Privacy Violations in Constrained Micro-grids: Adversarial Cases

Pacome L. Ambassa*, Anne V.D.M. Kayem*, Stephen D. Wolthusen[†‡] and Christoph Meinel[§]
*Department of Computer Science, University of Cape Town, Rondebosch, Cape Town, South Africa 7701
Email: pambassa@cs.uct.ac.za, akayem@cs.uct.ac.za
[†] Department of Mathematics, Information Security Group, Royal Holloway, University of London, Egham, UK
[‡]Norwegian Information Security Laboratory, Gjøvik University College, Gjøvik, Norway
Email: stephen.wolthusen@rhul.ac.uk
[§]Hasso-Plattner-Intitut, Potsdam, Germany
Email: meinel@hpi.de

***Abstract*—Smart micro-grid architectures are small scale electricity provision networks composed of individual electricity providers and consumers. Supporting micro-grids with computationally limited devices, is a cost-effective approach to service provisioning in resource-limited settings. However, the limited availability of real time measurements and the unreliable communication network makes the use of Advanced Metering Infrastructure (AMI) for monitoring and control a challenging problem. Grid operation and stability are therefore reliant on inaccurate and incomplete information. Consequently, data gathering and analytics raise privacy concerns for grid users, which is undesirable. In this paper, we study adversarial scenarios for the privacy violations on micro-grids. We consider two types of privacy threats in constrained micro-grids, namely inferential and aggregation attacks. The reason is that both attacks capture scenarios that can be used to provoke energy theft and destabilize the grid. Grid destabilzation leads to distrust between suppliers and consumers. This work provides a roadmap towards a secure and resilient smart micro-grid energy networks.**

***Keywords*-Aggregation attack, inference attack, micro-grid, privacy.**

I. Introduction

A recent report [1] estimated that nearly 1.3 billion people or 18% of the world's population did not have access to electricity in 2011. A vast majority of people without reliable access to electricity lives mostly in rural and isolated areas in developing countries. In developing regions, electricity access is undermined by the absence of supply from the national power grid and/or load shedding [2], [3]. A suitable way of providing power in rural and remote communities is through Smart micro-grids (MGs) networks which are based on a distributed power generation and a low-cost communication network [4] [3].

In such MGs, a large propotion of electricity is generated from volatile renewable sources. Energy management is essential to grid stability [5]. Demand Management (DM) and energy market are two approaches used to regulate energy distribution. DM is a planning mechanism for smoothing the power demand profile of the MG over time, and this helps avoid periods of power over-consumption that could result in mismatching the power supply and demand profile. Moreover, DM is improved by performing load prediction to enable estimation of the future load demands and generation projection. On the other hand, local energy markets play an important role in making the MG more reliable and resilient to the variable nature of energy generation and consumption.

To ensure the reliable operation of power grids, monitoring is necessary for data collection and state estimation of the MG. The standard smart grid monitoring relies on an Advanced Metering Infrastructure (AMI) such as smart meters (SMs), highly calibrated, trustworthy sensors and an extensive communication infrastructure. Due to their high cost, SMs are not ideal for community-based micro-grids. In addition, insecure communication channels make the security and dependability of the MG network a challenge. As an example of the unique security challenges that emerge in the context of smart micro-grids, an adversary can very easily gain access to private information by monitoring transmission between nodes [6].

The power consumption information from the household within micro-grids creates a large amount of time series data that are privacy-sensitive. Research results have shown that energy consumption patterns can be used to leak private information about the activities and behavior of the inhabitants of a household [7], [8], [9] [10]. Privacy-preserving solutions based on anonymization and data perturbations have been proposed to address this problem. These schemes work well on big data and high computation capacity networks. Existing privacy-preserving solutions will not work well for such micro-grids.

In this paper, we model inference and aggregation attacks for energy theft and destabilization in constrained MGs. We demonstrate that these attacks are possible because existing solutions fail to handle small data and computationally limited scenarios effectively. Subsequently, we provide a discussion on how privacy violations can affect micro-grids to understand the consequences of attacks presented.

The remainder of the paper is structured as follows. In Section II, a brief review of related work is given. Section III presents an isolated community MG system model and identifies security requirements. Privacy threat models and

978-1-5090-2461-2/16 $31.00 © 2016 IEEE
DOI 10.1109/WAINA.2016.98

IEEE computer society

a variety of MG privacy attacks are presented in Section IV. Section V presents the consequences of privacy threats in MGs. Finally, Section VI concludes the paper and offers some directions for future work.

II. Related Work

Security and privacy issues are critical for building dependable small scale power network systems. Many works have been carried out to address security and privacy in large-scale smart power grid environments.

The notion of pseudonymization was one of the pioneering privacy solutions that worked by replacing data set identifiers with a pseudonym [11].

Efthymiou and Kalogridis [12] present a simple pseudonymization approaches where a Trusted Third Party (TTP), escrow mechanism manages the pseudonyms to make linking attacks difficult. However, Jawurek *et al.* [13] demonstrated that link attacks can be used to foil pseudonymization schemes, if the adversary has access to external background knowledge.

k-anonymity was subsequently proposed in [14] as a privacy enforcing scheme for datasets. *k*-anonymity works by identifying a set of quasi-identifiers that are then hidden in a cluster of at least *k* records. However, *k*-Anonymity and its improvements *l*-diversity [15] and *t*-closeness [16] cannot be directly applied to time series data set as the attributes are both quasi-identifiers and sensitive attributes [17].

Data perturbation approaches, particularly differential privacy, have also been studied as effective privacy preserving mechanisms in the area of smart power networks [18],[19],[20]. While on one hand this approach theoretically preserves the privacy against arbitrary adversaries, on the other hand, differential privacy has vulnerabilities in the case of correlated MG power data [21], [22]. Furthermore, [23] have also proven that a differential private solution is vulnerable to tracker attacks.

This work identifies privacy attacks that would affect the dependability and security of the MG network. We postulate that privacy leaks can be maliciously exploited for energy theft or discourage use of the network by internal users. By inference about household appliance usage patterns as a subgoal towards the goal of undetected energy data modification (energy theft), we extend the attack tree for energy theft proposed by Jiang *et al.* [24].

III. System Model and Security Requirements

Our MG system model is comprised of three components namely, the power network model, the communications networks Model, and the MG users. MG user include energy consumers, producers, and a super user or a utility company. The power network includes a group of distributed generators supported by renewable energy generation sources such as solar power.

In the power network, micro-generation emanating from a subset or all of the users is connected to the distribution network. However, due to the volatility of renewable energy, the amount of energy generated does not match the power demand on the grid at all times.

To manage demand effectively, the MG is supported by a communication network. The communication network enables power consumption/production data collection and monitoring. We structure the MG communication network as a three-tiered hierarchy comprised of a household, neighborhood, and back-haul network.

- **Household network**: The Household network is located on the user's premises and is comprised of a network of sensors where each sensor is connected to an electrical appliance in the household. All of the sensors are tied directly to a household power consumption data aggregation device via a wireless sensor network. For simplicity, throughout the rest of the paper, we will consider that the power consumption data aggregation device is a mobile device (e.g., a mobile phone). The wireless network communication is handled by short range low-cost protocols such as Bluetooth, and ZigBee. Reasons for using a wireless network are centered on cost minimization.
- **Neighborhood Network**: We presume that every household belongs to a cluster that is linked to a data concentrator node such as a smart meter. As such, every household mobile device, reports the aggregated energy consumption of the household to the data concentrator node to which it is linked. The goal of doing this is to drop the cost of installing a data concentration node at every household. A further advantage is that this minimizes the risk of privacy de-anonymization attacks. Every mobile device periodically reports the household's power consumption to the data concentrator and the data concentrators are densely interconnected via a mesh network in order to minimize the risk of lost data.
- **Back-haul Network**: Finally, we employ a back-haul network to handle the transfer of the power consumption data from the aggregation points to some data center for billing purposes.

Besides the power and communication network, we have the grid's actors. MG users can fall into either one of or all of the following three categories, namely consumers, producers, and trading operators.

- Users (consumers) are private entities that consume electrical power. The user can be represented as a household with appliances. The household may also produce energy. In that case, it uses a certain amount of its generation for itself and sell the excess unconsumed energy produced to the network. Users needing additional energy to satisfy their demand cover their energy needs by bidding for the required energy amounts over short time intervals.
- Grid operator (GO) or utility is an entity that owns a part of the generation in the distribution network. It can

be, for example, a community-based Non-Governmental Organization (NGO).

- Energy Trading Operator (ETO) is a third party that facilitates the efficient exchange of energy. It buys energy from producer and utility and sells it to the consumer. It drives the energy market by auctioning energy and allowing users to bid for electricity.

A market model for micro-grid can be classified as centralized or distributed. In a central scenario, a supplier (ETO) buys energy from producers and sells in advance into the retails market based on short terms prediction of energy production, e.g. based on the weather forecast. This requires analytic services and a sufficiently large collection of data. The ETO is interested in making some profit, so its primary concern is not consumer interest. A distributed case is an open market where renewable energy producer and consumers participate in the local markets and trade energy over short time intervals [25], [26] i.e. energy producer auctioning and consumer bidding for electricity. We term this a peer to peer market. In this paper, we consider the central scenario with an ETO.

A. Security Requirements

The major properties of a resilient MG network are dependability and security. Dependability encompasses reliability, safety and maintainability [27] and security goals include availability, integrity, confidentiality and privacy [24] [28][29].

- Confidentiality implies that sensitive information should only be accessed by authorized entities.
- Integrity: data transmitted must be correct without any unauthorized manipulation
- Availability: data should be accessible by authorized entities whenever they need the data.
- Privacy: the entities cannot infer any private information from the shared energy data

Security threats within the MG network attempt to compromise one or more security services. Attacks affecting the security goals of the MG include passive and active attacks. In a passive attack, the attacker passively observes ongoing communication and does not send any messages. Examples of passive attacks include eavesdropping attacks. While in an active attack the attacker modifies the communication by injecting the packets in the network. Examples of active attacks include replay attacks, message modification attacks and Denial of Service (DoS) attacks [29].

IV. Privacy Threat Model

In this section, we present an overview of the privacy threat model in MG. In particular, we focus on privacy violations that are geared at provoking energy theft and economic incentives rather than on ones aimed at destroying the network. The reason for focusing on these two aspects is that the user participation in the grid is conditional on the trust the users have in the grid's reliability. Events that result in energy consumption misreports or theft impact negatively on user trust. To this end, we consider two main privacy violation attacks from e-health and online social networks, namely inference and data aggregation attacks [30], [31]. Inference attacks use data collected (even maliciously) to infer information about the users and data aggregation attacks use the access to the data sets to deduce some protected information. Inference and aggregation attacks are of particular interest for a constrained MG because such attacks can be provoked even when the attacker possess inaccurate and incomplete information [31].

In the following, we begin by presenting a running example to contextualize the attack scenario and then proceed to offer attack models for both the inferential and aggregation cases of privacy violations.

A. Running Example

We consider a smart micro-grid environment comprising two households namely, **A** and **B**. Both households at a given time collect their aggregated energy consumption to two separate sink nodes. For simplicity, we denote these as, Mobile **A** and Mobile **B**. In addition, we suppose that both households are within proximity of each other so Household **A** could easily also reports consumption to Mobile **B** instead of to Mobile **A**. Fig.1 depicts the scenario described above.

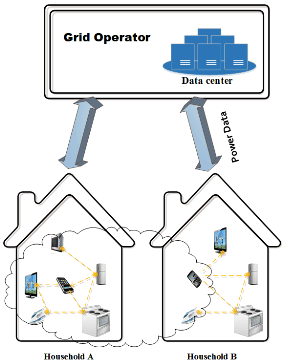

Figure 1. Micro-grid: Communication Network

We consider that the communication medium within the household is wireless. The wireless transmission range from **A**'s house overlaps with **B**'s house network. Because wireless communication propagates over radio signals, any network node within radio range can capture the signal. This means that when a snapshot of appliance power consumption from **A**'s household is transmitted to the Mobile **A**, Mobile **B** could eavesdrop on communications to obtain a subset of energy consumption data from **A**'s household.

B. Inference Attack Model

An inferential attack occurs in the context described in Fig.1 when a malicious neighboring user, say **B**, gain information from the network traffic in the overlapping area. It then proceeds by analyzing that information to deduce unauthorized details about the presence and behavior of the users in **A**'s household. We consider two cases of inferential attacks namely, direct and indirect inferential attacks.

1) Direct inferential attack (DIA): is the most simple form of attack. DIA uses energy data directly accessed, together with basic observation to deduce some private information. DIA attacker is a malicious neighbor, which is considered weak but ingenious and requires minimum or no computation to deduce the information required [32]. An example of DIA in MG network is a Presence Privacy Attack (PPA). PPA developed by Li *et al.* [33] relies on the concept of dependence between the temporal component of the energy time series consumption data and the household activities.

PPA can be provoked as follows: let consider the running example described and depicted in Fig.1. The vector of power readings from **A**'s household is $V_A = X_1, ..., X_d$ of size d and that a sub-vector, say $V_{As} = X_j ... X_d$ with $X_j ... X_d \subset X_1, ..., X_d$ gets reported to Mobile **B**. Now suppose that instead of discarding these values, **B**'s device records them and **B** observes that in **A**'s household, several key devices are not on. **B** then proceeds to look out of the window and notes that the lights in the household are turned on. By further observation, **B** also notices that the car has been away for three days. So, he deduces that **A** is away and that the lights have been turned on simply to give the impression of household presence.

2) Indirect Inferential Attacks (IIA): rely on the fact that the attacker (malicious neighbor user) can analyze energy time series data to infer private information including household consumption, user behaviors and lifestyle [9]. IIA builds on the direct inferential attacks by expanding the sphere of knowledge of the attacker.

To provoke the attack the adversary, say **B**, proceeds by collecting different versions of the aggregation vector V over a period T. We consider in this case that n readings are recorded at various times within the period T. By statistical correlation, the attacker **B** can then proceed to make accurate deductions about the behavior in **A**'s household.

In order to illustrate how the IIA happens, consider our running example depicted in Fig.1. The adversary says **B** compromises a portion of **A**'s household network traffic and obtains the consumption vector V_{As} in transit. This is possible because **B**'s household is close to **A**'s household and have overlapping radio range. So an eavesdropping attack is possible for data acquisition [28]. **B** collects **A** data over some time. Once data are collected **B** deduces what appliance was on by using a mathematical function of appliance load model described in [34]. So **B** uses it to deduce what appliance was used and when. By further observation, **B** also notices that the appliance or set of appliances Y is repeatedly turned on at time W. In this way by gathering and analyzing data over a certain amount of time. For example, assuming that **B** gathers **A**'s household data over a week, he may accurately discriminate between classes of devices [35]. Then **B** can draw conclusions e.g. on the suitable time to launch a targeted data modification attack. The attack happens as a consequence of knowledge accumulated over time and data statistically manipulated.

C. Aggregation Attacks

Information aggregation attacks require the adversaries to use information retrieval and data mining techniques to collect small pieces of private information that pertain to the same targeted user from a single or several disparate databases Sources of the data can include social networks, public records, water grids, etc.

In order to provoke aggregation attacks, we consider that the aggregated energy consumption data from each household at a given interval is collected and stored at the Grid operator control centers. To this end, from the communication network architecture described in Fig.1, we consider direct exchanges between the household network via a mobile device and the grid operator. The MG network comprises n households which consume energy, a grid operator (GO) and an ETO that is running the central MG energy market.

To protect consumers' privacy, we consider that anonymous household energy consumption data –i.e. explicit household identifiers– are removed and replaced by a pseudonym, are transmitted to the GO intermittently. We also consider a set of n households where the stream of time series data, which is the consumption of a household say $i, (1 \leq i \leq n)$, represented by $V_i = X_1, X_2, ..., X_p$, V_i is continuously received from household and transmitted to the GO at sliding windows. GO stores the data from the set of n households into a time series database Db at GO's server for billing. $Db = \{V_i : i \in [1, n]\}$ contains an unordered set of n sub-sequence of time series possibly of different lengths. Db is a dynamic data set as a new stream of data continuously arrive at regular time interval.

We also assume that the ETO is honest-but-curious. That is to say, the ETO will execute the protocol as specified but is also curious and will use knowledge of anonymous information received for privacy violation.

Information aggregation attack has been define in papers [30], [14]. In similar ways, in this paper, two main attacks are considered for the information aggregation scenario in a MG particularly in data set and cross-data set aggregation.

1) In database aggregation: Takes place when records belonging to the same entity (household), can be identified when access to the protected data set. In the case of a dynamic data set such as the stream of time series shared in the MG network, it corresponds to associations among the different streams of data originating from the same household collected at different intervals of time [36].

An instantiation of in database aggregation attack consists of an adversary finding the correlation between different time series streams V_i originating from the same household, with the aim of re-identifying the considered household say, **i**. The adversary proceeds by analyzing the data collected at different time windows T to find common patterns or trends.

In order to explain how this attack happens, we consider a MG system with three participants: ETO (consider for simplicity that the entity playing the role of ETO and GO is the same), households **A** and **B**. At a given time period T, The GO collects a stream time series V_A and V_B from household **A** and **B**. V_A and V_B are stored on a data set *Db*. Table I presents *Db* consisting of V_A and V_B at two periods.

Table I
TABULAR REPRESENTATION OF *Db*

	Period of time	Consumption vector
1	1	V_1
2	1	V_2
3	2	V_3
4	2	V_4

The ETO has access to *Db* illustrated in Table I. ETO is aiming to re-identify a household, say **A** from the anonymized time series database *Db*. ETO applies standard techniques for pattern discovery (or 'motif discovery') on $V_i, i \in [1,4]$. ETO compares V_i and V_j, $i, j \in [1,4]$ with $i \neq j$. ETO executes queries to find similarities on the subsequence of data (see method proposed in [37]) and identify the correlated pattern. By doing so, ETO can retrieve all the subsequence in the data base that are similar or belonging to the household **A**. This results from the fact that stream time series data belonging to the same household say, **A** are correlated and uniquely identifiable [10]. Finally, if the ETO possesses further information, for example on **A**'s household behavioral patterns, ETO can easily deduce to which household the time series belong and hence depseudonymize the data set. This is particularly easy in a MG with a small sized data set.

2) Cross Database Aggregation: Private information from the targeted user across two or more data sets are retrieved and aggregated by the attacker. The attack arises because the attackers have access to many different data set from different heterogeneous sources, sometimes with a different level of protection. For instance, data sources can originate from electricity, water, gas, telephone, online social network or public records. The attack is carried out by aggregating and cross-linking data from multiple data sets about the same targeted entity an then compiles the correlated information from the target household. The intersection of data from different sources may disclose some previously protected data.

To provoke such an attack, an attacker uses information retrieval techniques to find the bridges between the different databases. The attacker then aggregates the data from the different databases to deduce private information from a specific household say, **A**. Note that we are assuming here that the attacker is authorized to access multiple databases.

V. IMPACTS OF PRIVACY ATTACKS IN MICRO-GRIDS

As mentioned before, the primary concern is that undetectable data modification attacks can be provoked to facilitate misreporting of household consumption. This not only creates a situation of distrust but may also lead to unbalanced demand and supply, thus, affecting the stability of the MG operation.

A. Electricity Theft

Energy theft occurs when the attacker steals electricity from a neighbor and misreports consumption, with the incentive of monetary gain. Energy theft results in a higher bill for the targeted household. Let V_A and V_B be the consumption of household **A** and **B** at a given time window T. The attacker, say **B** compromises an arbitrary number of sensor meters from **A**'s household (i.e., a captured sensor node that has been reprogrammed by the attacker). In this way it creates a slight variation in the appliance sensor's reading and obtains a modified consumption report $V_{\tilde{A}}$, with $V_{\tilde{A}} > V_A$. In the meantime the attacker misreports his consumption by under estimating some of its appliance's sensor measurements and obtains $V_{\tilde{B}} = V_B - (V_{\tilde{A}} - V_A)$. In practice, this knowledge can be obtained by the inferential privacy attacks described in Section IV-B. As this attack helps to create a profile of the household appliances usage patterns of the targeted household. The malicious user say, **B**, utilizes the knowledge he gains about appliance load profile and time when **A**'s household used them. To infer the appropriate time either to corrupt a few measurements as possible or to corrupt the magnitude of the measurement [32]. Inferential attacks help to modify data at the level of an appliance in such a way that the resulting consumption data looks similar to normal consumption. The model of such attacks are similar to some extend to the false data injection attacks [38] and a relaxed version proposed by Sandberg *et al.* [39].

B. Unstable Micro-grid Operation

Fair competition is expected on the energy market at the condition that the set of consumer's households (participants) obtained information about loads and the dynamic energy price structure. Participation in the MG energy market is conditional on the knowledge of dynamic energy price. Household energy consumption patterns help the energy supplier (ETO) to approximate present and future demand. The energy supplier (ETO) may take advantage of such a privacy violation to classify consumers. For marketing reasons, ETO would like to discriminate between households by transmitting market data to a certain group of high consumers and not transmitting to the group of lower consumers. To illustrate the above problem in our considered MG with ETO and two households **A** and **B**. Privacy violation may provide ETO with the identity of either household **A** or **B** and the consumption patterns and behaviors. Knowing the average demand of **A**'s household. ETO can discourage **A** from bidding when the prices are low by either delaying/not sending the message with the prices signal to **A** or having various prices across multiple households in order to make more profit. This is equivalent to a denial of service attack and creates an unfair commercial practice during the period of low generation. Moreover, such a practice leads to a large portion of households not trusting the system. Loss of trust can discourage consumers from using the power grid, leading to unbalanced demand and supply as they will be less demand and a large part of production will not be used. This may result in unstable MG operation.

VI. Conclusions

In this paper, we presented two categories of privacy threats that arise from data sharing in MG. An inferential attack was presented to illustrate the difficulty of securing communication in a household network with low powered processing capacity and limited bandwidth. We described both inferential and aggregation attacks with an illustration for a small MG. We considered privacy breaches that lead to distrust between the consumer and the supplier. This as a consequence can discourage consumers from using the power grid and may lead to the destabilization of the power grid. It is, therefore, important to come up with ways of assuring privacy protection to ensure a successful MG operation.

Acknowledgments

This work was partially supported by the joint SANCOOP Programme of the Research Council of Norway and the National Research Foundation of South Africa (NRF) under the NRF grant 237817 as well as the Hasso-Plattner-Institut. The authors gratefully acknowledge the anonymous review comments for helping improve the presentation of the paper.

References

[1] (IEA), "World energy outlook 2013," *OECD/IEA*, 2013.

[2] ——, "Technology roadmap smart grids," Paris, 2011.

[3] S. Chowdhury and P. Crossley, *Microgrids and Active Distribution Networks*, ser. IET renewable energy series. Institution of Engineering and Technology, 2009.

[4] A. Llaria, O. Curea, J. Jiménez, and H. Camblong, "Survey on microgrids: Unplanned islanding and related inverter control techniques," *Renewable Energy*, vol. 36, no. 8, pp. 2052 – 2061, 2011.

[5] F. Eichinger, D. Pathmaperuma, H. Vogt, and E. Müller, "Data Analysis Challenges in the Future Energy Domain," in *Computational Intelligent Data Analysis for Sustainable Development*, ser. Data Mining and Knowledge Discovery Series, T. Yu, N. Chawla, and S. Simoff, Eds. Chapman and Hall/CRC, 2013, ch. 7, pp. 181–242.

[6] L. Yang, H. Xue, and F. Li, "Privacy-preserving data sharing in smart grid systems," in *Smart Grid Commun. (SmartGridComm), 2014 IEEE Int. Conf. on*, Nov 2014, pp. 878–883.

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

[8] H. Khurana, M. Hadley, N. Lu, and D. Frincke, "Smart-grid security issues," *Security Privacy, IEEE*, vol. 8, no. 1, pp. 81–85, Jan 2010.

[9] M. Lisovich, D. Mulligan, and S. Wicker, "Inferring personal information from demand-response systems," *Security Privacy, IEEE*, vol. 8, no. 1, pp. 11–20, Jan 2010.

[10] E. Buchmann, K. Böhm, T. Burghardt, and S. Kessler, "Re-identification of smart meter data," *Personal Ubiquitous Comput.*, vol. 17, no. 4, pp. 653–662, Apr. 2013.

[11] N. I. of Standards and Technology, "Guidelines for smart grid cyber security: Vol.2,privacy and the smart grid," http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf, National Institute of Standards and Technology Interagency Report 7628, Tech. Rep., August 2010.

[12] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Smart Grid Commun.(SmartGridComm), 2010 1st IEEE Int.Conf.on*, Oct 2010, pp. 238–243.

[13] M. Jawurek, M. Johns, and K. Rieck, "Smart metering de-pseudonymization," in *Proc. of the 27th Annu. Comput. Security Applications Conf.*, ser. ACSAC '11. New York, NY, USA: ACM, 2011, pp. 227–236.

[14] L. SWEENEY, "k-anonymity: A model for protecting privacy," *Int.Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[15] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Discov. Data*, vol. 1, no. 1, Mar. 2007. [Online]. Available: http://doi.acm.org/10.1145/1217299.1217302

[16] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *Data Engineering, 2007. ICDE 2007. IEEE 23rd Int. Conf. on*, April 2007, pp. 106–115.

[17] S. Kessler, E. Buchmann, T. Burghardt, and K. Böhm, "Pattern-sensitive time-series anonymization and its application to energy-consumption data," *Open Journal of Inform. Systems (OJIS)*, vol. 1, no. 1, pp. 3–22, 2014.

[18] E. Shi, T.-H. H. Chan, E. G. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *NDSS*, 2011.

[19] G. Ács and C. Castelluccia, "I have a dream! (differentially private smart metering)," in *Inform. Hiding*, ser. Lecture Notes in Comput. Sci. Springer Berlin Heidelberg, 2011, vol. 6958, pp. 118–132.

[20] P. Barbosa, A. Brito, H. Almeida, and S. Clauß, "Lightweight privacy for smart metering data by adding noise," in *Proc. of the 29th Annu. ACM Symp. on Appl. Computing*, ser. SAC '14. New York, NY, USA: ACM, 2014, pp. 531–538.

[21] D. Kifer and A. Machanavajjhala, "No free lunch in data privacy," in *Proc. of the 2011 ACM SIGMOD Int.Conf.on Management of Data*, ser. SIGMOD '11. New York, NY, USA: ACM, 2011, pp. 193–204.

[22] B. Yang, I. Sato, and H. Nakagawa, "Bayesian differential privacy on correlated data," in *Proc. of the 2015 ACM SIGMOD Int.Conf.on Management of Data*, ser. SIGMOD '15. New York, NY, USA: ACM, 2015, pp. 747–762.

[23] R. Sarathy and K. Muralidhar, "Some additional insights on applying differential privacy for numeric data," in *Proc. of the 2010 Int. Conf.on Privacy in Statistical Databases*, ser. PSD'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 210–219.

[24] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. S. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Sci. and Technology*, vol. 19, no. 2, pp. 105–120, April 2014.

[25] E. Buchmann, S. Kessler, P. Jochem, and K. Bohm, "The costs of privacy in local energy markets," in *Business Informatics (CBI), 2013 IEEE 15th Conf.on*, July 2013, pp. 198–207.

[26] S. Kessler, C. Flath, and K. Böhm, "Allocative and strategic effects of privacy enhancement in smart grids," *Inf. Syst.*, vol. 53, no. C, pp. 170–181, Oct. 2015.

[27] A. S. Tanenbaum and M. Van Steen, *Distributed Systems: Principles and Paradigms*. Prentice-Hall, 2006.

[28] E. Shi and A. Perrig, "Designing secure sensor networks," *Wireless Communications, IEEE*, vol. 11, no. 6, pp. 38–43, Dec 2004.

[29] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *Commun. Surveys Tutorials, IEEE*, vol. 16, no. 4, pp. 1933–1954, Fourthquarter 2014.

[30] B. Luo and D. Lee, "On protecting private information in social networks: A proposal," in *Data Engineering, 2009. ICDE '09. IEEE 25th Int. Conf. on*, March 2009, pp. 1603–1606.

[31] F. Li, J. Y. Chen, X. Zou, and P. Liu, "New privacy threats in healthcare informatics: When medical records join the web," in *9th Int. Workshop on Data Mining in Bioinformatics*, Washington D.C., 07/2010 2010.

[32] L. Yang and F. Li, "Detecting false data injection in smart grid in-network aggregation," in *Smart Grid Commun.(SmartGridComm), 2013 IEEE Int. Conf. on*, Oct 2013, pp. 408–413.

[33] H. Li, S. Gong, L. Lai, Z. Han, R. Qiu, and D. Yang, "Efficient and secure wireless communications for advanced metering infrastructure in smart grids," *Smart Grid, IEEE Trans. on*, vol. 3, no. 3, pp. 1540–1551, Sept 2012.

[34] P. Ambassa, A. Kayem, S. Wolthusen, and C. Meinel, "Robust snapshot algorithm for power consumption monitoring in computationally constrained micro-grids," in *IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA)*, Nov 2015, (In Press).

[35] J. Lines, A. Bagnall, P. Caiger-Smith, and S. Anderson, "Classification of household devices by electricity usage profiles," in *Proc. of the 12th Int. Conf. on Intelligent Data Engineering and Automated Learning*, ser. IDEAL'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 403–412.

[36] V. Ashby, S. Jajodia, G. Smith, S. Wisseman, and D. Wichers, "Inference and aggregation issues in secure database management systems," Tech. Rep. 005 (Volume 1/5, Nat. Comput. Security Center, Tech. Rep., 1996.

[37] S. Yingchareonthawornchai, H. Sivaraks, T. Rakthanmanon, and C. Ratanamahatana, "Efficient proper length time series motif discovery," in *Data Mining (ICDM), 2013 IEEE 13th Int. Conf. on*, Dec 2013, pp. 1265–1270.

[38] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. of the 16th ACM Conf. on Comput. and Commun. Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 21–32.

[39] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Preprints of the 1st Workshop on Secure Control Systems, CPSWEEK 2010, Stockholm, Sweden*, 2010, qC 20120206.