Master's Thesis

Privacy-preserving Smart Metering Using DC-Nets

Gregor Garten

February 11, 2022

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

1. Reviewer: Dr. Stefan Köpsell
2. Reviewer: Dr. Elke Franz
Supervisor: 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 Background

This section introduces an overview of concepts for the basic understanding of this work. Therefore, the key components of the smart grid are explained, what structural changes and what challenges will occur in the smart grid that need to be solved. Because this thesis requires a basic understanding of the German smart grid, the stakeholders and their interests in the smart grid are explained. In addition, the technical guideline from the BSI is introduced because it defines a first security-relevant standard that is required for all Smart Meters in the German smart grid. Moreover, this chapter discusses the current state of research and what solutions are discussed in the scientific community.

1.1 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.Due to the increased integration of renewable energies, the distribution from the traditional few electricity producers (e.g. nuclear power plants, coal-fired power plants), which were responsible for a large part of the electricity generation, is changing to many smaller producers (e.g. wind turbines). But, renewable power generation is often dependent on external environmental factors. In order for the electricity grid to be stable despite fluctuations in power generation, smart meters have been introduced to increase the overall grid quality through regular communication of status information and power consumption. Smart Meters enable 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 will be discussed in more detail in the next paragraph.(Quelle:Smart Grid Communications)(Privacy Survey2013)

Smart Meter

Smart meters are the key component in a smart grid. A smart meter is an electricity meter which has an interface to the Internet. The additional functions that a smart meter offers to a regular electricity meter allow a two-way communication between

the control center and the smart meter. The interconnection of electricity meters and control center via the Internet is also called Advanced Metering Infrastructure (AMI). The resulting communication between both components 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 for a grid operator 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. Beforehand, power flows could only be measured up to substations. Moreover, the advanced functions 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. Additionally, in combination with the consumption of all users and the current electricity supply, real-time pricing becomes possible. Not only the customer can be offered a better electricity contract, the smart meters no longer have to be read out at home by a technician from the electricity provider. As a result billing becomes 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)

1.2 Smart Meter Privacy

The main advantage of the smart grid is the advanced communication between the consumers smart meter and the energy suppliers. The 15-minute messages from the electricity meter provide the electricity supplier with a regular update on the status of the electricity grid and there is no longer any need to rely on forecasting models based on data from the past. However, sending user information in such a short period of time 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 has 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. The two problems are referred to as Metering for Billing and Metering for Operations. At first it is described how simple behavioral analyses are generated by electricity consumption. Subsequently, solutions to Metering for Billing and Metering for Operations will be presented, that have been discussed in the scientific community so far.(Privacy-Aware Smart Metering)

1.2.1 Non-intrusive load monitoring

Interpreting power consumption with the intent of identifying devices at 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 connected them to electricity meters. They were able to record the current power consumption up to every 5 seconds. They developed a 5 step procedure to detect household appliances. In the following the 5 steps of the NILM procedure are explained:

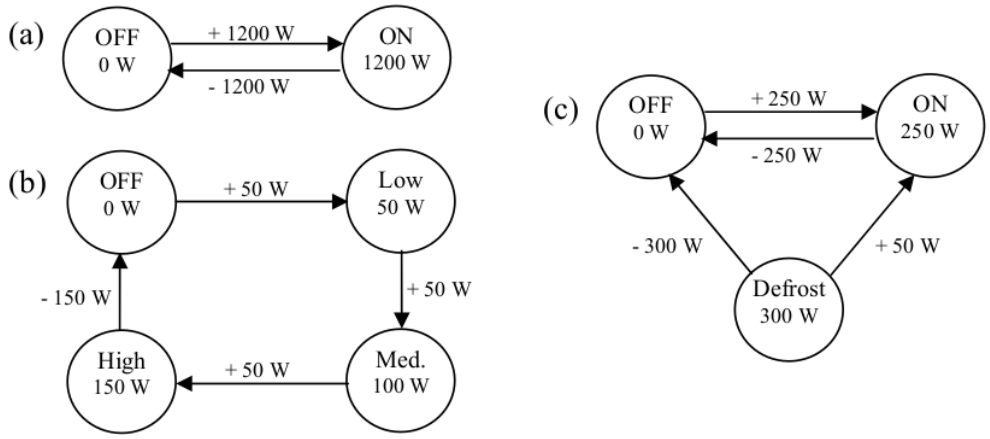

Figure 1.1: Sample Appliances after performing step 3. (a) represents a toaster that has 2 states. (b) is a lamp that has 3 different brightness levels. (c) shows a refrigerator with defrost mode.

1. Edge Detection:
   First, the intercepted electricity consumption is stored. Afterwards, a search in the stored data for strongly rising or strongly falling edges is performed. These edges indicate that a device may have been switched on or off at one specific moment.

2. Cluster Analysis:
   The stored events of steeply rising or steeply falling edges are visualized in a graph with the following characteristics. Each event is ordered according to how much power was consumed or how much power was "released" from the device (e.g. when it was switched off). This causes similar events to be recognizable as clusters in the diagram. Essentially, a cluster analysis is then applied to the diagram and each found 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 1.1.

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 1.2.

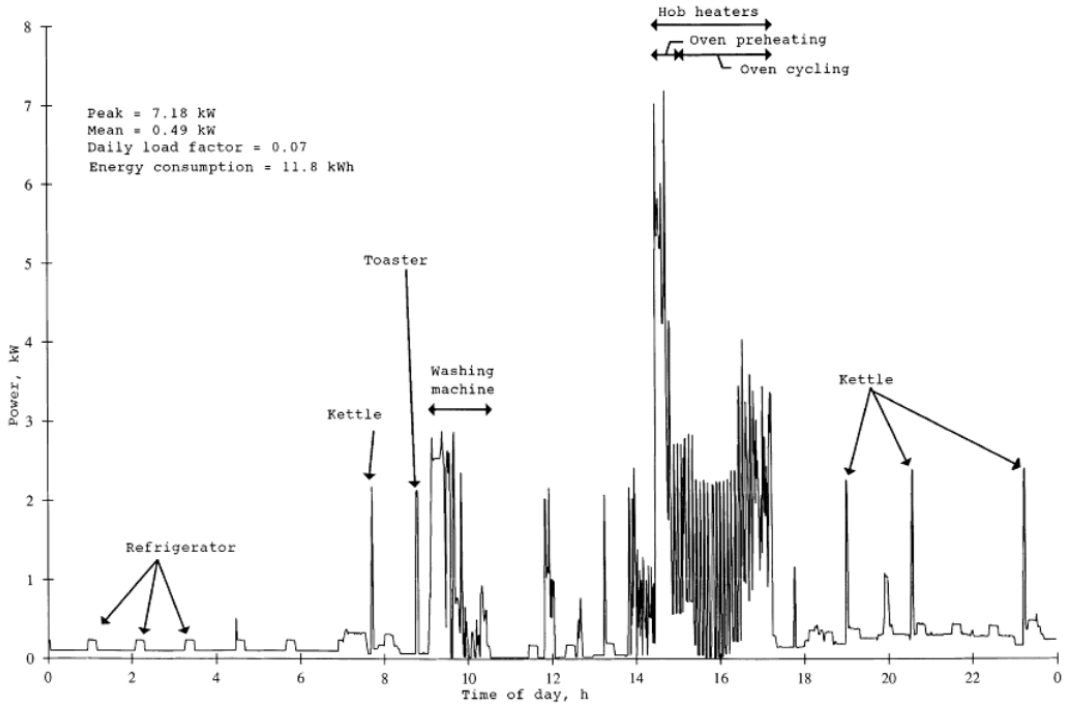

Figure 1.2: The electricity consumption of a household with drawn household appliances detected by NILM.

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) Through Nilm, simple observations can be made without analyzing the household behavior for a longer time. For example, it can be noticed when no one is at home because no lamps are on. It can also be quickly assumed that the house inhabitants are on vacation, if the power consumption is lower than usual over days. For burglars, this information would be particularly useful, as they would have no problem knowing when is a suitable time to break in.

High Resolution Analysis

Since then, research in the field of intrusive monitoring has continued. It was investigated both how much information can be extracted from the household through electricity consumption when electricity consumption was measured particularly frequently. Furthermore, it was investigated whether assumptions can be made about the behavior in the household even at low resolution. For example, in the paper(Multimedia

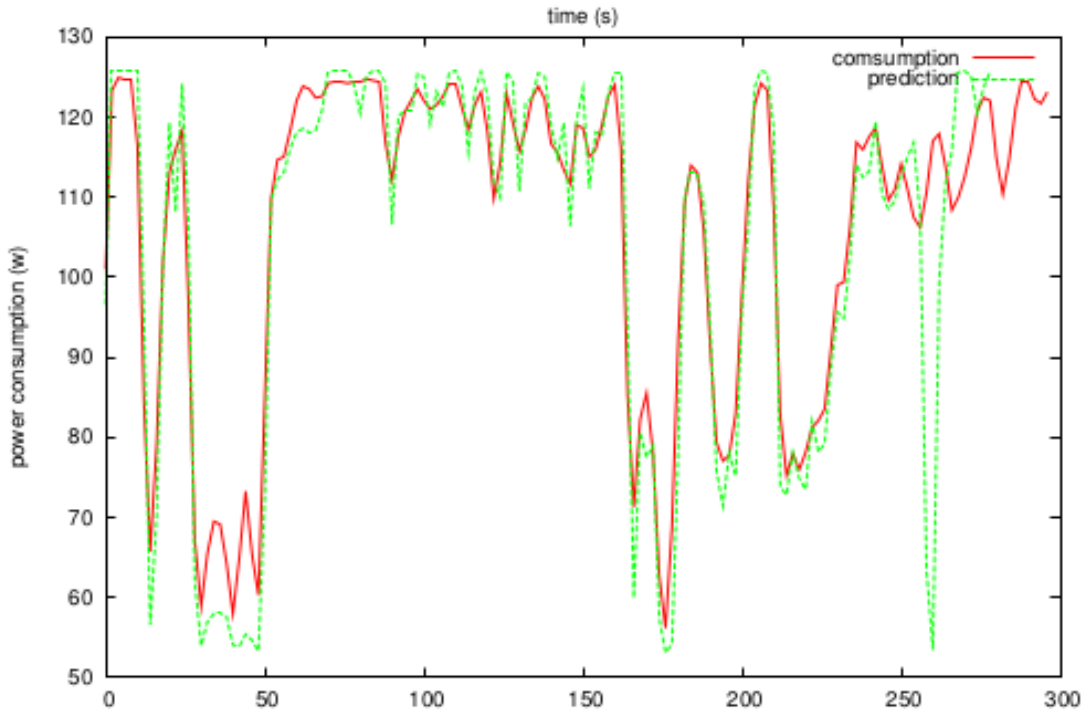

Figure 1.3: The power consumption of a TV in green vs. the estimated power consumption of the TV using the prediction function in red.

Content), the movie being watched could be determined by the power consumption of an LCD television. TV power consumption is strongly influenced by blacklighting activities and each movie has a unique brightness signature. This unique signature was exploited to make a statement about the film being viewed.

In the paper, the power consumption of the TV was measured every 2 seconds and is stored. After 5 minutes analysis of the consumption, the content of the program could be determined with high probability. For this purpose, a Power Consumption Prediction Function was trained to estimate the power consumption of the TV based on the brightness of movie sequences. The input of the prediction function is 5 minute sequences of a movie and the output is the possible power consumption of the TV. In order to recognize a movie, the possible power consumption of the TV by the prediction function is stored over the 5 minute movie sequences. If the same 5 minute sequences are running on a TV, the power consumption can be compared with the prediction of the function by a correlation coefficient. For multiple matches with a correlation coefficient higher than 0.85, an additional optimization algorithm is applied to estimate the movie. Later, the paper also showed that the power consumption could be used to identify which TV channel was being watched. In the figure 1.3 the result of the estimation of the prediction function is shown in green and in red the actual power consumption of a LCD TV for the same movie sequence can be seen.

Low Resolution Analysis

Another approach is to work backwards from large data sets to obtain detailed information from aggregated electricity consumption. The NILM procedure attempted to have household appliances detected from individual households and then behavioral analyses could be generated from the detected household appliances. A common approach with low-resolution electricity data is to identify the numerous factors that influence total electricity consumption and to filter them out.(großes Paper) But with low resolution methods, a variety of approaches are being pursued. For example in (A Neuron Nets Based) an artificial neural network was trained to identify household appliances from electricity consumption. The power consumption was measured only every 15 minutes. But this is the same time interval that the SMGW use as well. With the low resolution, only the household appliances that have a high overall impact on power consumption, such as refrigerators, were considered. A total of 10 different household appliances were attempted to be correctly identified from the electricity consumption. With the final trained ANN, an accuracy of 90
In another work(Energy Disaggregation), the power consumption of appliances was measured only every hour. The experiment tried to disaggregate a aggregated power consumption with Discriminative Sparse Coding. The experiment was conducted as follows. First, the disaggregation algorithm was trained with electricity consumption of houses from a large data set. Then, the trained algorithm was applied to the aggregated electricity consumption of 2 houses. The algorithm was expected to determine up to 52 individual household appliances from the electricity consumption. The results in the paper showed that the disaggregation algorithm with Discriminative Sparse Coding was up to 55.05 percent correct in its decisions.[1]

1.3 Related Work

After NILM was discovered, the scientific community started to look for possible solutions to technically prevent the analysis of electricity consumption. In this chapter, the different approaches in Metering for Operations and Metering for Billing are presented. Although in this thesis only a solution of Metering for Operations is presented, for completeness the solutions for Metering for Billing are introduced as well.

1.3.1 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

[1] Considering the fact that the time interval is so small and 52 different household appliances were considered, the accuracy of 50 percent is extraordinarily good. If the algorithm would only guess, the accuracy would be at 1.9 percent.

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 towards the electricity supplier. 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 procedure, a smart meter communicates with a trusted third party. Certificates formed with a public key infrastructure are 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 additionally 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 en-

cryption 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 is supported. These algorithms 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 meters, which are used for further communication with a central storage. The smart meter encrypts its data and sends it to the central storage. The central storage also saves 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.

mathe

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. Moreover, 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 the approach by Vetter et al. is that the different functionalities, namely storage of data and key acquisition for confidentiality and authenticity are realized 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 the keys. In addition, a common problem to consider is how the procedure deals with a few participants.
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 generated key is used to encrypt the electricity consumption and the encrypted result 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 unknown. This

prevents the smart meter from exposing itself during communication with the operator. Groups are formed among smart meters and a smart 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. A disadvantage of this procedure is that if a smart meter leaves the group, then a new aggregated key must be formed and the operations are quite computationally expensive(Privacy-enhanced architecture for smart metering)

Battery Solutions

The battery approach describes a household with a connected battery that is charged, e.g. by grid purchase or by photovoltaic panels. The goal of the approach is that the battery feeds energy into the household in such a way that the grid operator can no longer detect private information based on the electricity consumption.

The figure 1.4 shows the electricity consumption of a private household with a connected battery that is charged via solar panels. 3 lines can be seen. The red line shows the electricity consumption of the household. The green line shows when the battery is discharged (when the battery is feeding power to the household). The blue line is the power consumption that the grid operator can see. In the figure you can see that when the battery brings electricity to the household, then grid operator sees that a household does not consume electricity. In other cases, the grid operator sees that electricity is being consumed, but it is much less than the house actually consumes because the battery offsets some of the electricity consumption. In other words, if a household is connected to a battery, the grid operator cannot make correct statements about the behavior of the people in the household.

An algorithm for batteries was proposed in(Protecting consumer privacy from electric load monitoring). This method uses an algorithm that can control the battery to produce a constant characteristic curve in consumption. The algorithm targets a static and fixed current consumption. The target consumption is calculated differently by the algorithm depending on the house consumption and battery capacity. If the power consumption is below the consumption set by the algorithm, then the battery is charged with the difference from the target consumption. If the power consumption is above the target consumption set by the algorithm, the battery is discharged with the difference from the

Figure 1.4: The power consumption of a household during the day (red) with battery (green) and the power consumption that the power provider can access (blue).

target consumption. If the consumption is significantly higher, so that the battery can no longer absorb the additional consumption, then it is switched to recovery mode. In recovery mode, the target consumption is temporarily increased, so that the battery can charge on the side, even though the house is currently consuming a lot of power. If the recovery mode can be switched off, then a new target consumption is calculated based on the new data. It is important to remember that this method does not anonymize power consumption, so it is even more important to measure how much information can still be extracted from power consumption. There are the following metrics to calculate how much privacy is gained by the algorithm.

1. Relative Entropy:
   Relative entropy[2] is used to compare two sources of information. In this case it would be the power consumption with the algorithm and the power consumption without the algorithm. These two loads form a stochastic process and can then be analyzed with the calculated relative entropy. (Affordable privacy for home smart meters)

2. Cluster Classification:
   The cluster classification has already been explained for the NILM method and

[2] Relative entropy is often referred in literature as Information Gain or Kullback-Leibler divergence

described in this paper at [ref]. Cluster Classification is well known as a machine learning approach, but it can also be used as a metric to evaluate privacy. Here one would perform a cluster analysis with the battery method and once without. Then one looks at the number of clusters in both measurements and if fewer clusters are found with the battery method, then this is considered a privacy gain.

3. Regression Analysis:
   In the regression analysis, first a cross-correlation and afterwards a simple linear regression is performed. More precisely, both power consumptions are "superimposed" at the point of their maximum cross-correlation. Subsequently, a linear regression is performed and the privacy is evaluated on the basis of the quality of the predictor.

Drawbacks

Although various approaches to solving Metering for Operations are discussed, the following drawbacks must also be considered.

1. Pseudonymization:
   Pseudonymization does not provide protection against the attacks described in Ref[Nilm]. The only thing pseudonyms protect is the identification of the SMGW. Once it is possible to assign the pseudonym to a customer, the pseudonym becomes invalid and the electricity consumption can be uniquely assigned to a customer.

2. Aggregation with Trusted Third Parties
   The approach of trusted third parties is difficult to realize in the smart grid scenario. This is because the question of the neutrality of the TTP remains open. The service of the TTP is not free and it remains unclear which entity in the system will pay for the TTP. If the customer were to bear the costs, then the electricity provider could question the neutrality of the TTP. However, it is much more likely that the electricity provider will pay for the TTP's service. In this case, the neutrality of the TTP would be open to doubt by the customer, since the TTP could be dependent on payments from the electricity provider.

3. Battery Approaches:
   Battery methods are a good way to mask actual electricity consumption. However, it is also a physical device that needs to be installed in the home and is costly at the same time. Widespread installation of batteries on a large scale is therefore unlikely in the next few years, as not every household has the funds for this investment.

4. Aggregation without Trusted Third Parties:
   A disadvantage of Aggregation without Trusted Third Parties procedures is that they are more complex at the conceptual level than the proposals from the other categories. In addition, many Aggregation without Trusted Third Parties approaches involve homomorphic encryption schemes that are very computationally intensive. Nevertheless, the author believes that this category is the most appropriate for protecting client anonymity, because there is no need to rely on TTP or invest a lot of money as in the battery approaches.

1.3.2 Metering for Billing

In order to fully protect the privacy of a household, metering for billing procedures must also be applied. Otherwise, conclusions about electricity consumption may be drawn from the billing. A simple solution would be to increase the frequency of the billing period. But at the same time it is also in the interest of the customer to buy electricity as cheaply as possible and the customer can be offered better electricity contracts if the billing period is shorter. In addition, it cannot be guaranteed that the customer's privacy is not violated in more complex electricity contracts by other features, even if a higher billing period is used. This master thesis focuses mainly on the metering for operations problem. By implementing Trusted Platform Modules (TPM) in German smart meters, the problem is considered to be solved. But for completeness, frequently proposed solutions in the scientific community are presented.

Billing with a Trusted Third Party

The advantages and disadvantages of a TTP have already been explained in the upper section[ref]. The principle is similar to metering for operations. The smart meter sends its measurements to the TTP and the TTP calculates the bill over the time period specified in the electricity contract. The billing is then sent to the electricity provider. On paper, this approach is simple, but important practical questions often remain unanswered. For example, who is paying the trusted third party? In this case, the trusted third party provides a service to the electricity provider. However, if the electricity provider pays for the service, then the trusted third party is no longer independent[quelle].

Billing with a Trusted Platform Module

Billing can also be implemented on the smart meter with a Trusted Platform Module. A TPM is a chip that is installed within the smart meter and thus additional security features can be used on the smart meter. The TPM contains a cryptographic processor that can generate random numbers, generate RSA keys, generate SHA-1 hashes and it has an encryption-decryption-signature engine. In addition, the TPM can be used to prove that nothing has been tampered with the smart meter after in got deployed. A secured smart meter can therefore perform correct billings at the customers side and the electricity provider can trust the smart meter, although it is located at the customer's home. However, the TPM is installed by the electricity provider and it only guarantees the validity of the billing. If the electricity provider decides to send additional sensitive information within the calculations in the TPM, the TPM has no advantage for the end user.(Privacy-Aware Smart Metering)

Billing Secured via Advanced Cryptography

Lastly, there is the cryptographic commitment method. With this approach, no other participant needs to be trusted. A smart meter can use a cryptographic commitment to prove that each bill was calculated correctly. So with cryptographic commitments,

billing can be done on the customer side. A commitment is a cryptographic application and works as follows. Both sides agree on the same commitment procedure. Then it is possible that one side can generate a c=(x,r) as an obligation. Here x would be the calculation and r would be a random number. If one wants to check the commitment for correctness, then there is an Open(c,x,r) function that returns True (if correct) or False (if incorrect). Cryptographic commitments are mathematically constructed so that it is easy to compute a c=(x,r), but hard to find an x /= x' with an r' such that open(c,x',r') returns True. In this use case, the following procedure is often used. [pedersen]
Commit(x, r) · Commit(y, s) = Commit(x+y, r+s)
$Commit(x,r)k$ = Commit(x · k, r · k) mathe
The special feature of the method of [pedersen] is that at the same time non-homomorphic properties are satisfied. Without going into exact technical details, cryptographic commitments work as follows in a smart grid.
The smart meter generates a cryptographic commitment for each measurement. Via a public key infrastructure, the smart meter and the electricity provider receive cryptographic keys. With these keys, the smart meter can sign its commitments and then send them to the electricity provider. The electricity provider checks the commitments for correctness and if all data is correct, the electricity provider sends back a list with electricity prices and the corresponding time stamps. The meter now knows at each point in time how much electricity was consumed and what the price was. By exploiting the homomorphic properties of the procedure, the smart meter can now calculate the electricity prices. The electricity price in this case would be the variable k. So the smart meter creates new cryptographic obligations with the electricity price calculated on the consumption and sends these new obligations to the electricity provider. The electricity provider can verify the correctness by performing the same calculations as the smart meter. If the results with the Open(c,x,r) method return true, then the calculations were performed correctly by the smart meter. This method is suitable for simple electricity tariffs when only a factor on the electricity consumption needs to be calculated. If an electricity contract is more complex with different conditions such as a higher electricity price if a certain electricity consumption is exceeded, then this approach can no longer be implemented.

1.4 Technical guideline TR-03109

This paragraph will discuss the technical guideline published by the BSI[3]. The BSI is the entity of the German federal government that deals with digital security issues and releases recommendations as well as mandatory security guidelines for critical infrastructures. Among other things, technical guidelines are published in which security standards are defined for different IT systems like Smart Meters. The technical guideline BSI-TR-03109 defines minimum requirements for functionality, security and interoperability that individual components of smart meters in Germany must fulfill. The guideline as a whole consists of 6 different documents, which are shown in Figure 1.5. Based on the guidelines, it is possible to have Smart Meter devices certified by test

[3] BSI - Bundesamt für Sicherheit in der Informationstechnik(eng. Federal Office for Information Security)

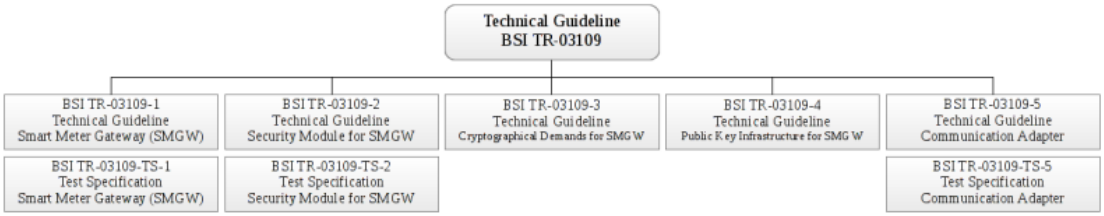

Figure 1.5: All documents from BSI that are subdivided under the Technical Guideline 03109.

centers. Unless otherwise described, all information are derived from the most recent technical guideline[quelle].

Stakeholder in the Smart Grid The technical guideline describes all stakeholders that participate in a power system. The most important stakeholders for this work are described.

Consumer:
The consumer is the person who uses electrical energy, gas, water or heat. In addition, the consumer is the owner of the measurements processed and stored in the SMGW. In order to interact with the SMGW, the consumer uses a communication device. All necessary data can be retrieved and displayed through it.

SMGW administrator:
A Smart Meter Gateway Administrator (GWA) a trusted entity and each SMGW is assigned a GWA. The GWA handles the configuration, monitoring and control of SMGWs and it is even possible to perform updates of SMGWs via the GWA.

Authorized external entities:
External market participants (EMT) are all other authorized participants in the energy network that can establish a communication connection with the SMGW. These include power grid providers and electricity suppliers. The SMGW ignores all other communication requests that do not come from the GWA or EMTs in order to prevent attacks.

There are several other actors such as Controllable Local Systems, service technicians and meters. However, these actors do not play a major role in the protocol that is proposed here. In Figure 1.6 is a exemplary power grid shown with the Stakeholder in the Smart Grid. Every SMGW is connected to one administrator(GWA), which configurates the communication profile of the SMGW. When pseudonymization is activated, the information is not sent directly to the electricity provider, but first to the GWA. Afterwards, the GWA forwards the data to its electricity provider.

grafik nochmal überarbeiten

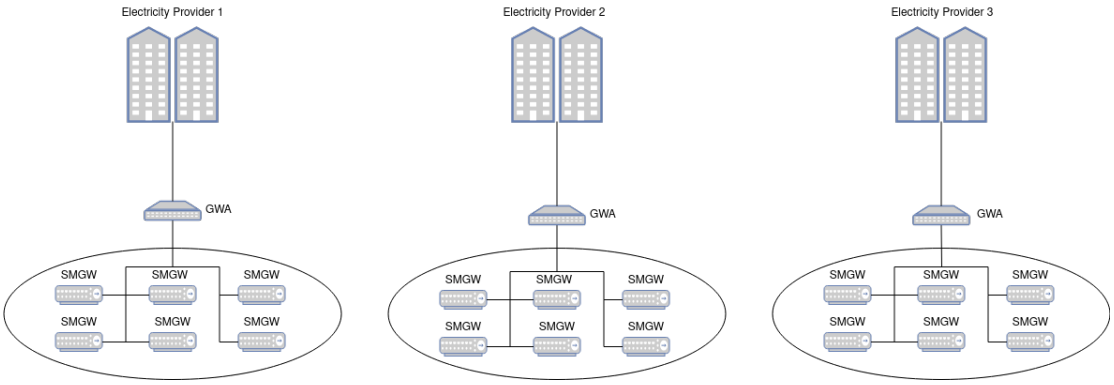

Figure 1.6: An exemplary electricity grid in the TG-03109

1.4.1 Interfaces and functions of the Smart Meter Gateway

A smart meter or as described in the technical guideline a smart meter gateway(SMGW) must provide 3 different physical interfaces as shown in 1.7.

1. Local Metrological Network (LMN):
   The LMN is the communication interface in which communication takes place with the connected meters for energy and material quantities (electricity, gas). An SMGW can communicate with one meter from one end user or with several meters from different end users. In practice, however, one SMGW is often responsible for one meter. The measured values are sent from the meters via the LMN to the SMGW and stored there.

2. Wide Area Network (WAN):
   The WAN is the only communication interface with which the SMGW can communicate with EMTs or GWAs over the Internet. If a request is made to the SMGW that was not sent by these authorized participants, then the request is discarded and ignored.

3. Home Area Network (HAN):
   In HAN, an SMGW interacts with Controllable Local Systems (e.g., photovoltaic systems). In addition, users and service technicians can use the HAN interface to display information about power consumption through functions offered by the SMGW.

Functionality of the smart meter gateway

First, the task of SMGW is to store the measurements sent by meters from the LMN. Then, the readings are processed in the SMGW and sent to the authorized EMTs in the WAN after processing. An SMGW must also perform the tasks of a firewall and separate the 3 interfaces. It is therefore impossible for an EMT or GWA to make requests to devices located in the HAN or LMN, even if it is allowed to interact with the SMGW over the WAN. The processing of data from the SMGW is shown in Fig

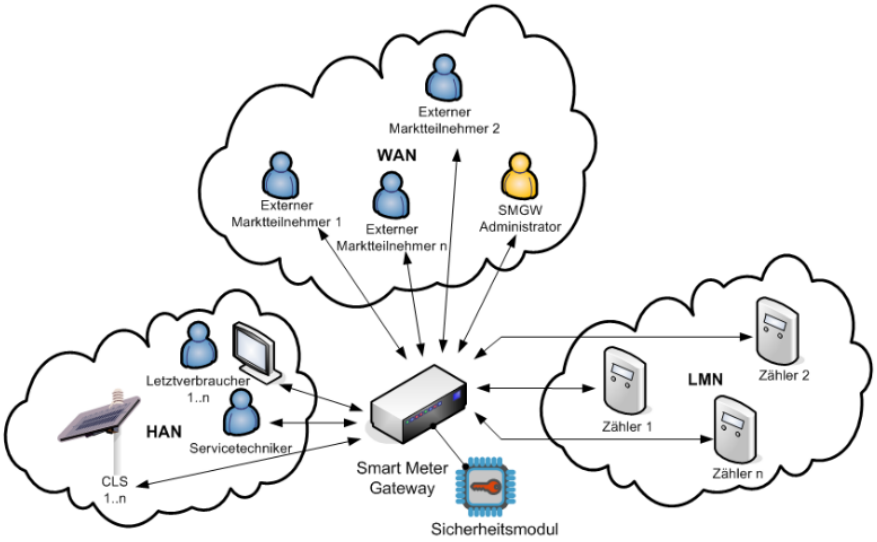

Figure 1.7: An overview of all interfaces and possible stakeholders that can communicate with SMGW.

1.8. Since the WAN interface is the most important interface for this work, it will be discussed in more detail.

Functions of the SMGW in the WAN

The tasks performed by the WAN have already been explained in the paragraph above. Now the functions and security mechanisms offered by the SMGW to guarantee secure interaction on the WAN will be described.

1. Transmission of measured values based on evaluation and WAN communication profiles:
   Communication profiles of GWAs are stored in SMGW. The communication profiles determine how the data is processed in the SMGW and forwarded to EMTs.

2. Pseudonymization:
   Data that is not relevant for billing must be pseudonomized for data protection reasons. For this purpose, the unique identification number that each SMGW has is replaced by a pseudonym. Subsequently, the information is not sent directly to an EMT, but is forwarded to the EMT via the GWA. This additionally protects the identity of the sending SMGW.Even if peusodonymization does not allow an SMGW to be directly assigned, the described attack in [ref] and the resulting behavioral analysis is still possible. Since no other security mechanisms are available from the SMGW, the question must be asked whether pseudonymization as proposed in the technical guideline is sufficient.

3. Time synchronization:
   In order for the cost electricity consumption to be calculated correctly, it is essential

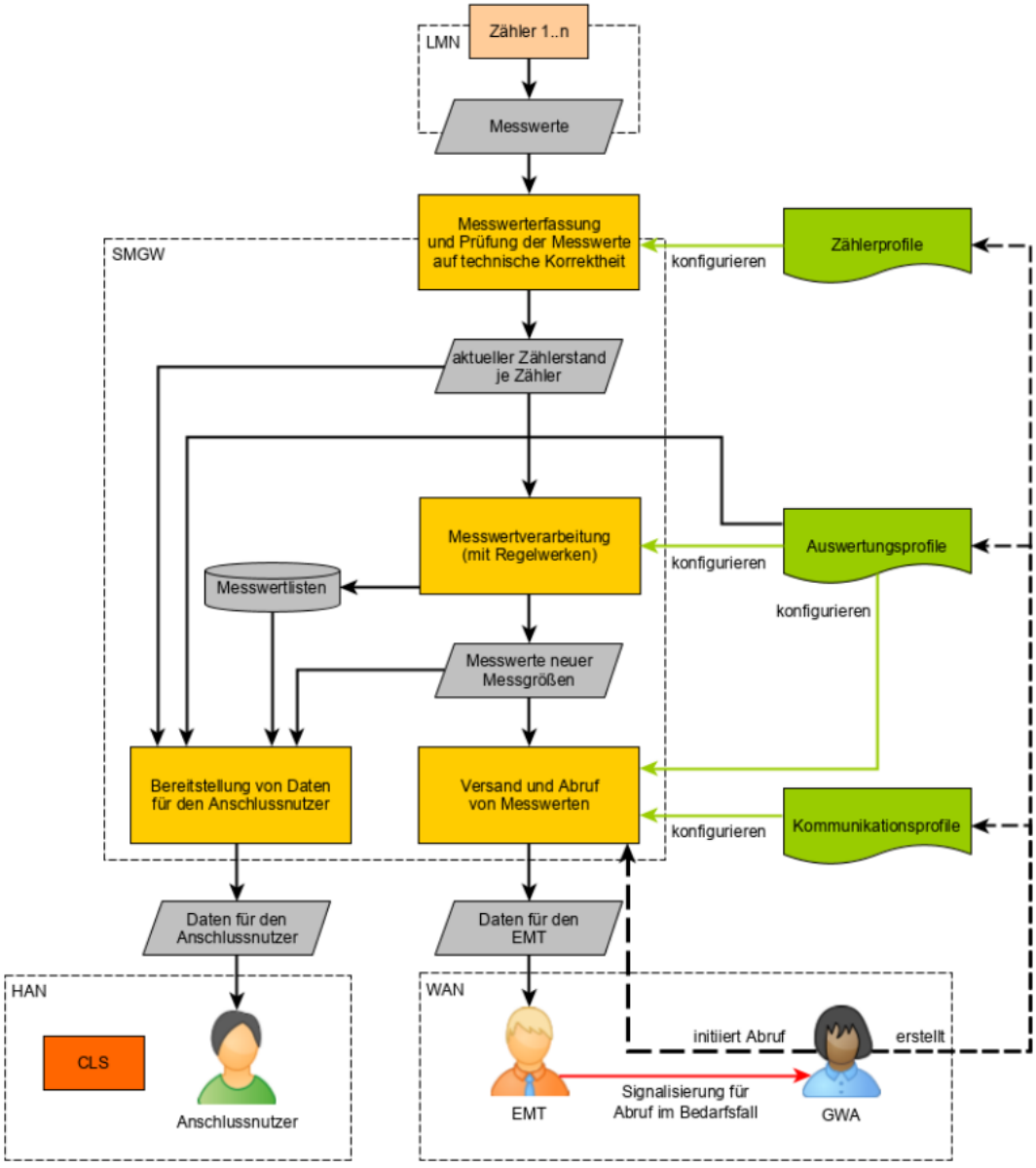

Figure 1.8: An overview of the measured value processing within the SMGW with configuration profiles from the GWA.

that the SMGW have an accurate time. For this purpose, the system time of the SMGW is synchronized with the time server of the GWA at regular intervals.

4. Wake-Up Service:
   A GWA is able to force a communication link with the SMGW. This is done via a data packet signed by the GWA. The SMGW then establishes a fixed preconfigured communication connection to the GWA. This enables the GWA to execute administration commands on the SGMW.

Stakeholder Motives

It has already been explained in this chapter which participants in the power grid interact with each other. Now in particular it will be discussed which motives the different participants have and which malicious motives can be pursued by the participants or by attackers.

Customer's Motives

For the costumer, all the security goals defined above are important. But by far the most important is the security goal of anonymity through the smart meter. Possible attacks on the electricity consumption penetrate deeply into the private sphere of each customer. Therefore, no conclusions may be drawn from the electricity consumption of a customer.
On the other hand, unethical customers may try to steal electricity to save energy costs. The smart meter is located in or on the customer's house. An unethical customer could attempt to tamper directly with the smart meter's hardware or software. The attempts could look like this, a Costumer could try to reduce the recorded electricity consumption at the Smart meter or the Smart meter could be manipulated to measure less electricity when electricity prices are high and more electricity when electricity prices are low.

Electricity Provider's Motives

For the electricity provider, the authenticity of the billing is the most important security objective because From the electricity provider's point of view, the customer is not trustworthy in the calculation of the bill. In addition, the customer has access to the smart meter at almost any time in an environment trusted by the customer. Unlike analog meters, smart meters cannot be mechanically attacked. But if a customer manages to change the software of the smart meter, the billing can be manipulated at the same time. On the other hand, the electricity provider can also be an overly intrusive electricity provider. In the paragraph [Ref NILM] it was explained how a behavioral analysis can be created from the electricity consumption. This sensitive information could be used to gain an additional source of income. In [SSRN] it was listed which questions could be answered by a Nilm analysis. Quote: "On what days and during what times do you watch TV? How much home time do you spend in front of your computer?" or "Are any of the appliances in your household failing or operating below optimal efficiency? Do you own (and so presumably like) lots of gadgets?". Advertising

companies would certainly pay money for this kind of information in order to be able to advertise more accurately. For this reason, it is presumed that the electricity provider is considered an honest-but-curious adversary.

1.4.2 Security Objectives

The smart meter attempts to achieve the 3 security objectives of confidentiality, integrity and availability. The 3 security goals are often summarized as CIA. Another important security goal for this work is anonymity. The 4 definitions are essential for the understanding of this work. Therefore, the terms are explained below.

1. Confidentiality:
   It is not possible for an unauthorized party to gain information about the content of the data sent.

2. Integrity:
   It is not possible for an unauthorized party to modify the content of data without data without this being noticed.

3. Availability:
   It is not possible for an unauthorized party to interfere with the functionality of a service.

4. Anonymity:
   Verbergen der Identität vor dem Kommunikationspartner??? Vllt wer hat die Daten gesendet, wer hat den Stromverbrauch gesendet?

In the ref[3] chapter, the design of the network protocol is presented, which fulfills the mentioned security objectives and thus protects the privacy of the customer from the electricity provider or an attacker. For an attacker his main goal is to try to bypass the security objectives to obtain additional information about the customer.

1.4.3 Attacks on the Smart Grid

In Germany, the smart grid is one of the critical infrastructures. This means that the failure of the smart grid could lead to a significant compromise of public safety or other serious consequences. Such systems are threatened by all sorts of attackers.

Eavesdropping

Eavesdropping may be the weakest type of attack and it is often used by a passive attacker or by an active attacker as a preparation for a larger attack. Successful eavesdropping on the communications of the smart meter could be useful to e.g. intruders. However, curious neighbors might also have an interest in the behavior inside the house. Turning on/off lights implies that someone is at home or leaving the house. Therefore, eavesdropping on electricity consumption could provide information about when is a suitable time to break in. To prevent eavesdropping, smart meter communication

is encrypted to maintain confidentiality. Cryptographic algorithms such as AES are widely used today and have been analyzed for weaknesses over the years by a number of researchers. Hence, a successful attack on encrypted data to extract information is extremely unlikely.

Active Attackers

The objective of active attackers may not necessarily be to analyze a user's electricity consumption. They may want to disable availability through e.g. denial of service attacks. These attacks could leave major damage to the power grid and are definitely a realistic threat[quelle]. But this thesis focuses on smart meters and the anonymization of electricity consumption. That's why it is assumed that the active attacker does not carry out system-wide attacks on the power grid. Rather, it is assumed that the attacker attempts to take control in the proposed DC network. Among other things, it is assumed that the attacker has the theoretical ability to take over one or more SMGW and send messages through the SMGW. In addition, if the attacker has taken over an SMGW, it can perform all operations that are possible through the proposed DC network.
In the next section, the conceptual solution of the DC-Net is proposed and how the DC-Net could be implemented in the technical guideline of the BSI. It also describes which attacks on the DC-Net are possible with the defined attacker model.