A Privacy Model for Smart Metering

Jens-Matthias Bohli[†], Christoph Sorge[‡], and Osman Ugus[†]

[†] NEC Laboratories Europe, Kurfürsten-Anlage 36, 69115 Heidelberg, Germany
E-mail: {bohli,ugus}@nw.neclab.eu
[‡] Universität Paderborn*, Department of Computer Science, Warburger Str. 100, 33098 Paderborn, Germany
E-mail: christoph.sorge@uni-paderborn.de

***Abstract*—Electricity suppliers have started replacing traditional electricity meters with so-called smart meters, which can transmit current power consumption levels to the supplier within short intervals. Though this is advantageous for the electricity suppliers' planning purposes, and also allows the customers a more detailed look at their usage behavior, it means a considerable risk for privacy. The detailed information can be used to judge whether persons are in the household, when they come home, which electric devices they use (e.g. when they watch TV), and so forth. In this work, we introduce the "smart metering privacy model" for measuring the degree of privacy that a smart metering application can provide. Moreover, we present two design solutions both with and without involvement of trusted third parties. We show that the solution with trusted party can provide "perfect privacy" under certain conditions.**

I. Introduction

The adoption of smart electricity meters can contribute to reduced carbon dioxide emissions in two ways. Firstly, they allow showing customers their electricity consumption in an illustrative manner, which can be a motivation for saving energy. Studies suggest an energy saving potential of around 15% [1]. Secondly, smart meters enable dynamic pricing dependent on the current supply situation, making it easier to shift electricity consumptions to times when renewable energy sources (e.g., wind energy) are available. This way, less peak-load electricity generation plants—which tend to be inefficient, and often based on fossil fuels—are required.

The roll-out of smart meters has already begun, and the new technology is rapidly adopted in countries throughout the world. However, this development is not without its problems. If the current electricity consumption is transmitted to the electricity supplier nearly in real time, the supplier can exactly observe the customer's behavior. The electricity consumption profile differs between devices, so given a sufficient resolution on the time axis, the supplier knows when the customer watches TV, when his washing machine runs, etc. It is easy to determine whether or not a customer is at home.

As a result, privacy concerns have been raised in newspaper articles [2], reports by data protection authorities [3], and in the research community [4]. The German electricity supplier Yello Strom received the German "Big Brother Award" in 2008 for its plans to introduce smart meters and to network electrical devices, and the associated lack of transparency concerning the data transmitted [5]. The smart meters offered by this company are now on the market.

We believe the criticism to be justified, but consider the benefits of smart metering to be too significant to refrain from adopting this technology. Therefore, we investigate approaches that keep these benefits, while significantly improving customers' privacy.

Our contribution: In this paper, we identify requirements for the privacy protection of smart metering (section III). As a principle, we want to allow an electricity supplier to receive aggregated information. The company should know the *current* overall consumption of electricity by its customers, or specific groups of customers, as well as the *sum* of a customer's electricity consumption during a billing period (possibly weighted with prices). We introduce a "smart metering privacy model" (section IV) for measuring the degree of privacy that a smart metering application can provide. Moreover, we present and evaluate two solution designs both with and without involvement of trusted third parties (section V). We show that the solution with a trusted party can provide "perfect privacy" in the presented smart metering privacy model, depending on the underlying encryption algorithms.

II. Related Work

While the protection of smart meter readings against third-party eavesdroppers can be achieved with standard cryptographic solutions, the authors are not aware of any previous publications tackling the smart meter privacy problem with respect to the electricity supplier. There is, however, related work in other fields.

In the database world, the concept of k-anonymity [6] can be used when releasing information from a database. The underlying idea is to reveal the information in such a way that for any combination of attributes potentially known from external sources, there are at least $k-1$ other tuples of these attributes containing the same information. The concept of k-anonymity is not suited to the smart metering problem, as there is no central entity releasing the smart meter readings—our idea is rather to avoid the collection of too much personally identifiable information by the electricity supplier.

In the field of telecommunications, the most relevant related work is on anonymization techniques, such as onion routing (which is, for example, implemented in TOR [7]) and Crowds [8]. The latter also defines degrees of anonymity, which can be used to evaluate privacy-enhancing technologies.

The modeling aspects of this paper have been inspired by numerous privacy-related articles using games, a recent example being [9].

*Work done while at NEC Laboratories Europe

978-1-4244-6826-3/10/$26.00 ©2010 IEEE

III. Requirements on Smart Metering

A smart metering application (SMA) consists of an electricity supplier (ES) and a set of smart meters $S = \{\mathsf{sm}_1, \ldots, \mathsf{sm}_n\}$ for some $n > 1$. We denote by $e_{i,j} \in R$ the electricity consumption measured by sm_i in the period j. Here, R denotes a set of all possible energy consumptions that can be measured by a smart meter. We denote by t the number of time periods included in one billing period. Then, the ES must get to know the sums $\sum_{i=1}^{|S|} e_{i,j}$ for all $j \in \{1, \ldots, t\}$ and the sums $\sum_{j=1}^{t} e_{i,j}$ for all $\mathsf{sm}_i \in S$ (but no additional information). The events in a smart metering application can be described by the matrix (e_{ij}).

Informally speaking, the electricity supplier should know

- the sum of the current electricity consumption of all customers (or all customers in a certain pre-defined group),
- the sum of electricity consumption values of an individual customer over a given time period (e.g. one month or one year),
- but not the current electricity consumption of any individual customer.

The problem, however, is not purely a mathematical one. The following properties are also required for an application in the real world:

- The electricity supplier must be able to compute an approximation of the current electricity consumption even if some of the values are missing (e.g., due to loss of connectivity at some of the customers' premises). In other words, the electricity supplier gets to know an approximation of $\sum_{i=1}^{|S|} e_{i,j}$ for a fixed j even if up to r ($r < |S|$) values $e_{i,j}$ are unknown. As an example, if the values $e_{1,j}, \ldots, e_{r,j}$ are unknown, knowing the sum $\sum_{i=r+1}^{|S|} e_{i,j}$ and the number r would allow the supplier to estimate the contribution of the missing customers.
- The electricity supplier must be able to compute the sum of a customer's electricity consumption within the defined time frame t even if some of that customer's values $e_{i,j}$ were originally missing. The customer may, for example, provide this information at a later point in time, once his connectivity has been restored.
- The initial setup complexity per period should be low.

We base our solutions on the assumptions that smart meters are trusted devices, i.e. there is tamper-resistant hardware available to store key material when necessary, and to perform the computations necessary for the presented protocols.

IV. Privacy Model for Smart Metering

In this section, we introduce a "smart metering privacy model" for measuring the degree of privacy that a smart metering application can provide.

Privacy Model for Smart Metering. The privacy of the smart meter application is defined by a cryptographic game. We use a right-or-left type of game to define privacy. In such a game, the adversary A will choose two scenarios that should be indistinguishable for a smart metering application. The challenger will simulate one scenario with the smart meter protocol and give the resulting transcript to the adversary. The adversary A will win the game if he can guess correctly which scenario was simulated. We say that A breaks the privacy of the smart meter application if A wins the game with a significantly higher probability than possible by random guessing.

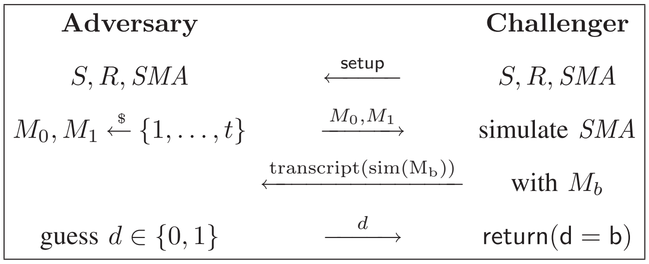

Fig. 1. The experiment SMPB(b) for $b \in \{0,1\}$ to define smart metering privacy.

To prepare the game, a setup process is executed in which S and R are defined and all parameters and keys necessary for the smart meter application protocols SMA are chosen. As before, S denotes a nonempty set of smart meters and R denotes a sample space for all possible energy consumptions. We assume that an abnormal energy consumption during a period could be detected without being considered as a privacy break. Therefore, the sample space represents all energy consumptions $e_{i,j} \in [0, z]$, where z is an expected maximum consumption per period for which privacy should hold. As the ES is potentially interested in breaking the privacy, the adversary obtains all secrets that are held by ES. Still, we do not exclude other attackers (different from the ES).

The adversary then decides for two electricity consumption scenarios denoted by two consumption matrices $M_0 = (e^0_{ij}), M_1 = (e^1_{ij})$.

As learning the sums $\sum_{i=1}^{|S|} e^b_{i,j}$ for all $j \in \{1, \ldots, t\}$ and the sums $\sum_{j=1}^{t} e^b_{i,j}$ for all $\mathsf{sm}_i \in S$ does not constitute a privacy break, it must hold that $\sum_{i=1}^{|S|} e^0_{i,j} = \sum_{i=1}^{|S|} e^1_{i,j}$ and $\sum_{j=1}^{t} e^0_{i,j} = \sum_{j=1}^{t} e^1_{i,j}$. This ensures that the adversary cannot win the game by learning these values. We note that all energy consumptions $e^b_{i,j}$ are chosen from R by the adversary.

SMPB Game. The electricity consumption scenarios M_0 and M_1 are given as input to the challenger who will choose a random bit $b \in \{0,1\}$ and simulate the smart meters over time using the consumption matrix M_b. The produced transcript with all messages that have been sent is delivered to the adversary. The adversary will output its decision, a bit, $d \in \{0,1\}$ and win the game if $d = b$. Dependent on the random bit b, we call the according game SMPB(b) for "smart meter privacy break", as sketched in Figure 1.

The chances of an adversary A to correctly guess the simulated scenario M_b are used to measure the privacy level of the SMA system.

Definition 1: Considering the SMPB game and the adversary A for a given SMA, the *smpb-advantage* of A is defined as

$$\mathbf{Adv}^{smpb}_{SMA}(S,R) = \\ \left|\Pr[\mathrm{SMPB}(0)^{\mathrm{A}}_{\mathrm{SMA}} = 0] - \Pr[\mathrm{SMPB}(1)^{\mathrm{A}}_{\mathrm{SMA}} = 0]\right|. \quad (1)$$

Informally speaking, the *smpb-advantage* of A denotes the adversary's advantage over random guessing in determining which energy consumption scenario is simulated in the game.

Definition 2: An SMA is *δ-privacy preserving* if $\mathbf{Adv}^{smpb}_{SMA}(S,R) < \delta$. An SMA is *perfectly privacy preserving* if $\mathbf{Adv}^{smpb}_{SMA}(S,R) = 0$.

PRACTICAL IMPLICATIONS OF THE SMPB GAME. We have proposed a game-based approach for measuring the privacy level that a smart metering application can provide. The idea behind this approach is to model ideal conditions for the adversary. In the real world, the quality of a smart metering privacy solution may depend on the actual usage patterns, i.e. the values $e_{i,j}$; section V-B will present a solution where this is the case. By letting the adversary choose these values, we make sure that the worst possible conditions (from a privacy perspective) are considered. It is possible for an adversary to choose the matrices M_0 and M_1 so that even correctly guessing just one individual value $e_{i,j}$ allows winning the game. If the smart metering application perfectly protects the customers' privacy, the protocol transcripts for both matrices are indistinguishable for the adversary (e.g., the electricity supplier) despite these preconditions. This means that a smart metering application has to produce random-looking transcripts to protect the privacy of smart meters.

As the row sums and the column sums of electricity consumption matrices are legitimate public knowledge, our game is defined so that knowing them does not mean an advantage for the adversary.

V. SAMPLE DESIGNS FOR ACHIEVING PRIVACY

In this section we describe two smart metering architectures. The first solution uses a trusted third party (TTP) to protect the privacy of smart meters. A statistical approach for achieving the required properties is presented as our second solution without involvement of a TTP.

A. Solution with a TTP

The solution uses a TTP as an aggregation proxy. More specifically, smart meters send their readings to the TTP using some form of encrypted communication. To prevent the energy supplier from analyzing the individual energy consumptions against statistical patterns, the TTP does not send the individual values but their aggregation (i.e., sum of all smart meters' readings during the period) to the ES. Moreover, at the end of a billing period, the TTP sums up individual consumptions for each smart meter, tags the sums with the identity, and sends these values to the electricity suppliers as well. The TTP helps keeping identity information separate from the detailed usage information. Note that the TTP itself maybe seen as a threat to privacy; however, as it does not need to have a contractual relationship with the customers, it does not need to know their real-world identities[1], thus reducing (though not eliminating) that threat. Sender anonymity is achieved since there is no direct connection between the electricity supplier and the smart meters.

MODELLING OF THE TTP PROTOCOL. We consider a set of smart meters S, and a set of all possible energy consumptions R. The adversary will choose two consumption matrices $M_0 = (e^0_{i,j})_i, j$ and $M_1 = (e^1_{i,j})_i, j$ with $\sum_{i=1}^{|S|} e^0_{i,j} = \sum_{i=1}^{|S|} e^1_{i,j}$ and $\sum_{j=1}^{t} e^0_{i,j} = \sum_{j=1}^{t} e^1_{i,j}$. If we assume that the ES cannot eavesdrop on the network communication between the consumers and the TTP, the transcript produced by the challenger is essentially empty, containing only the sums $\sum_{i=1}^{|S|} e^b_{i,j}$ and $\sum_{j=1}^{t} e^b_{i,j}$ that are reported to ES. Therefore it is obvious that the adversary cannot distinguish between $SMPB(0)$ and $SMPB(1)$ and the advantage is 0. Thus perfect privacy holds for the TTP protocol.

If we assume eavesdropping capabilities for the ES, the transcript that is produced by the challenger using the TTP protocol contains encryptions of all individual consumption values $e^b_{i,j}$, and perfect privacy holds only with the assumption of perfect encryption such as the one-time pad. However, the protocol can still be considered secure with practical encryption schemes such as AES. The security in this case is superpolynomial in the key length of the encryption key.

OBSERVATION. This simple mechanism allows an attack by the electricity supplier if the SMPB game is not played fairly. It might be considered practical to let the electricity supplier create the groups of smart meters whose readings are aggregated: The ES has the contractual relationships with the customers, and it might also be helpful for the ES to select groups based on its electricity network topology or geographical features. If using that approach, the following attack is possible: Assume the TTP provides the electricity supplier with the aggregated electricity consumption of, say, groups containing 50 smart meters each. The electricity supplier could now create a group with one real smart meter and 49 fake smart meters each of which reports a pre-determined value chosen by the electricity supplier. By submitting electricity consumption values for each of them and subtracting them from the retrieved sum, it would be easy to compute the actual power consumption of the 50th smart meter. However, this attack requires n fake groups for breaking privacy of n smart meters. Attempting this on a large scale can easily be detected if the approximate total number of (real) customers is known to the TTP.

B. Solution without a TTP

This solution has the main aim of being simple. The basic principle is that each electricity meter takes its current reading $e_{i,j}$ and adds a random value $r_{i,j}$ drawn from a known distribution with a known (finite) variance σ^2 and expectation μ. This results, basically, in the sent value to be distributed around the sum of the actual value and the expectation of the

[1] ES and TTP can agree on arbitrary identifiers for each smart meter; the ES needs to know the mapping to an actual customer, who receives the bill. The TTP is only required to sum up the electricity consumptions for each smart meter identity over the course of several time periods.

distribution. Instead of $e_{i,j}$, the value to be transmitted will be $e_{i,j} + r_{i,j}$. For simplicity, we assume the expectation of the random distribution to be $\mu = 0$ (without loss of generality, as the expectation needs to be known, anyway). The smart meters determine the random values $r_{i,j}$ independent from each other.

The expected value of the sums of all c electricity readings for each period does not change: The expected value of $e_{i,j} + r_{i,j}$ is $e_{i,j}$, since the expected value of the random distribution is 0. Consequently, the same holds for $\sum_{i=1}^{c} e_{i,j} + r_{i,j}$.

The individual variance of $e_{i,j} + r_{i,j}$ is σ^2, as $e_{i,j}$ is not drawn from a random distribution. Individual distributions being independent from each other, the variance of that sum distribution (i.e., the distribution of $\sum_{i=1}^{c} e_{i,j} + r_{i,j}$ is equal to the sum $c\sigma^2$ of the single (identical) variances).

According to the central limit theorem (and taking into account that $\mu = 0$),

$$\frac{\sum_{i=1}^{c} r_{i,j}}{\sigma\sqrt{c}} \tag{2}$$

can be approximated with a standard normal distribution for large enough c (which we can safely assume for $c > 30$).

To see if this approach may be helpful in practice, we have to introduce some more assumptions. First of all, let the individual smart meters' random distributions be normal distributions with parameters $\mu = 0$ and σ.

We want to achieve individual readings which are as blurry as possible. We measure this with the width of the 50% confidence interval. This should be at least $2v$, where v should be sufficient to hide typical power consumption behaviour (e.g., v could be set to $0.1kWh$ for the aggregated power consumption of 15 minutes—this value would, however, still be insufficient for hiding the electricity consumption of a washing machine). Using the formula for the confidence intervals of a normal distribution, we get

$$v = N(0.75)\sigma = 0.6745\sigma \Rightarrow \sigma = 1.483v \tag{3}$$

, where $N(x)$ is the $x-$quantile of the standard normal distribution.

For the sum distribution, on the other hand, we want to have as precise values as possible. Here, we use the 99.9% confidence interval, as electricity suppliers will want to have a high confidence in the aggregated value. Let the width of that confidence interval be $2w$. Assuming an average electricity consumption of 100 W per household, which is equivalent to 0.025 kWh in 15 minutes, a 1% deviation amounts to $w = 0.00025kWh$ per smart meter. As a result, a reasonable requirement could be trying to reach a 99.9% confidence interval with a maximum width of $2 \cdot 0.00025$ kWh.

We now use the fact that the term given in formula 2 follows a standard normal distribution. This even holds exactly if the individual smart meters use normal distributions.

A 99.9% confidence interval for this standard normal distribution has a width of $2 \cdot 3.2905$. For the distribution of $\sum_{i=1}^{c} r_{i,j}$, this means that the confidence interval width is $2 \cdot 3.2905 \cdot \sigma\sqrt{c}$. On a per-customer basis, this leads to

$$w = \frac{3.2905 \cdot \sigma}{\sqrt{c}} \tag{4}$$

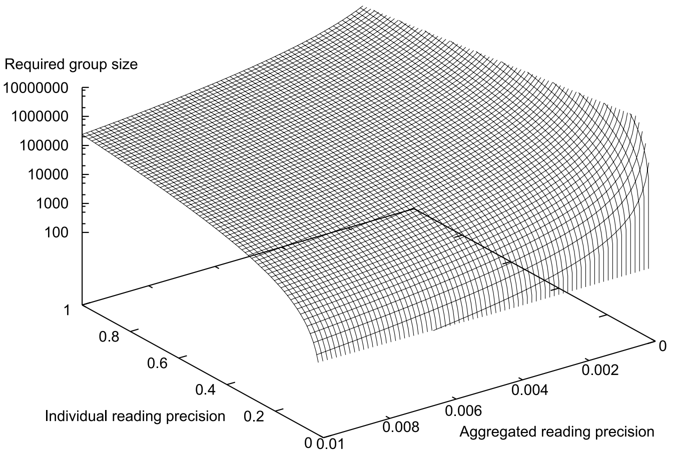

Fig. 2. Precision of individual and aggregated readings

With $w = 0.00025kWh$, $\sigma = 1.483v$, $v = 0.1$ kWh, we get

$$c = (\frac{3.2905 \cdot 1.483 \cdot v}{w})^2 \tag{5}$$

Using the example numbers for v and w as specified above, we come to

$$c = (\frac{3.2905 \cdot 1.483 \cdot 0.1kWh}{0.00025kWh})^2 = 3,810,000 \tag{6}$$

This result means that, to satisfy the above-mentioned conditions, at least 3,810,000 customers are needed. With small groups, it is not easily possible to achieve the desired level of privacy—this will probably be a major issue of practical deployments of this scheme. A more advanced selection of the individual probability distributions, not necessarily independent of each other, may be helpful as a refinement. Figure 2 shows the tradeoff between the precision of individual and aggregated readings. Individual precision is half the width of the 50% confidence interval, while the precision of the aggregated readings is half the width of the 99.9% confidence interval for the average user's reading. On the z axis, we show the number of smart meters in a group. The scales on the x and y axes have been selected under the assumption of short (i.e., about 15 minutes) reading intervals. They can be thought of as kWh values, but in fact, only the relation between the x and y axis values is relevant.

In addition to the transmission of a value per period, the ES also needs aggregated information at the end of the billing period. In this approach, we have to rely on each smart meter, which is a trusted device, to transmit this aggregated information over a secure channel when required.

We evaluate the approach using the game from Section IV. In the first step, the adversary chooses energy consumption matrices M_0, M_1. In order to achieve the best possible distinction between the two, the best strategy for the adversary is to set half of the entries $e_{i,j}^{0}$ of M_0 to 0, and the others to the maximum permitted value z. The entries of M_1 are then chosen as $e_{i,j}^{1} = z - e_{i,j}^{0}$.

Now when the adversary is given the protocol message of one smart meter and one period, its decision function is simple: If the transmitted smart meter reading $e_{i,j} + r_{i,j}$ is smaller than $\frac{z}{2}$, the adversary assumes that $e_{i,j} = 0$, and selects the corresponding scenario. Otherwise, it assumes that $e_{i,j} = z$. As defined in equation 1, we consider only the cases in which the adversary decides for scenario 0. As a further simplification and without loss of generality, we assume that $e_{i,j} = 0$ in scenario 0, and $e_{i,j} = z$ in scenario 1 (we can do so because of the problem's symmetry).

The adversary will decide for scenario 0

- if this is the correct scenario, and $r_{i,j} < \frac{z}{2}$.
- if scenario 1 would be correct, and $r_{i,j} \leq -\frac{z}{2}$

Since r is drawn from a normal distribution, we can now compute the probabilities from equation 1:

$$\Pr[\mathrm{SMPB}(0)^{\mathrm{A}}_{\mathrm{SMA}} = 0] = \Phi(\frac{z}{2}) \tag{7}$$

$$\Pr[\mathrm{SMPB}(1)^{\mathrm{A}}_{\mathrm{SMA}} = 0] = \Phi(-\frac{z}{2}) = 1 - \Phi(\frac{z}{2}) \tag{8}$$

In these equations, Φ is the cumulative distribution function of the probability distribution from which r is drawn—in our case, a normal distribution with expectation $\mu = 0$ and variance σ^2.

Let Φ_S be the distribution function of the standard normal distribution. We then have $\Phi(\frac{z}{2}) = \Phi_S(\frac{z}{2\sigma})$. Using the value for σ selected in equation 3, $\sigma = \frac{v}{N(0.75)}$, we get

$$\Phi(\frac{z}{2}) = \Phi(\frac{N(0.75)}{2} \cdot \frac{z}{v}) \tag{9}$$

The adversary can observe more than one transmitted value, of course. The more transmitted messages it observes, the better are its chances of winning the game. As discussed above, the sum of k normal distributions with identical variances σ^2 is again a normal distribution with variance $k\sigma^2$ (we call its cumulative distribution function Φ^k). Here, k is the number of messages observed by the adversary, i.e. the product of the number of smart meters and the number of periods. We assume in this case the adversary decides for scenario 0

- if this is the correct scenario, and $r^k_{i,j} < \frac{zk}{2}$,
- if scenario 1 would be correct, and $r^k_{i,j} \leq -\frac{zk}{2}$.

where r^k is drawn from a normal distribution with variance $k\sigma^2$, meaning a standard deviation of $\sqrt{k}\sigma$. With this, we can compute the advantage of the adversary:

$$\Pr[\mathrm{SMPB}(0)^{\mathrm{A}}_{\mathrm{SMA}} = 0] = \Phi^k(\frac{zk}{2}) = \Phi_S(\frac{zk}{2\sqrt{k}\sigma}) \tag{10}$$

$$\Pr[\mathrm{SMPB}(1)^{\mathrm{A}}_{\mathrm{SMA}} = 0] = 1 - \Phi^k(\frac{zk}{2}) = 1 - \Phi_S(\frac{zk}{2\sqrt{k}\sigma}) \tag{11}$$

Therefore, we have

$$\mathbf{Adv}^{smpb}_{SMA}(S, R) = 2\Phi_S(\frac{zk}{2\sqrt{k}\sigma}) - 1 \tag{12}$$

With the values selected above, we get

$$\mathbf{Adv}^{smpb}_{SMA}(S, R) = 2\Phi_S(\frac{z\sqrt{k} \cdot N(0.75)}{2v}) - 1 \tag{13}$$

This equation shows that the adversary's advantage gets big if it observes many messages, or if the amplitude of the added noise (represented by σ, or by v) is small in comparison to the maximum possible value z. In our model, the adversary's advantage easily gets very big. If a high precision for the aggregated values is needed, as we assumed in the previous considerations, it is close to 1 for any realistic parameter combinations. This does not necessarily mean that the approach is not useful for practical scenarios, as the assumptions of the game favor the adversary, and privacy will be better in practical scenarios. However, more research is necessary to develop this approach to a solution that is both applicable in practice and provably secure from a privacy perspective.

VI. Evaluation

Besides the main privacy requirement, as modelled in Section IV and discussed in the descriptions of the solution approaches, both approaches also fulfill the other requirements set forth in Section III.

If some *missing values* occur during a period, the ES can still estimate the current overall electricity consumption. In case of the TTP approach, the TTP can inform the ES about the number of missing values, or can perform the estimate itself. Without a TTP, that estimation gets even simpler, as the ES itself knows the previous values it got from the respective smart meters.

When one customer's *aggregated readings* are needed for billing purposes at the end of a billing period, they can be sent by the smart meter itself (which is a trusted device), or by the TTP in case of the solution from Section V-A. Neither of our approaches requires any *setup* per period.

VII. Conclusion

In this paper, we have presented initial work on smart meter privacy. This includes modeling of the problem, as well as two solution approaches. Future work will further refine the solution approaches, e.g. by considering other probability distributions to be used for the approach without TTP.

References

[1] G. Wood and M. Newborough, "Dynamic energy-consumption indicators for domestic appliances: environment, behaviour and design," *Energy and Buildings*, vol. 35, no. 8, pp. 821–841, 2003.

[2] A. Jamieson, "Smart meters could be 'spy in the home'," *Telegraph.co.uk, Oct 11*, 2009, http://www.telegraph.co.uk/finance/newsbysector/energy/6292809/Smart-meters-could-be-spy-in-the-home.html.

[3] M. Karg, "Datenschutzrechtliche Bewertung des Einsatzes von "intelligenten" Messeinrichtungen für die Messung von gelieferter Energie (Smart Meter)," https://www.datenschutzzentrum.de/smartmeter/20090925-smartmeter.pdf, Sep 2009, unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

[4] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *Security & Privacy, IEEE*, vol. 7, no. 3, pp. 75–77, May-June 2009.

[5] R. Tangens, "Big Brother Award 2008, category Technology: Yello Strom GmbH," http://www.bigbrotherawards.de/2008-en/.tec.

[6] L. Sweeney, "k-anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[7] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: the second-generation onion router," in *SSYM'04: Proceedings of the 13th conference on USENIX Security Symposium.* Berkeley, CA, USA: USENIX Association, 2004, pp. 21–21.

[8] M. K. Reiter and A. D. Rubin, "Anonymous web transactions with crowds," *Commun. ACM*, vol. 42, no. 2, pp. 32–48, 1999.

[9] S. Vaudenay, "On Privacy Models for RFID," in *Advances in Cryptology - Asiacrypt 2007*, ser. Lecture Notes in Computer Science. Springer-Verlag, 2007, pp. 68–87.