Master's Thesis

Privacy-preserving Smart Metering Using DC-Nets

Gregor Garten

December 6, 2021

TU Dresden
Faculty of Computer Science
Institute of Systems Architecture
Chair of Privacy and Data Security

Supervisors: Dr. Stefan Köpsell
Dr. Elke Franz
Betreuender Mitarbeiter: Dipl.-Inf. Tim Lackorzynski

Lorem Ipsum

Selbständigkeitserklärung

Hiermit erkläre ich, dass ich diese Arbeit selbstständig erstellt und keine anderen als die angegebenen Hilfsmittel benutzt habe.

Dresden, den **?today?**

Gregor Garten

Abstract

. . . abstract . . .

write abstract

Contents

Todo list

List of Figures

List of Tables

1 Introduction

adopt title page

adopt disclaimer

write introduction

1.1 A Section

Referencing other chapters: 2 3 4 5 6 7

Name	Y	Z
Foo	20,614	23 %
Bar	9,914	11 %
Foo + Bar	30,528	34 %
total	88,215	100 %

Table 1.1: Various very important looking numbers and sums.

More text referencing Table 1.1.

1.2 Another Section

Citing [**bellard2005qfa**] other documents [**bellard2005qfa**; **boileau06**] and Figure 1.1. Something with umlauts and a year/month date: [**becher04:˙feurig˙hacken˙mit˙firew**]. And some online resources: [**green04**], [**patent:4819234**]

1.3 Yet Another Section

add content

1.4 Test commands

DROPS L^{4}LinuxNOVA QEMU `memcpy` A sentence about BASIC. And a correctly formatted one about ECC.

Figure 1.1: A long description of this squirrel figure. Image taken from `http://commons.wikimedia.org/wiki/File:Sciurus-vulgaris_hernandeangelis_stockholm_2008-06-04.jpg`

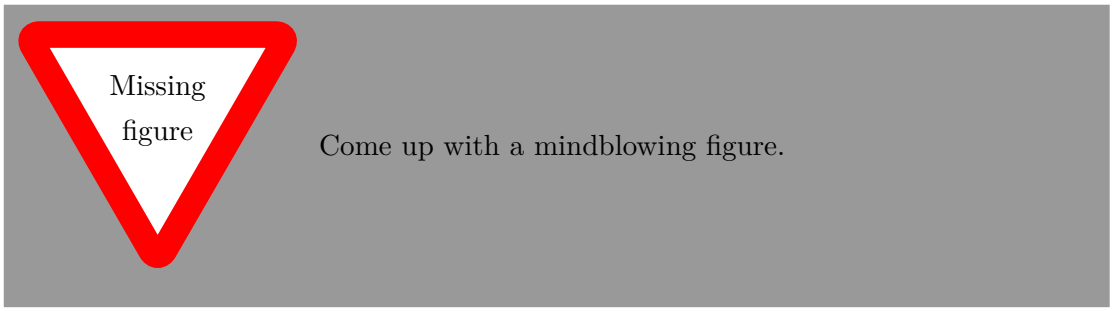

Figure 1.2: A mindblowing figure

2 Technical Background

This section introduces an overview of the basic concepts for this work. Therefore, the key components of the smart grid are explained, what structural changes and what challenges the smart grid will bring. In addition, this chapter discusses the current state of research.

2.1 Smart Grid

The original energy network was mainly considered as a transmission system to send electricity from the generators via a elongated network of cables and transformers to the consumers.Instead of a few electricity producers (e.g. nuclear power plants, coal-fired power plants), which were responsible for a large part of the electricity generation, there are now many smaller producers (e.g. wind turbines). However, renewable power generation is often dependent on external environmental factors. In order for the smart grid to be stable despite fluctuations in power generation, smart meters have been introduced. This enables the electricity provider to receive the electricity consumption of a household every 15 minutes. It offers the possibility to get more easily the current electricity demand from the consumers. Previously, the current electricity demand was simulated from load forecasting models. If the demand should increase spontaneously, peaker plants, mainly consisting of coal-fired power plants, would be turned on to quickly meet this demand. This is costly and environmentally unfriendly. Since then, structural changes have been made to optimize the energy grid and make it more intelligent by exchanging information in near-real-time. This allows the demand to be matched to the available supply. The fundamental component of the smart grid are the smart meters, which were already mentioned. They which will be discussed in more detail in the next section.(Quelle:Smart Grid Communications)(Privacy Survey2013)

2.2 Smart Meter

Smart meters are the key component in a smart grid. A smart meter is an electricity meter that has an interface to the Internet. It enables two-way communication between the control center and the meter. This is also called Advanced Metering Infrastructure (AMI). Two-way communication improves the quality of the power grid and makes it possible to offer services that would not be feasible without a smart meter. For example it's now practicable to detect power outages.As a result, the power grid operator can detect power failures on its own. Previously, the operator was dependent on customer calls to detect power outages. Another new feature is detailed monitoring of power

flows at the smart meter. Before, power flows could only be measured up to substations. This new function enables electricity network operators to quickly detect changes in consumption behavior and react to them without having to use peaker plants, which are costly and environmentally unfriendly. Depending on the setting, smart meters can send electricity consumption to the electricity provider at least every 15 minutes. In combination with the consumption of all users and the current electricity supply, a better price can be achieved. This is also called real-time pricing. So not only can the customer be offered a better electricity contract, in addition the meters no longer have to be read at home by a technician from the electricity provider. This makes billing easier for customers and electricity providers. Furthermore, customers can also check their current electricity consumption via the interfaces provided by the smart meter in order to analyze their own behavior and to reduce their consumption. (Privacy-Aware Smart Metering)

2.3 Smart Meter Privacy

The main advantage of the smart grid is the communication between the consumers and the energy suppliers. It is precisely this communication that solves a lot of structural problems in today's energy system. However, sending user information every 15 minutes allows for new methods that can be used to create accurate behavioral analyses in one's own home. Sending private electricity consumption data is therefore very sensitive information and must to be protected. This is not an easy task, because on the one hand the electricity consumption must be protected and anonymized, and on the other hand the billing and costs must be clearly assignable to a person. In the following paragraphs, we will describe how simple behavioral analyses are generated by electricity consumption. Subsequently, solutions to Metering for Billing and Metering for Operations will be presented, which have been discussed in the scientific community so far.(Privacy-Aware Smart Metering)

2.3.1 Non-intrusive load monitoring

Interpreting power consumption with the intent of identifying devices in the home is called non-intrusive load monitoring (NILM). George Hart and Fred Schweppe were the first to develop non-intrusive load monitors in 1985 and connect them to electricity meters. They were able to record the current power consumption up to every 5 seconds. Then they did the following steps to identify appliances in a household:

1. Edge Detection:
   Look for sharply rising or steeply falling edges in the stored electricity consumption. These edges indicate that a device may have been switched on or off at that moment.

2. Cluster Analysis:
   The events of steeply rising or steeply falling edges are saved. These events are then visualized in a graph with the following characteristics. Each event is ordered

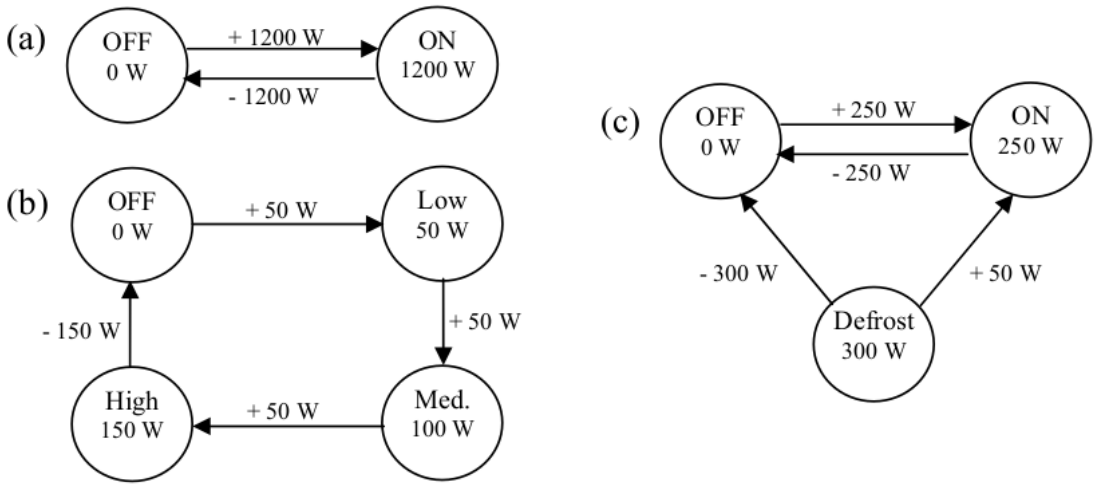

Figure 2.1: An example of a NILM analysis.

according to how much power was consumed or how much power was "released" from the device (e.g. when it was switched off). Essentially, a cluster analysis is then applied to the diagram and each cluster represents a household appliance.

3. Appliance Model Construction
   Since different household appliances have been determined by the clusters, appliance models can now be constructed. In this step, different states in which an appliance can be in, are found based on the different power consumption. An example of how the result of a appliance model looks like can be seen in Figure 2.1.

4. Behavior Analysis:
   Once the majority of the household appliances have been identified, the behaviors of people in the household can be analyzed. In real time, it is possible to track the use of devices, since individual signals can be identified as they occur and do not need to be reconstructed anymore. At this point, several approaches can be taken to provide behavioral analysis. A common approach is to track how long a device has been in use and create statistics on how each device has been used. A daily analysis can be viewed in Figure 2.2.

5. Appliance Saving:
   The last approach is to name the household appliances found(washing machine, etc.) and store them in a database. So that in the case of a further household analysis, it is possible to fall back on appliances that have already been found.

The founder of NILM G. W. Hart himself said in 1989: "Specifically, I recommend that legal restrictions be enacted or clarified so that electric power usage is considered as private as any phone conversation."(Residential Energy Monitoring) Hence, there is a need for a privacy-preserving solution for smart meters. Although the original NILM approach measured power consumption every 5 seconds, there are now methods to

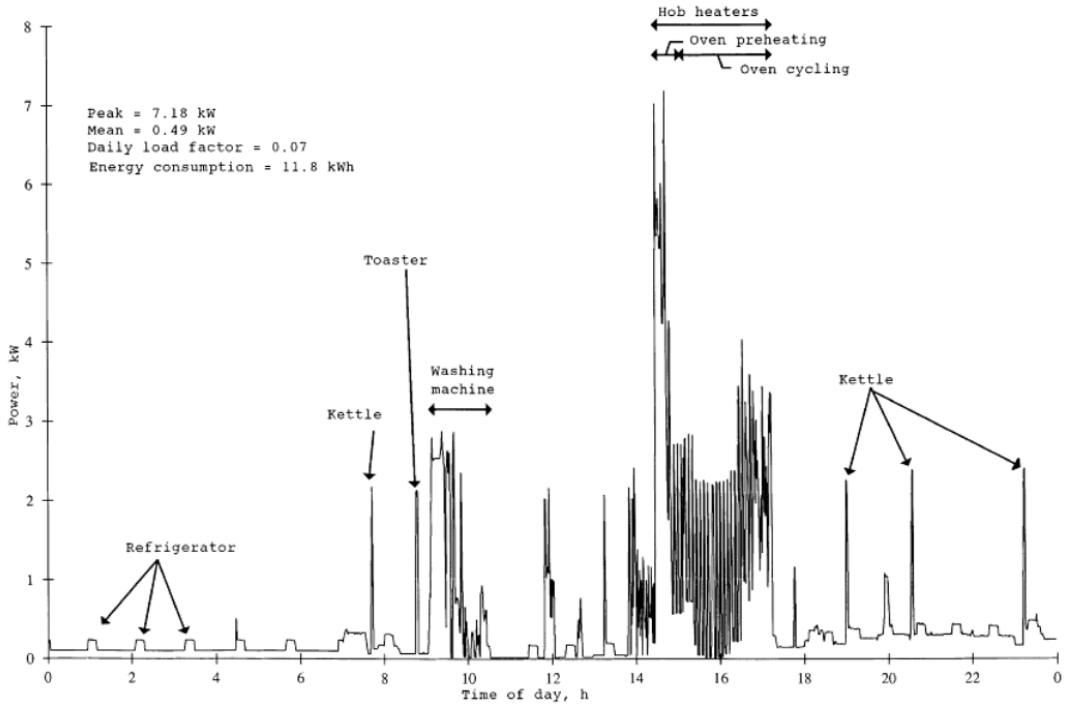

Figure 2.2: An example day of a NILM analysis.

identify household appliances when power consumption is measured every 15 minutes.(A Neuron Nets Based)

2.3.2 Metering for Operations

The paragraph deals with solutions for Metering for Operations, which has been previously discussed in other scientific works. At Metering for Operations, there is currently no established consensus on a solution. Various technical proposals have already been presented in scientific papers, but there is a lack of uniform criteria and often different conditions are set for the power grid. One reason for this could be that smart grids are realized differently in other countries. In the following, the different approaches are divided into categories and presented conceptually.

Anonymization or Pseudonymization Without Aggregation

This approach describes the removal of smart information that allows identification. Identifiable information can also be replaced by pseudonyms. Solutions with trusted third parties are often used in this case. A trusted third party usually acts as an intermediary between the customer and the power grid provider. The trusted third party must be acknowledged by all participants and take a neutral position. In practice, however, this is difficult to achieve because the trusted third party is often hired as a service provider by the electricity supplier and is therefore also paid by the supplier.

In the paper "A privacy-preserving Concept for Smart Grids" by Petrlic[quelle], a trusted third party is used as an intermediary. In the proposal, a smart meter communicates with a trusted third party. Certificates formed with a public key infrastructure can be used to verify and validate information flows from smart meters at the TTP. As soon as the Trusted Third Party has checked the correctness of the smart meter information, it can pseudonomize/anonymize all the necessary information. Only then is the further processed anonymized information forwarded to the electricity provider by the TTP in encrypted form. This means that the electricity provider cannot assign individual electricity consumption to its customers. With this procedure, smart meters can be anonymized. However, if it is possible for an attacker to record the data traffic between the smart meter and the TTP, then the attacker could forward the time stamps and smart meter identification to the electricity provider. Using these two pieces of information, the electricity provider could at least gain some insight, since it would be possible to match when information is sent to the TTP and when it is received by electricity provider.(Privacy-Aware Smart Metering)

Aggregation with Trusted Third Parties

In the attack just described, the electricity provider tries to link two events. One is the arrival of the message at the TTP and the other is the arrival of the message at the provider itself. One way to prevent this attack is aggregation. In this case, the smart meter sends its electricity consumption to the TTP. Certificates are also sent from the smart meter so that the TTP can check the information for correctness and authenticity. Instead of forwarding the information to the electricity provider, the TTP waits until all smart meters have sent their data for which the TTP is responsible. This data is all added up and a message is sent from the TTP to the electricity provider with the total electricity consumption of all smart meters. From the aggregated value, it is not possible to extract an individual smart meter's electricity consumption, which is why the electricity provider cannot filter out information about individual customers.(A Privacy Model for Smart Metering)
Homomorphic encryption approaches also fall into this category. Homomorphic encryption algorithms allow simple operations such as addition and multiplication to be performed on the encrypted messages. In some homomorphic encryption schemes, only addition OR multiplication are supported. These are then called partial homomorphic encryption. There are also bihomorphic encryption approaches. Here not only the operations on the ciphertexts are homomorphic, but also the operations on the keys. This means that if a plaintext a is encrypted with the key x and a plaintext b is encrypted with the key z, that one can decrypt the ciphertexts enc(a+b) with the keys x+z. A bihomomorphic encryption approach with TTP has been proposed by Vetter et al.[quelle] In this case, the TTP acts as the key authority. This means that it creates all cryptographic keys and forwards them to the smart meter, which is then used for further communication with a central store. The smart meter encrypts its data and sends it to the central storage. The central storage also stores the incoming data in encrypted form, so that no unencrypted data can be found on the storage. In addition, the central

storage has no access to the keys and thus has no way to decrypt the information or access meaningful data. Therefore, the central repository has to be trusted only in terms of functionality. If an electricity provider wants to know the electricity consumption of its customers, it makes a request to the central repository, which sends the aggregated encrypted data to the electricity provider. In order for the electricity provider to decrypt the data, the key authority has to release the correct keys. It is impossible for the electricity provider to query the value of just one smart meter. This is because the key authority can only issue keys that can decrypt aggregated totals. It is guaranteed by the homomorphic encryption method which is used. The advantage of using this approach is that the different functionalities, namely storage of data and key acquisition for confidentiality and authenticity is realised from different participants.(Privacy-Aware Smart Metering)

Aggregation Without a Trusted Third Party

The solution proposed in this thesis is also one of the methods that aggregate without a trusted third party. The advantage of this approach is that no one has to trust a trusted third party. In general, one has to ask the questions who aggregates the data and who generates/uses the keys. In addition, a common problem to consider is how the procedure deals with a few participants/customers.
In the solution of Mármol et al. again a bihomomorphic encryption method is proposed. The approach of Mármol has already been discussed and implemented in a master thesis at this chair.[quelle biselli] As a reminder, bihomorphic encryption algorithms can perform simple operations such as addition on both the ciphertext and the keys. This property is exploited in the presented method of Mármol. Since it aggregates the keys and not the power consumptions as before. Furthermore, it does not matter which bihomomorphic encryption method is used, as long as all smart meters agree on one method. A key is generated from every smart meter in the power grid. Afterwards, the key is used to encrypt the power consumption. The key is then used to encrypt the electricity consumption and the encrypted data is sent to the network operator. The transmission channel to the network operator is chosen in such a way that the identity of the smart meter remains secret. This prevents the smart meter from exposing itself during communication with the operator. Groups are formed among smart meters and a smater meter aggregator is selected in each group. The aggregator is selected randomly and all smart meters send their keys to this aggregator. Subsequently, the keys are summed up at the aggregator and sent to the network operator. The network operator receives a single key and with this key it can only decrypt the messages from one smart meter group. additionally, the operator has to add up all the messages and only then it will be possible to decrypt the messages. There is a possibility that aggregator cooperates with the network operator. The aggregator would then be able to send individual keys from smart meters to the operator. While the operator would not be able to match the key to any message, by brute force it could decrypt all messages with that key and see which decrypted message has meaningful content. To prevent this attack, an additional measure is taken. All smart meters in a group organize themselves topologically in a ring structure. In this ring structure, all smart meters cooperate with each other

and change their keys every round in such a way that the individual key of a smart meter changes, but not the summed key of all smart meters. Even if the aggregator forwards the keys to the network operator, they would no longer be valid in the next round.(nochmal nachlesen, warum nicht eine individuelle Nachricht entschlüsselt werden kann) A disadvantage of this procedure is that if a smart meter leaves the group, then a new aggregated key must be formed.(Privacy-enhanced architecture for smart metering)

Battery Solutions

write state

3 Design

. . . design . . .

write design

4 Implementation

. . . implementation . . .

write implementation

5 Evaluation

. . . evaluation . . .

write evaluation

6 Future Work

. . . future work . . .

write future work

7 Conclusion And Outlook

. . . conclusion . . .

write conclusion