DETECTING POWER OUTAGES IN LOW-VOLTAGE NETWORKS FROM TELECOMMUNICATIONS NETWORKS DATA

Marleen Bahe, Matthias Herlich, Peter Dorfinger
Salzburg Research Forschungs-gesellschaft – Austria
<first>.<last>@salzburgresearch.at

Josef Leist, Christian Wohlsein
Salzburg AG für Energie, Verkehr und Telekommunikation Austria
<first>.<last>@salzburg-ag.at

Markus Radauer, Gerald Hörack, Walter Schaffer
Salzburg Netz GmbH – Austria
<first>.<last>@salzburgnetz.at

ABSTRACT

Equipping low-voltage networks with sensors to detect power outages would be a large effort; consequently, low-voltage networks usually do not contain sensors to detect power outages.
When telecommunications equipment is affected by a power outage, the disconnection from the telecommunications network can be automatically detected almost in real-time.
To test the feasibility of detecting power outages from telecommunication losses, we analyzed the disconnections of telecommunications equipment in retrospect to determine if the cause was a power outage.
Our analysis showed that the ability to detect power outages from telecommunication losses depends on the prevalence of telecommunications equipment and the similarity of the telecommunications and energy network topology.
In the future, methods similar to the ones described in this paper can be used to inform an energy network operator about outages and make it easier for a telecommunications provider to determine the causes of connection losses without the need to install any additional equipment.

INTRODUCTION[1]

Low-voltage networks often do not have an automatic detection of power outages. Such outages are usually detected by the customers and then reported by telephone to a customer center. Automatic detection of power outages within the low-voltage network can save time, reduce costs and increase customer satisfaction. However, it usually requires installing additional hardware. An alternative we test in this paper is to use available information from telecommunications networks. The main idea is, if the power supply fails, telecommunications networks will fail as well. These telecommunications failures will be automatically detected and can be used to infer the root cause. To determine the feasibility of the concept, we analyzed how effective the detection of power outages with telecommunications networks would be by a Data Over Cable Service Interface Specification (DOCSIS) network. This network provides automatic detection of outages and there is a lot of end user equipment in the operation area of the distribution system operator represented in this work. Although the number of customer systems in the DOCSIS network is significantly smaller than the number of customer systems that can be affected by an outage, it is possible to detect outages for most of the customer systems. This is because of the tree structure of the network.

RELATED WORK

There is research [1] on finding the optimal placement of outage sensors within a network by using as few as possible sensors while achieving a high detection rate. The proposed outage detection framework for power distribution networks achieves a mean detection error probability of 10 % by having a sensor density of 30 % for a typical feeder.
Another approach to detect power and communication outages is to use news of natural disasters, since outages are consequences of events like these. One paper [2] considered Twitter messages to search for keywords that are related to power and communication outages. Machine learning algorithms were used to define these keywords and to interpret the messages for classification of the type of outage. Other work [3] also presents a machine learning method to detect the location of a power outage from Twitter messages.
A cooperation between energy and telecommunications providers, to share outage information, exists [4,5], but we are not aware of any technical documentation.
In contrast to all other work presented in this section, we use the automatic detection of connection loss in telecommunications networks to infer whether the cause is in the power network.

EXPERIMENTAL SETUP AND METHODS

The algorithm to decide whether an outage alert of the DOCSIS network is caused by a power outage or not is based on the fact that the DOCSIS network and the power network overlap. Both networks have a structure of trees

1 This paper is a preprint of a paper accepted by CIRED 2023 and is subject to Institution of Engineering and Technology Copyright. When the final version is published, the copy of record will be available at IET Digital Library.

and at the leaf nodes are customer systems that are supplied with power, telecommunications services or both.

Telecommunications network

Within the telecommunications network, we are focusing on the DOCSIS network as most of the telecommunications customers are in the DOCSIS network. Additionally we will use diagnostics from other telecommunications networks such as Smart Meters equipped with GSM modules, fixed wireless access and fiber-optic networks. Most of the Smart Meters are connected with PLC (power line communication). We do not take into account this network, as PLC does not offer reliable diagnostics on the reachability status of the Smart Meters.

DOCSIS network

The DOCSIS network consists of 1500 trees with 10 600 amplifiers in total. There are 630 trees with only one amplifier and the other trees have 11.5 amplifiers on average. At the leaf nodes, there are 108 000 customer systems, whereby one amplifier supplies between 0 and 400 customer systems.

Our collected data of DOCSIS outages covers the range between 2019 and 2022.

The outage detection within telecommunications networks is usually optimized for the detection of telecommunication outages and drops data, which is not needed for this purpose. The raw data to detect power outages is often not available for historical events.

In our case, the outage detection within the DOCSIS network is implemented by an automatic check every 5 minutes, comparing how many customer systems are now offline compared to the last check. An alert is generated for the amplifier which is the furthest up within the appropriate tree, to which the condition "all but one customer systems are offline" applies. The reason for all but one is that wrong tree assignments may exist in the data.

Since there were repetitions of alerts from the same subtree, online reports within the list of alerts and faulty alerts, the list of all alerts had to be preprocessed.

Whereas the data of the alerts are collected over a time range of 3 years, the historical data of the network topology is available at only one point in time. Due to construction work within the network, this results in discrepancies. For example, we see alerts for amplifiers that are not present in the network topology. This means that we underestimate the real potential of our approach.

As a future step, we plan to implement a prototype system with a decision algorithm, that is fed with live data and with status messages (online or offline) for each customer system separately.

Other telecommunications networks

In addition to the DOCSIS network, in the next step we consider using the following networks to detect power outages:

(1) the GSM-based Smart Meter network
(2) the fixed wireless access communication
(3) the fiber-optic network

Power network

The power network consists of 5300 trees. The root node of a tree is denoted as node 1. Each node 1 is connected to one or two nodes 2. In total 16 720 low-voltage feeders and over 400 000 customer systems are supplied with power. Because the data represents only a single point in time and does not reflect changes over time, some customer systems and low-voltage feeders are not listed in the topology.

If there is an outage of a complete node 1 within the high or middle voltage network, an outage alert with seconds accuracy is generated. For our analysis, outages between 2010 and 2021 were considered.

With an outage in the low voltage network, one of several feeders are affected. Since there is no automatic detection of feeder outages, outages are manually documented if an affected customer reports the outage. We have used a list of reported outages between 2010 and 2022. Because the data of the network topology is captured only once, outage messages occur which are not attributable.

DETECTION ALGORITHM

To calculate the potential of detecting low-voltage network outages by unreachable telecommunications equipment, we used both power and telecommunications network topologies. Thereby, we assumed a low-voltage problem would affect customer systems in the same feeder. Then, we analyzed for each feeder where its customer systems are located in the DOCSIS network. According to the following cases (visualized in Figure 1), different conclusions are possible:

(1) None of the customer systems on a feeder are part of the DOCSIS network: no outage detection.
(2) All customer systems of a feeder are located in one subtree of the DOCSIS network and there are no other customer systems in the DOCSIS network subtree: an outage can be detected, but the cause cannot be assigned to one of the networks.
(3) All customer systems of feeder are located in one subtree within the DOCSIS network and the subtree contains customer systems from another feeder: an outage can be detected and assigned to the correct network.
(4) The customer systems of a feeder are distributed over several subtrees in the DOCSIS network: an outage can be detected and assigned.

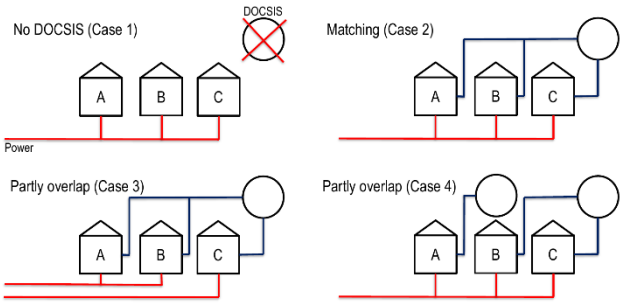

Figure 1: Cases of network overlaps for detecting outages

This first analysis assumes outages are equally probable in both types of networks. However, in reality the outage rates differ, so we numerically analyzed the outage alerts from several years and approximated probabilities of outages dependent on time, weekday, month and region (city or county).
Furthermore, other telecommunications networks also provide automatic outage detection. They can be used in the same way as the DOCSIS network to detect power outages. We extended our analysis similarly to include these sources of information.

RESULTS AND DISCUSSION

In a first step, we have analyzed the intersection of the power network and the DOCSIS network to estimate the potential that they can provide information about each other. Then, we tried to find outage alerts that occur in the power network and in the DOCSIS network. These allow us to estimate the number of DOCSIS outage alerts, which are caused by outages in the power network. Since the collected alerts from the DOCSIS network are generated per amplifier and not per customer system, we also analyzed the potential detectability of power outages from outage alerts from single customer systems within the DOCSIS network. Finally, we considered historical data from real power outages and DOCSIS outages to evaluate the statistical frequency of outages dependent on time, weekday, month and geographical location.

Overlap of power network and DOCSIS network

Within the low voltage network, there are 16 720 feeders that can be affected by an outage. Since there are no outage sensors that belong to this network, we considered outage reports from the DOCSIS network to indicate power outages from these feeders. In a first step, it is interesting to analyze the intersection of the power network and the DOCSIS network. Therefore, we have evaluated the number of feeders of the power network, that contain at least one customer system of one of the DOCSIS network. In Figure 2, it can be seen that, 10 347 feeders contain equipment from the DOCSIS network. Furthermore, there is an intersection of 1836 feeders with outage reports from the GSM Smart Meter network. Interestingly, there are only 367 feeders, which contain both types of customer systems. In addition, the reports from other telecommunications networks can increase the information content. In total, there are 12 254 feeders, that contain at least one customer system from any telecommunications network. These feeders cover 85 % of the customers systems.

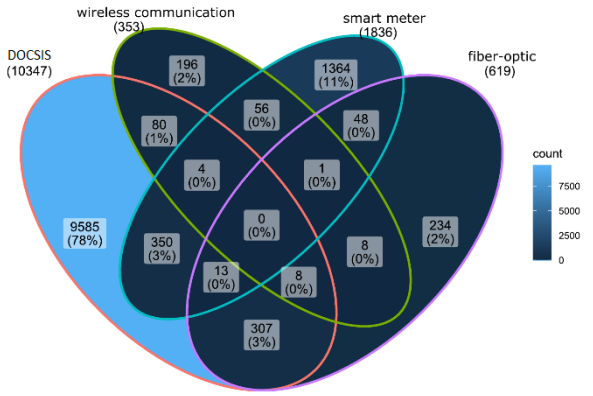

Figure 2: The Venn diagram shows the overlap of customer system from telecommunications networks for the 16 720 feeders within the power network.

Overlap of power outages and DOCSIS outages

For the intersection of the different outages documented in the past, we take the list of real outages within the high and middle voltage network and then search for outage alerts within the list of the DOCSIS network in a temporal propinquity of 24 hours. This shows that 30.4 % of the power outages also show up in the alert system of the DOCSIS network. From the other perspective, 11.3 % of the DOCSIS outage alerts are consequences of outages within the power network and occur up to 10 minutes after the actual outage in the alert system (the status of the amplifiers within the DOCSIS network is updated only every 5 minutes).
If we do the same analysis with the outages within the low voltage network, the result is sobering. Only 0.4 % of the recorded outages can be found in the list of DOCSIS outage alerts.
The reason for the small intersection is the aggregation during the generation of alerts in the DOCSIS network per amplifier. If an outage in the low voltage network does not affect all customer systems (besides one) of any amplifier, there will be no alert and this power outage is not detectable. The outages of the low voltage network are too small or too distributed for triggering an outage alert of the DOCSIS network, when the DOCSIS outages are aggregated to the amplifier level.
The generation of alerts per amplifier is a step of aggregation that leads to an incomplete view of the status of the whole network. It can happen that only a few customer systems are offline without any alert, if customer systems at the same amplifier are online. For the detection of outages within the DOCSIS network, this view might be sufficient. For detecting power outages, which indeed cause situations like this one, it would be helpful if the status of every customer system is reported.

Detecting power outages from telecommunications networks

In the next step, we tested how a hypothetical alert system would work, if it had access to the status of each customer systems (and not aggregated to each amplifier). Therefore, we have calculated for how many customer systems it is principally possible to detect outages from the overlapping telecommunications networks. The following Table shows the fraction of covered low-voltage feeders, for which a power outage can be detected with the help of the telecommunications networks (D = DOCSIS, S = GSM Smart Meter, W = fixed wireless access communication and F = fiber-optic).

Table 1: Fraction of covered feeders by telecommunications technology

Case	D [%]	D&S [%]	D&W [%]	D&F [%]	All [%]
1	38.1	29.2	36.5	36.4	26.7
2	5.9	5.0	5.8	5.7	4.7
3 + 4	55.9	65.8	57.6	57.9	68.6

By only using the outage reports from the DOCSIS network, for 55.9 % of all low-voltage feeders an outage detection is possible. By querying Smart Meters we can increase the percentage by 10 %. In addition, if all data sources are combined, the detection of low-voltage outages in 68.6 % of the feeders can be realized. We conclude that the combination of telecommunications networks is suited to detect most power outages.

Because the number of customer systems per feeder differs, the following Table shows for how many customer systems, a power outage detection is possible because of telecommunications systems somewhere in the feeder. It shows the percentage of customer systems at feeders in power network, for which a power outage can be detected with the help of outage reports from the telecommunications networks (D = DOCSIS, S = GSM Smart Meter, W = fixed wireless access communication and F = fiber-optic)

Table 2: Fraction of customers in feeders covered by telecommunications technology

Case	D [%]	D&S [%]	D&W [%]	D&F [%]	All [%]
1	22.9	20.8	21.4	21.7	18.5
2	5.2	4.9	5.1	4.8	4.4
3 + 4	71.9	74.3	73.5	73.5	77.1

Interestingly, the feeders which contain equipment from the DOCSIS network are feeders with many customer systems. In total, the detection of low-voltage outages should be possible for 77.1 % of all customer systems.

Frequency of types of outages in historical data

Our algorithm to classify whether an outage alert is caused by an outage in the DOCSIS network or in the power network is based on the assumption that each type of outage is equally probable. To get a better prognosis, we computed the probability of the type of outage by looking at historical data of real outages in both types of networks. For this purpose, we used historical data of outages over several years.

First, we considered all customer systems of the power network and the DOCSIS network. More specifically, we determined how many times, on average, a customer system is affected by an outage of each type. It turned out, that on average, a customer system is affected by a DOCSIS outage 64 times as often as a customer system is affected by a power outage (in the low-voltage network). This means, by looking at an outage alert, which could be either an outage in the DOCSIS network or in the low-voltage network, that with a probability of 1.5 % this alert is caused by a power outage (in the low-voltage network). Furthermore, we have also analyzed if the probability of outage type depends on the features: weekday, month and geographical region. Indeed, there are dependencies, which are visualized in Figure 3. The largest difference is that outages a far more probable in Region F than in any other region.

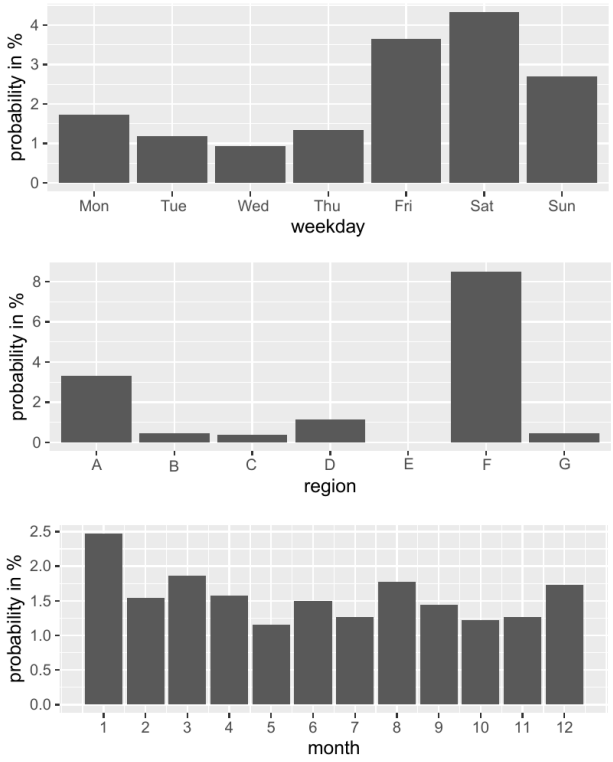

Figure 3: Probability that a telecommunications outage is caused by of a power outage in the low-voltage network (compared to an outage in the DOCSIS network) dependent on the features: weekday, geographical region and month.

CONCLUSION

We described how outage data from a telecommunications network can be used to detect power outages in a low-voltage power network. This information can be used by both the power network operator and the telecommunications network operator to increase the availability of the network. Telecommunications outages which have been aggregated to detect telecommunications outages might not be helpful to detect power outages. To detect power outages the aggregation has to be avoided or adopted for multi-purpose usage. In conclusion, we estimate that for 77.1 % of all customer systems, our method is able to detect outages in the low-voltage network by looking at outage alerts of telecommunications networks.

In a next step, we plan to test the algorithm for classification of outage type on live data.

REFERENCES

[1] Raffi Avo Sevlian, Yue Zhao, Ram Rajagopal, Andrea Goldsmith, and H Vincent Poor, "Outage detection using load and line flow measurements in power distribution systems," IEEE Transactions on Power Systems, vol. 33, no. 2, pp. 2053–2069, 2017.

[2] Udit Paul, Alexander Ermakov, Michael Nekrasov, Vivek Adarsh, and Elizabeth Belding, "# outage: Detecting power and communication outages from social networks," in Proceedings of The Web Conference 2020, 2020, pp. 1819–1829.

[3] Huina Mao, Gautam Thakur, Kevin Sparks, Jibonananda Sanyal, and Budhendra Bhaduri, "Mapping near-real-time power outages from social media," International Journal of Digital Earth, 2018.

[4] Westenergie, "Vodafone dockt an Störungsauskunft.de von Westenergie an", 2022-1-19, https://news.westenergie.de/vodafone-dockt-an-stoerungsauskunftde-von-westenergie-an/

[5] Henning Gajek, „Vodafone kooperiert mit störungsauskunft.de", 2022-01-22, https://www.teltarif.de/stoerungen-vodafone-westenergie/news/86993.html