Essay

Gregor Garten
gregor.garten@mailbox.tu-dresden.de
Technische Universität Dresden
Dresden, Sachsen

1 PROBLEM STATEMENT

The electrical grid is facing a structural transformation through the increase of power sources. Instead of few power plants, which are producing a high amount of electricity, the electrical grid is changing to more and more smaller producers like wind turbines or other renewable technologies. Even single-family houses are able to inject electricity into the power grid through solar panels installed on the roof. As a consequence the electrical grid gets a third participant the so called prosumers who can consume electricity as well as produce it. The new distribution of consumers, producers and prosumers poses a difficult task for grid operators since it becomes harder to track electricity supply and demand. To tackle this issue, smart meters are introduced to the power grid by installing them in the households. Smart meters can send the current electricity consumption of the customers to the electricity provider solving the problem of demand and supply. However, that creates a new privacy problem for the customers. Smart meters usally communicate every 15 minutes with the electricity provider enabling the possibility for a accurate behavior analysis of the customer like daily routines and religious affiliation. In this master thesis the goal is to implement a solution which provides all the advantages of smart meters like better electricity rate, but also solve the privacy issues.

2 MOTIVATION

The introduction of smart meters into the power grid poses a new challenge to the privacy of households. First, the higher resolution of data allows a behavior analysis based on electricity usage patterns. This information could be stored by electrical providers and used further for specialized advertisement on households. Second, some individuals may want to hide their electricity consumption now or in the future. Because global warming steadily raises the awareness of the society and sustainable living becomes more important. Therefore a high electricity consumption can harm the image of people [4].

3 BACKGROUND

The smart meter privacy problem can be divided into two sub-problems: Metering for Billing and Metering for Operation. Only if those two problems are handled properly it is possible to achieve real privacy. In metering for operation the goal is to implement a privacy preserving solution which prevents a behavior analysis based on electricity usage patterns. Since the electrical provider only needs an overview of the electrical consumption of all smart meters in an area. Furthermore it is important to find a solution for metering for billing that makes it impossible to indirectly learn about the electricity consumption by billing the customer. At the same time the billing has to be valid and cant be tampered. This master thesis will primary focus on metering for operation.
First approaches of the analysis of electricity usage patterns can be found in 1999 [1]. Afterwards several processes are suggested in different works to solve the issue. A common approach is to hire a trusted third party, which is another agent in the power grid trusted by all participants. The trusted third party act as a computation center, which receives all information from smart meters in a specific location, computes it and sends the anonymized information to the electricity provider. Therefore the electricity provider can't assign the data to specific households. Another feasible solution is a implementation of a homomorphic cryptographic scheme. These are asymmetric algorithms with the possibility of basic operations like addition on the ciphertext. That allows the smart meter to encrypt its information

and send it to a central storage. In the central storage the encrypted messages of all smart meters are summed together and a electricity provider can ask for that information to gain the total electricity consumption of a region. More approaches can be found in [2][3].

4 OUR APPROACH AND EVALUATION

This master thesis will focus on a solution which is called dining cryptographer network often referred as DC-net. It is invented by David Chaum and secures anonymous communication. In a previous work two small power grids are created with Gridlab-D. The task is to implement a DC-net into the simulator and analyse which effects the DC-net has on the simulations and if sender anonymity is achievable for the smart meters. If smart meters can communicate anonymously with the electricity provider, the provider can't assign the data to specific households. Afterwards different questions need to be answered in a evaluation. For example how much information can be extracted out of the aggregated data from the smart meters or how much smart meters have to be aggregated to attain a specific level of privacy. Therefore the collected data has to be visualized to gain an overview and to simplify the analysis of the results. Also a interesting approach is to create an experimental environment which emulates a micro power grid. For this various raspberrypis would imitate real components of a power grid, which would communicate with the proposed solution. The insights of the experimental environment could additionally prove the results of the simulation or it could be a first hint for refutation of the approach.

5 SOLVING THE PROBLEM

Smart meters should achieve sender anonymity if a DC-net is implemented into the power grid simulation. Therefore smart meters could communicate the aggregated overall electricity consumption without fearing, that the electrical provider is misusing the private data of individual households as it is not feasible to gain information of the attained data.

6 TIMEPLAN

Week	Task
Week 1 - 4	review literature and common proposed solutions for related work and state of the art chapter.
Week 5	Start design phase for an implementation into Gridlab-D. Find potential parts of the software where the algorithm can be implemented without restrictions for further extensions (if something needs to be fixed/changed later)
Week 6 - 7	Implementation of the DC-Net into Gridlab-D
Week 8 - 9	Setting up an experimental environment with raspberrypis for additional collection of results
Week 10 - 12	Run different experiments. Collect results. Maybe corrections on the algorithm/experimental setup if problems occur.
Week 13 - 15	Analyse results. Create graphs to illustrate the results. Start writing.
Week 16 - 20	Continue writing. Start correction phase of the master thesis.
Week 21	End correction phase of master thesis.
Week 22	Some time for final details which are left over during the previous weeks.

Table 1: Timeplan for the master thesis.

REFERENCES

[1] S. Drenker and A. Kader. Nonintrusive monitoring of electric loads. *IEEE Computer Applications in Power*, 12(4):47–51, 1999.

[2] Zhong Fan, Parag Kulkarni, Sedat Gormus, Costas Efthymiou, Georgios Kalogridis, Mahesh Sooriyabandara, Ziming Zhu, Sangarapillai Lambotharan, and Woon Hau Chin. Smart grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Communications Surveys & Tutorials*, 15(1):21–38, 2012.

[3] Sören Finster and Ingmar Baumgart. Privacy-aware smart metering: A survey. *IEEE communications surveys & tutorials*, 17(2):1088–1101, 2015.

[4] Dr. Heike Le Ker. "umwelt-heuchler" streit um al gores energieverbrauch.