.

[12] "RIPE database, daily snapshot," ftp://ftp.ripe.net/ripe/dbase/split.

[13] "RIPE Whois Database," www.ripe.net/data-tools/db/whois.

[14] "UCLA Internet AS-level Topology Archive, IPv4 Prefix Origin," http://irl.cs.ucla.edu/topology/ipv4/origin/.

[15] T. Erlebach, A. Hall, A. Panconesi, and D. Vukadinović, "Cuts and Disjoint Paths in the Valley-free Path Model of Internet BGP Routing," in *1st Int. Conf. on Combinatorial and Algorithmic Aspects of Networking (CAAN'04)*. 2004, pp. 49–62.

[16] "The CAIDA AS Relationships Dataset, 01.06.2014." http://www.caida.org/data/as-relationships/.

[17] S. Meiling, T. C. Schmidt, and M. Wählisch, "Large-Scale Measurement and Analysis of One-Way Delay in Hybrid Multicast Networks," in *37th Annual IEEE Conf. on Local Computer Networks (LCN'12)*. Oct. 2012.

[18] M. Luckie, "Scamper: A Scalable and Extensible Packet Prober for Active Measurement of the Internet," in *10th ACM SIGCOMM Conference on Internet Measurement (IMC'10)*. 2010, pp. 239–245.