A Decisional Attack to Privacy-friendly Data Aggregation in Smart Grids

Cristina Rottondi*, Marco Savi*, Daniele Polenghi*, Giacomo Verticale*, and Christoph Krauß†
* Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Piazza Leonardo da Vinci, 32, Milano, Italy
rottondi@elet.polimi.it, savi@elet.polimi.it, daniele.polenghi@mail.polimi.it, vertical@elet.polimi.it
† Fraunhofer Research Institution for Applied and Integrated Security, Parkring 4, Garching b. Muenchen, Germany
christoph.krauss@aisec.fraunhofer.de

***Abstract*—The privacy-preserving management of energy consumption measurements gathered by Smart Meters plays a pivotal role in the Automatic Metering Infrastructure of Smart Grids. Grid users and standardization committees are requiring that utilities and third parties collecting aggregated metering data are prevented from accessing measurements at the household granularity, and data perturbation is a technique used to provide a trade-off between the privacy of individual users and the precision of the aggregated measurements.**

In this paper, we discuss a decisional attack to aggregation with data-perturbation, showing that a curious entity can exploit the temporal correlation of Smart Grid measurements to detect the presence or absence of individual data generated by a given user inside an aggregate. We also propose a countermeasure to such attack and show its effectiveness using both synthetic and real home energy consumption measurement traces.

***Index Terms*—Smart Grid; Metering Data Aggregation; Differential Privacy; Decisional Attack.**

I. Introduction

In the next years, the electric grid will experience an unprecedented innovation process: according to the "Smart Grid" paradigm, the integration of Information and Communication Technologies (ICT) with the infrastructure for electricity dispatchment will improve the effectiveness of power distribution and optimize the grid management. The evolution of the electric grid will affect also the meters located at the customers' premises to monitor their power consumption, which will be replaced by "intelligent" electronic devices called "Smart Meters": such devices will be capable not only of generating fine-grained measurements of the electricity usage, but also of providing several value added services.

Since Smart Meters are connected to the Smart Grid communication network through the Automatic Metering Infrastructure (AMI) to send their readings to the power suppliers, privacy and confidentiality of metering data must be ensured. It has been shown [1], [2] that external subjects might access these data and infer private informations about the users by exploiting the electricity usage readings to profile the customers' behaviour and even to determine which household appliances are being used.

Therefore, a secure and privacy-friendly collection framework for data gathered by the Smart Meters must be integrated in the Smart Grid ecosystem. Privacy-preserving solutions include the usage of different types of encryption schemes and routing protocols, as well as techniques for data aggregation, anonymization and obfuscation through noise addition. In particular, the latter approach has been widely investigated in the recent literature (see [3] for a survey), since it has been proved (e.g. in [4]) that process of aggregation/anonymization performed over exact data is not sufficient to avoid information leakages. A possible way to perform obfuscation of individual energy consumption measurements is to place batteries at the customers' premises in order to offset electric loads themselves, thus masking occupant and device behaviors [5]. The drawback of this approach is the cost of installation and maintenance of the energy storage devices.

The approach we adopt in this paper is to apply data perturbation techniques relying on noise addition performed by the metering device itself, as inspired by the concept of differential privacy [6]. In particular, we combine such techniques with the privacy-preserving distributed data aggregation infrastructure based on multiparty computation presented in [7], [8], in order to allow grid managers and external parties to obtain real-time aggregated energy consumption measurements with a sufficiently high level of precision, while preventing them from identifying the presence/absence of the consumption trace generated by a given customer inside the aggregate.

Such architecture relies on communication Gateways located at the users' premises and equipped with an Hardware Security Module providing cryptographic capabilities (according to the requirements of the Protection Profile, mandated by the German Federal Office for Information Security [9]), which collects the measurements generated by the local Meters, encrypt and aggregate them in a distributed fashion according to the aggregation rules specified by multiple External Entities (e.g. utilities, grid managers and third parties).

The main novel contributions of this papers are the following:

- we formalize the notion of *decisional attack* for time series, which is representative of a class of privacy attacks aimed at breaching the property of *indistinguishability* of any two users
- we propose a possible countermeasure to such attack and show its effectiveness through numerical results, obtained

Cristina Rottondi is funded by Fondazione Ugo Bordoni

with both synthetic and real home energy consumption measurement traces.

The remainder of the paper is structured as follows: Section II provides a brief overview of the related work, while Section III recalls some background notions. Our proposed data aggregation architecture is described in Section IV. The formalization of the attacker model and the decisional attack are discussed in Section V, while Section VI proposes a countermeasure to mitigate its effects. The effectiveness of attack and countermeasure is shown in Section VII through numerical results, in case of synthetic and real measurement traces. Section VIII concludes the paper.

II. Related Work

Our definition of *decisional attack* builds upon the notion of differential privacy, which was first introduced in [6]. Differential privacy refers to a general scenario in which it must be guaranteed that the removal or addition of a single item in a statistical database has negligible impact on the outcome of any query on that database. The author gives a formal definition of differential privacy as a measure of the trade-off between the accuracy of the aggregated data and the probability of identifying the contributions of individual data inside the aggregate, also describing how to achieve a certain level of differential privacy by exploiting data perturbation techniques performed by noise injection in the users' data. Our *decisional attack* for time series is based on the same principle: it consists in providing the adversary with the measurements of a given user i and with two aggregates, only one of them containing the data of user i. The attack succeeds if the attacker guesses which aggregate contains the data generated by user i. However, while the principles of differential privacy can be applied to the framework of a generic database, our approach is more focused on the specific characteristics of Smart Grid time series, resulting in simpler definitions.

Privacy-preserving data aggregation in Smart Grids can be achieved through various techniques: for a comprehensive overview on such approaches, the reader is referred to [10]. However, to the best of our knowledge, our proposed privacy-preserving infrastructure is the first allowing data collection for multiple subjects interested in accessing aggregated energy consumption measurements, each of them specifying its own aggregation request in terms of set of monitored users.

Some other papers combine cryptographic schemes with differential privacy techniques in order to compute aggregate statistics: in [11], a protocol for the distributed generation of random noise is proposed, aimed at the distributed implementation of privacy-preserving statistical databases. To do so, the protocol relies on a verifiable secret sharing scheme. Our proposed data aggregation is based on Shamir Secret Sharing scheme, which does not provide data integrity verification but is computationally less demanding.

Paper [12] designs a protocol for differentially private aggregation of temporally correlated time-series, which is achieved by perturbation of the Discrete Fourier Transform of the data and by distributed noise addition. The protocol is demonstrated to scale efficiently with the number of users, requiring a computational load per user of $O(1)$. Our solution also relies on noise addition, which is performed directly on the individual metering data.

Papers [13], [14], [15] apply the general notions expressed in [6] to the Smart Grid context. Paper [13] defines a scheme in which an electricity supplier is allowed to collect aggregated smart-metering measures without learning anything about the energy consumption and the household activities of individual users, and discusses how differential privacy is affected by considering multiple time slots. However, this paper does not deal with temporal correlation of smart-metering time-series data. Our proposal considers this feature, that can be exploited to reduce the level of privacy of the users' data.

Paper [15] deals with a scenario in which an untrusted aggregator collects privacy sensitive user data to periodically compute aggregate statistics. The proposed solution is resilient to user failure and compromise and supports dynamic joins and leaves of users. We also assume untrusted aggregation nodes, but we focus our attention on a static scenario.

Paper [14] defines a model of data aggregator capable of obtaining statistics about aggregated data without compromising the privacy of single users. The authors introduce a formal noise injection model and a new distributed data randomization algorithm in order to ensure users' differential privacy, assuming the existence of malicious users that reveal their statistics to the data aggregator. In this paper, we will use the same noise characterization. Moreover, the authors of [14] define an error bound for aggregated data and evaluate the trade-off between data utility and privacy. The same trade-off evaluation is discussed in papers [16], [17], which propose to filter low-power frequency components of smart-metering time-series data, in order to perform data obfuscation without compromising its statistical significance.

III. Background

a) Symmetric geometric distribution: Let α be a positive number such that $\alpha > 1$. The probability mass function of the symmetric geometric distribution $Geom(\alpha)$ is defined as:

$$\frac{\alpha - 1}{\alpha + 1}\alpha^{-|k|}$$

and k always assumes integer values.

The probability mass function of the unilateral geometric distribution $Geom^{+}(\alpha)$ is defined as:

$$(\alpha - 1)\alpha^{-k}$$

and k always assumes integer positive values.

The symmetric geometric distribution has zero mean and its variance is $2\alpha(\alpha - 1)^{-2}$.

b) Holder's inequality: Let p, q be real positive numbers such that $p, q > 1$ and $\frac{1}{p} + \frac{1}{q} = 1$, the Holder's inequality allows us to write:

$$\int_{-\infty}^{+\infty} |f(x) \cdot g(x)| \mathrm{d}x \leq \left(\int_{-\infty}^{+\infty} |f(x)|^{p} \mathrm{d}x \right)^{\frac{1}{p}} \left(\int_{-\infty}^{+\infty} |g(x)|^{q} \mathrm{d}x \right)^{\frac{1}{q}}$$

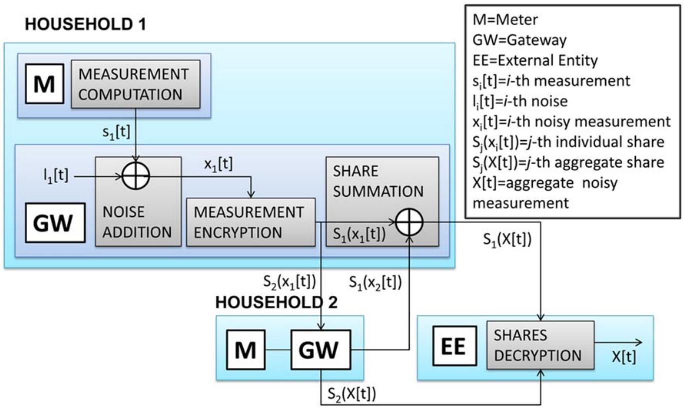

Fig. 1. The data aggregation procedure

If we consider $p = q = \frac{1}{2}$, it reduces to:

$$\int_{-\infty}^{+\infty} |f(x) \cdot g(x)| \mathrm{d}x \leq \sqrt{\int_{-\infty}^{+\infty} |f(x)|^2 \mathrm{d}x} \sqrt{\int_{-\infty}^{+\infty} |g(x)|^2 \mathrm{d}x}$$

Note that the equality holds iff $|f(x)| = c \cdot |g(x)|$, where c is an arbitrary constant.

IV. The Aggregation Architecture

In our data aggregation architecture we suppose N users (i.e. Meters) that are involved in the aggregation of their energy consumption measurements. At every time interval $t \in \mathbb{N}$, the measurements $s_i[t]$ generated by each Meter i ($1 \leq i \leq N$) are gathered by the the Gateway locally connected to the Meter itself. Note that a Gateway could be responsible for gathering the measurements of multiple Meters, e.g. all the Meters in a block of flats. After collecting the metering data $s_i[t]$, the Gateway performs noise injection by adding to $s_i[t]$ a zero-mean white noise $l_i[t]$ with power σ_l^2, as defined in [13], [6], [14], obtaining the noisy time-series metering data $x_i[t] = s_i[t] + l_i[t]$.

Our architecture (first introduced in [18] to perform exact data aggregation and briefly reviewed here) relies on Shamir Secret Sharing (SSS) scheme with threshold w which requires the Gateway to split $x_i[t]$ into w shares and allows the correct reconstruction of the measurement if at least $\bar{t} \leq w$ shares are available, where $\bar{t}$ is a design parameter (for the sake of easiness, in this paper we assume $\bar{t} = w$). The shares $S_j(x_i[t])$ ($1 \leq j \leq w$) of the noisy samples $x_1[t], \ldots, x_N[t]$ are then forwarded to the neighboring Gateways, which aggregate them with their local measurements according to the aggregation rules specified by the External Entities (EEs) by means of a set Π_e of Meters they want to monitor. Thanks to the homomorphic properties of SSS with respect to addition, the aggregated data obtained by summing the shares is the same that would be obtained by *first* summing the individual data and *then* encrypting the aggregate. Therefore, at each time interval t the EE expects to obtain the quantity:

$$X_e[t] = \sum_{i \in \Pi_e} x_i[t] = \sum_{i \in \Pi_e} s_i[t] + l_{tot}[t]$$

Note that $l_{tot}[t] = \sum_{i \in \Pi_e} l_i[t]$ is characterized by the power $\sigma_{l,tot}^2$ and that a well designed system should provide the minimum $\sigma_{l,tot}^2$ while providing a required level of privacy.

Note also that the architecture includes an additional node called Configurator, which is responsible for checking the compliance of the aggregation rules to the security policies of the grid and to instruct the Gateways accordingly. The routing of the communication flows among the network nodes can be performed either by the Configurator itself, with a centralized approach, or in a distributed fashion relying on the Chord peer-to-peer routing protocol. For a thorough discussion of the aggregation procedure and the associated communication protocol, the reader is referred to [18], [7]. Once the measurement aggregation is completed, the e-th EE (with $e \in E$, where E is the set of EEs) receives w aggregated shares $\bar{S}_j[t] = \sum_{i \in \Pi_e} S_j(x_i[t])$, and recovers the noisy aggregated measurement $X[t] = \sum_{i \in \Pi_e} x_i[t]$ through the Lagrange Interpolation algorithm.

An example of our proposed architectural model is depicted in Figure 1, which shows a scenario with $N = 2$ Meters monitored by a single EE and assumes $w = 2$. For the sake of easiness, we assume that each Gateway is associated to only one Meter. Therefore, after splitting the measurement of Meter 1 in two shares $S_1(x_1[t])$ and $S_2(x_1[t])$, Gateway 1 sends $S_2(x_1[t])$ to Gateway 2 and sums the share $S_1(x_1[t])$ to $S_1(x_2[t])$, which it has beforehand received from Gateway 2. Gateway 2 behaves analogously. The EE collects the aggregated shares $\overline{S}_1(X[t])$ and $\overline{S}_2(X[t])$ and recombines them to obtain the aggregated measurement $X[t] = x_1[t] + x_2[t]$.

V. Adversary Model and Decisional Attack

We assume that Gateways and EEs behave according to the *honest-but-curious* attacker model, i.e. they honestly execute the protocol, but they store all their inputs and process them in order to obtain additional information about the individual data. The nodes are supposed to have infinite memory. However, they cannot alter the routing nor the content of the exchanged messages (see [8] for a preliminary discussion of the impact of dishonest intrusive attackers).

In this paper, we consider an attack scenario in which a malicious EE has auxiliary information on the individual time series. Therefore, we assume that some of the Gateways can create collusions with the EEs, providing them with the individual measurements $s_i[t]$ of the local Meters, before performing noise addition. The EEs' knowledge of the individual measurements allows them to efficiently perform the decisional attack described hereafter.

First, we introduce the property of **indistinguishability** of any two users, which must be satisfied by the privacy-preserving infrastructure and is defined as follows:

Definition We say that the aggregation architecture provides **indistinguishability** of any two users if a decisional attack succeeds with probability $0.5 + \epsilon$, where ϵ is an arbitrarily low system design parameter.

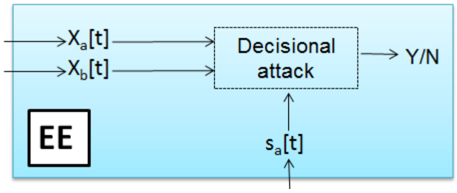

Fig. 2. The attack definition

To evaluate users' distinguishability, we define the following decisional problem:

Definition *Decisional Attack:* The adversary, i.e. the e-th malicious EE, is given the following noisy aggregate measurements:

$$X_a[t] = \sum_{i \in \Pi_e \setminus \{a,b\}} x_i[t] + x_a[t] = \sum_{i \in \Pi_e \setminus \{a,b\}} x_i[t] + (s_a[t] + l_a[t])$$

$$X_b[t] = \sum_{i \in \Pi_e \setminus \{a,b\}} x_i[t] + x_b[t] = \sum_{i \in \Pi_e \setminus \{a,b\}} x_i[t] + (s_b[t] + l_b[t])$$

These measurements are calculated over $|\Pi_e|$ participants and differ only by a single participant: a in the first aggregate and b in the latter. The attacker is also provided with the time-series smart metering data $s_a[t]$ of user a, which represents the auxiliary information. The adversary has to decide whether the user a participates in the noisy aggregate measurement $X_a[t]$ or $X_b[t]$. The attacker can perform any desired elaboration on the data: in particular, she can filter the aggregated data $X[t]$ with any Linear Time-Invariant (LTI) filter.

We suppose that the attacker knows $s_a[t]$ for $0 \leq t < T$. We consider a simple decision algorithm that calculates the correlation between the time-series $s_a[t]$ and $X_a[t]$ and between $s_a[t]$ and $X_b[t]$ as follows:

$$R_a = \sum_{t=0}^{T} X_a[t] s_a[t]$$

$$R_b = \sum_{t=0}^{T} X_b[t] s_a[t]$$

The adversary chooses the noisy aggregate measurement that results in the highest correlation with $s_a[t]$ and the attack succeeds if $R_a - R_b > 0$. Clearly, the higher is the noise power $\sigma^2_{l,tot}$, the less pronounced is the difference between R_a and R_b, thus making the probability of correct guess approach a coin toss.

Although the decisional attack is of limited interest for a real attacker, we believe that it has a significant theoretical value. In fact, any unspecified efficient algorithm capable of extracting personal information from the perturbed data can be used to successfully perform a decisional attack. Therefore, if for a given setup the decisional attack succeeds with low probability, then we expect that the amount of personal information that can possibly be extracted is negligible. Thus, preventing the attacker from detecting the presence of a known individual contribution inside an aggregated measurement through a decisional attack provides a valid countermeasure to a wide class of attacks affecting user's privacy.

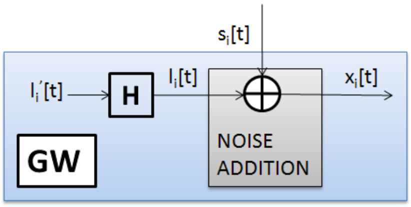

Fig. 3. The countermeasure definition

VI. Countermeasure Description

A. Countermeasure Description

As described in Section IV, the noise process $l_i[t]$ summed by the Gateways to the smart-metering data $s_i[t]$ is a zero-mean white noise. In Section V, we have defined a possible attack to reduce users' privacy exploiting the properties of correlation among signals.

Our proposed countermeasure to defy this kind of attack is shown in Figure 3. It consists in summing to the smart-metering data process $s_i[t]$ a zero-mean *colored* (i.e. correlated) noise $l_i[t]$, obtained by filtering the zero-mean white noise $l_i{}'[t]$ with a LTI digital filter H. This filter must be designed in order to minimize $\Pr\{R_a - R_b > 0\}$, i.e. the probability that the attack is successful. The expected value and the variance of $R_a - R_b$ can be calculated as:

$$\mathrm{E}[R_a - R_b] = \sum_{t=0}^{T} s_a[t]^2 - \sum_{t=0}^{T} s_a[t] s_b[t]$$

$$\mathrm{var}[R_a - R_b] = 2\sigma^2_{l'} \int_0^1 |\mathcal{H}(\phi)|^2 \cdot |\mathcal{S}_a(\phi)|^2 \mathrm{d}\phi \qquad (1)$$

where $\sigma^2_{l'}$ is the variance of the processes $l_a{}'[t]$ and $l_b{}'[t]$, ϕ is the normalized frequency and $\mathcal{S}_a(\phi)$ and $\mathcal{H}(\phi)$ are the Discrete Fourier Transform of $s_a[t]$ and of the impulse response $h[t]$ of the filter H, respectively.

In order to minimize $\Pr\{R_a - R_b > 0\}$, we design the filter H that maximizes the right-hand side of (1), which leads to the following maximization problem:

$$\max \int_0^1 |\mathcal{H}(\phi)|^2 \cdot |\mathcal{S}_a(\phi)|^2 \mathrm{d}\phi$$

Considering the Holder's inequality reported in Section III, we can easily write that maximum is obtained when:

$$|\mathcal{H}(\phi)|^2 = c \cdot |\mathcal{S}_a(\phi)|^2 \qquad (2)$$

with c an arbitrary constant.

In general, we can conclude that the filter H must shape the noise random process $l_i[t]$ such that its frequency characterization is as similar as possible to the frequency characterization of the data sequence $s_i[t]$.

In the remainder of this Section, we consider a synthetic and a data-driven model for smart-metering data. Synthetic data and real measurement traces allow us to design the filter H in these two specific scenarios, exploiting the signal characterization in terms of correlation between samples.

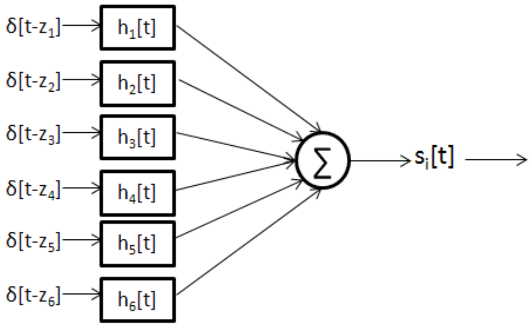

Fig. 4. The model using real measurement data

B. Synthetic data

We first assume that the time-series smart metering data of each user i is modelled as a colored Gaussian random process $s_i[t]$, obtained by filtering a white Gaussian process with an LTI filter K. The input of K is a white Gaussian random process $n_i[t]$ with mean μ_n and variance σ_n^2. We assume that all the N Meters generate independent data streams with the same statistical properties. The Gateways perform noise injection by adding to $s_i[t]$ a zero-mean white noise $l_i[t]$.

In this scenario, the countermeasure consists in filtering at the Gateways the zero-mean white noise $l_i{}'[t]$ with the filter $H = K$, which satisfies (2) obtaining the colored noise process $l_i[t]$, before adding it to the smart metering data $s_i[t]$.

In this way, it is difficult to discriminate the noise $l_i[t]$ from the smart-metering measurement $s_i[t]$, since they have similar spectral behavior.

C. Real measurements

We now define a data model that better matches real home energy consumption measurements. To do so, we consider six different categories of appliances (i.e. light bulbs, oven and microwave oven, television and personal computer, refrigerator, boiler, washing machine and dishwasher). The energy consumption pattern of the j-th appliance (provided by [19]) is sampled every fifteen minutes within a day, from 00:00 to 23:59, in order to obtain $T = 96$ samples, and modelled as a discrete impulse response $h_j[t]$.

These impulse responses are combined to generate the independent time-series $s_i[t]$ for each user i. Every process $s_i[t]$ is generated by summation of the appliances' consumption curves, each of them shifted in a circular way by an integer random delay z_j with uniform distribution in the interval $[0, 48]$ (maximum shift of 12 hours), as shown in Figure 4.

Also in this scenario, our countermeasure follows the approach defined in Section VI-A, i.e. the addition of colored distributed noise. Since K (see Section VI-B) is not uniquely defined, in this case we design H by using a *single-pole autoregressive (AR) spectral estimation* of the noiseless aggregate measurement $\sum_{i\in\Pi_e} s_i[t]$. In this way, we give to the noise a PSD characterization as similar as possible to the PSD characterization of the noiseless measurement, as defined in (2), through an LTI filter which is simple to be designed.

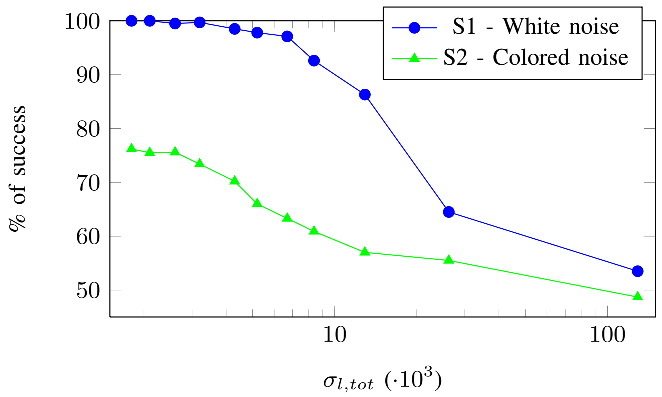

Fig. 5. Percentage of attack success as a function of the aggregate noise standard deviation $\sigma_{l,tot}$, using synthetic measurement traces and assuming $|\Pi_e| = 50$ and $T = 100$ samples.

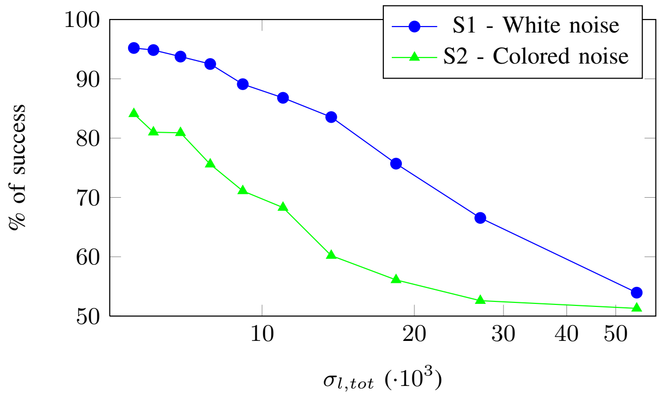

Fig. 6. Percentage of attack success as a function of the aggregate noise standard deviation $\sigma_{l,tot}$, using real measurement traces and assuming $|\Pi_e| = 50$ and $T = 96$ samples.

VII. Performance Evaluation

In order to evaluate the effectiveness of our proposed countermeasure to the decisional attack, we apply the decisional problem to different scenarios, with both synthetic and real home energy consumption traces. More in detail, we consider the following two scenarios:

S1. $X_a[t]$ and $X_b[t]$ are obtained by adding white noise with symmetric geometric distribution (see Section III for its definition), generated according to the algorithm defined in [14] ($l_i[t] \sim Geom(\alpha)$);

S2. $X_a[t]$ and $X_b[t]$ are obtained by adding colored noise with $l_i{}'[t] \sim Geom(\alpha')$ ($l_i[t] = l_i{}'[t] * h[t]$), in order to increase user indistinguishability;

Results are averaged over 4000 instances for each scenario, in order to have confidence intervals below 10%.

A. Numerical results with synthetic data

We first evaluate the performance of our proposed countermeasure using synthetically generated data traces. The values chosen for the simulation parameters are $\mu_n = 700$, $\sigma_n = 350$, while $k[t]$ is defined as a 9-samples triangular filter with unitary energy. Figure 5 plots the percentage of the attacker's success in the identification of the aggregate containing the individual data $s_a[t]$, for different values of the aggregate noise standard deviation $\sigma_{l,tot}$. Results show that the injection of colored noise considerably decreases the probability of correct guess (scenario S2) with respect to the usage of white noise (scenario S1). Moreover, for high values of $\sigma_{l,tot}$, the probability of success approaches 50% in both the scenarios, which means that the attacker obtains no additional information from the aggregated measurements and that the decision criterion can be assimilated to a coin tossing.

B. Numerical results with real data

We then consider real data traces, generated as described in Section VI-C, where $h[t] = u[t]\eta^t$ (with $\eta = 0.95$). Analogously to Figure 5, Figure 6 plots the percentage of the attacker's success as a function of the aggregate noise standard deviation $\sigma_{l,tot}$, for the two scenarios. The trend is similar with respect to Figure 5.

VIII. Conclusions

This paper discusses definition of privacy called *indististinguishability of any two users* and a corresponding decisional attack to the privacy of the users involved in the aggregation of individual energy consumption data gathered by the Smart Meters in the Automatic Metering Infrastructure of Smart Grids. Our approach captures the intuition that the privacy of a user is preserved if an observer cannot tell whether the user's data is present or missing in a given aggregate.

We consider a setup with a distributed data aggregation infrastructure relying on communication Gateways located at the customers' premises, which collect the measurements from the Meters, perform noise injection, encrypt the noisy data using Shamir Secret Sharing scheme and then aggregate the encrypted data. We show how an attacker can exploit the temporal correlation of the metering data in order to identify the presence of the measurements generated by a given user inside the aggregate, and propose a countermeasure to such attack. Numerical results obtained with both synthetically generated and real energy consumption traces show the effectiveness of our proposed technique.

References

[1] G. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870 –1891, dec 1992.

[2] C. Laughman, K. Lee, and R. e. a. Cox, "Power signature analysis," *Power and Energy Magazine, IEEE*, vol. 1, no. 2, pp. 56 – 63, mar 2003.

[3] K. Muralidhar and R. Sarathy, "Perturbation methods for protecting numerical data: Evolution and evaluation," in *Proceedings of the 5th Security Conference*, Apr. 2006.

[4] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, ser. SP '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 111–125. [Online]. Available: http://dx.doi.org/10.1109/SP.2008.33

[5] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, 2011, pp. 1932–1935.

[6] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2006, vol. 4052, pp. 1–12. [Online]. Available: http://dx.doi.org/10.1007/11787006_1

[7] C. Rottondi, G. Verticale, and C. Krauß, "Distributed privacy-preserving aggregation of metering data in smart grids," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, 2013.

[8] C. Rottondi, M. Savi, D. Polenghi, G. Verticale, and C. Krauß, "Implementation of a protocol for secure distributed aggregation of smart metering data," in *IEEE SG-TEP, 1st International Conference on Smart Grid Technologies, Economics and Policies*, Dec. 2012.

[9] Federal Office for Information Security, "Protection profile for the gateway of a smart metering system," 2011. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf

[10] M. Jawurek, F. Kerschbaum, and G. Danezis, "Sok: Privacy technologies for smart grids a survey of options." 2012. [Online]. Available: http://www.research.microsoft.com/pubs/178055/paper.pdf

[11] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: privacy via distributed noise generation," in *Proceedings of the 24th annual international conference on The Theory and Applications of Cryptographic Techniques*, ser. EUROCRYPT'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 486–503. [Online]. Available: http://dx.doi.org/10.1007/11761679_29

[12] V. Rastogi and S. Nath, "Differentially private aggregation of distributed time-series with transformation and encryption," in *Proceedings of the 2010 ACM SIGMOD International Conference on Management of data*. New York, NY, USA: ACM, 2010, pp. 735–746. [Online]. Available: http://doi.acm.org/10.1145/1807167.1807247

[13] G. Acs and C. Castelluccia, "I have a DREAM!(differentially private smart metering)," in *The 13th Information Hiding Conference (IH)*, 2011.

[14] E. Shi, T. Chan, and e. a. Rieffel, "Privacy-preserving aggregation of time-series data," in *NDSS Symposium*, Aug. 2011.

[15] T. Chan, E. Shi, and D. Song, "Privacy-preserving stream aggregation with fault tolerance," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, A. Keromytis, Ed. Springer Berlin / Heidelberg, 2012, vol. 7397, pp. 200–214.

[16] S. Rajagopalan, L. Sankar, S. Mohajer, and H. Poor, "Smart meter privacy: A utility-privacy framework," in *Smart Grid Communications, 2011 IEEE International Conference on*, oct. 2011, pp. 190 –195.

[17] L. Sankar, S. R. Rajagopalan, S. Mohajer, and H. V. Poor, "Smart meter privacy: A theoretical framework," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 837–846, 2013.

[18] C. Rottondi, G. Verticale, and A. Capone, "Privacy-preserving smart metering with multiple data consumers," *Computer Networks*, vol. 57, no. 7, pp. 1699 – 1713, 2013.

[19] "Micene Project," http://www.eerg.it/index.php?p=\\Progetti_-_MICENE, apr 2012.