An Efficient Privacy-Preserving Algorithm based on Randomized Response in IoT-based Smart Grid

Hui Cao
Computer School
Wuhan University
Wuhan, China
2013102110071@whu.edu.cn

Shubo Liu
Computer School
Wuhan University
Wuhan, China
liu.shubo@163.com

Zhitao Guan
School of Control and Computer Engineering
North China Electric Power University
Beijing, China
guan@ncepu.edu.cn

Longfei Wu
Department of Mathematics & Computer Science
Fayetteville State University
Fayetteville, NC, USA
lwu@uncfsu.edu

Haonan Deng
Computer School Wuhan University
Wuhan, China
State Grid Jibei Electric Power Company
Beijing, China
dhnzzz@126.com

Xiaojiang Du
Department of Computer and Information Sciences
Temple University
Philadelphia, PA, USA
xjdu@temple.edu

Abstract—**In this paper, we propose a new randomized response algorithm that can achieve differential-privacy and utility guarantees for consumer's behaviors, and process a batch of data at each time. Firstly, differing from traditional differential private approaches, we add randomized response noise into the behavior signatures matrix to achieve an acceptable utility-privacy tradeoff. Secondly, a behavior signature modeling method based on sparse coding is proposed. After some lightweight trainings using the energy consumption data, the dictionary will be associated with the behavior characteristics of the electric appliances. At last, through the experimental results verification, we find that our Algorithm can preserve consumer's privacy without comprising utility.**

Keywords—Differential Privacy; Randomized Response; Sparse Coding; IoT; Smart Grid

I. INTRODUCTION

Differential privacy [1-5] constitutes a strong standard for privacy guarantees in statistical databases. Due to its property of rigid and provable privacy guarantee, differentially private database mechanisms can make confidential data widely available for accurate data analysis and data statistics [2]. A recent privacy-preserving crowdsourcing mechanism, Randomized Aggregable Privacy-Preserving Ordinal Response (RAPPOR) [6], is proposed in 2014, which has substantially improved the statistical crowdsourcing technology. Since then, RAPPOR has been adopted and enhanced by many researchers to generate specialized Randomized Response algorithms that can be used in specific fields, such as machine learning [7-11].

RAPPOR may be used to solve the problem of privacy protection in smart grid which shares some similarity with the crowdsourcing environment. As the next-generation power system, smart grid is a special Internet of things system that envisioned to provide efficient and reliable energy delivery [12]. To realize fine-grained optimization and real-time management for energy supply, numerous smart meters are installed at the consumers' home to gather the energy consumption data at high frequency[13]. However, these detailed data usually include privacy-sensitive information with regard to the consumer's application consumption patterns, which raises the consumer's behavior privacy concerns [14].

Actually, there are numerous works contributing on the privacy preservation in smart grid[15-17], but it has some limitations. Existing differential privacy schemes in smart grid mainly focus on the individual energy consumption data [18-19] and adding noise into the energy consumption data is the common solution to provide differential privacy. Nevertheless, the obfuscated data may affect the data-utility and have a bad impact on several services such as electricity billing in smart grid.

RAPPOR provides strong privacy, efficient, and high-utility guarantees for each client string in data crowdsourcing. It is an intuitive idea to apply RAPPOR for differential privacy. However, in this case, both Basic RAPPOR or One time RAPPOR need to use Bloom filter that can hash a string or very few bits each one time. In consideration of massive batches of data, there are difficult to address, potentially causing surveyors to adopt the less effective privacy protections [8].

In the IoT and fog computing environment, the terminal devices often need to process data by batch. Although RAPPOR is a good machine of differential privacy, it is hard to process data in such volume.

In this paper, we propose an improved randomized response algorithm that could protect consumer's privacy from behavior signatures and our contributions are summarized as follows:

(1) The proposed algorithm is applicable for privacy protection of IoT. Differing from traditional differential private approaches, we add randomized response noise into the behavior signatures matrix to achieve an acceptable utility-privacy tradeoff.

(2) We propose a behavior signature modeling method based on sparse coding instead of boom filter. After some lightweight trainings using the energy consumption data, the dictionary will be associated with the behavior characteristics of the electric appliances.

(3) At last, the performance of our scheme is compared with the state of the arts. The experimental results show that our algorithm can achieve a good balance between data-utility and privacy, hence is better applicable to IoT applications.

The rest of this paper is organized as follows. Section II introduces the related work and background. In section III, our algorithm is presented in detail. In section IV, the performance of our scheme is evaluated. In section V, the paper is concluded.

II. RELATED WORK

A. Differential privacy

Dwork [1] has proposed the notion of differential privacy for privacy-preserving in statistical datasets. In addition, he has also proposed how to realize differential privacy by noise addition [20-21]. Differential privacy in smart grid has been discussed in [18-19], and the fault-tolerance problem during data aggregation has been analyzed in [22]. Barbosa [23] first-ly applied differential privacy against NILM (Non-Intrusive Load Monitoring) to protect the data collected by smart meters.

1) Definition of differential privacy

M is a privacy mechanism. For any datasets D_1 and D_2, differing from at most one element, M satisfies ε -differential privacy if the two datasets satisfy the following condition:

$$P_r\{M(D_1) \subseteq S\} \le e^\varepsilon \times P_r\{M(D_2) \subseteq S\}$$

S represents the range of $M(D_i)$. The smaller the value of ε is, the higher the degree of privacy preservation can be achieved.

2) Property2: Stable Transformations [21]

For any two databases E and F, we say T provides c-stable if it meets the following condition.

$$|T(E) \oplus T(F)| \le c \times |E \oplus F| \tag{1}$$

If the privacy preserving mechanism M provides ε - differential privacy and T is a c-stable transformation, the combination of $M \times T$ provides $(\varepsilon \times c)$ differential privacy.

B. Randomized responses

Erlingsson[6] proposed RAPPOR as a differential privacy machine, and answered how to recover distributional parameters from the responses. The consideration of several bits joint-ly, had to wait for a subsequent operation, Fanti[7] proposed an improved Algorithm to deal with several bits jointly. Vinterbo[8] extended RAPPOR to as n-dimensional

RAPPOR performs the following steps: Firstly, hash client's value onto the Bloom filter.

Then let

$$x_i^{'} = \begin{cases} 1, with probability\ \dfrac{1}{2}f \\ 0, with probability\ \dfrac{1}{2}f \\ x_i, with probability\ 1-f \end{cases}$$

x_i represents the original energy consumption data.

$x_i^{'}$ represents the data after being obfuscated by RAPPOR.

C. Sparse Coding

Sparse coding is a kind of method for learning sets of over-complete bases to represent data efficiently. It has multi-ple variances such as hierarchical sparse coding [24], non-negative sparse coding [25] and has been applied in many fields like NILM, audio classification [26] and source separation [27]. In the field of smart grid, Kolter [24] extended the sparse coding to improve the accuracy of a large-scale energy disaggregation task and Elhamifar's [27] designed a method based on sparse coding to extract signature consumption pattern. Jenatton [28] proposed an optimal method for the regularization of hierarchical sparse coding. Singh [29] proposed a greedy deep sparse coding for energy disaggregation.

The aim of sparse coding is to find dictionary $B_i \in R^{t \times n}$ such that the input vector x_i can be represented as a linear combination of n basis functions as follows.

$$x_i \approx B_i A_i$$

Here, B_i denotes the dictionary and the number of basis function n is larger than the dimensionality of data x_i. The activation matrix $A_i \in R^{n \times 1}$ is sparse, which means the sets of activations contain mostly zero entries. The sparse coding cost function is defined as follows.

$$\min_{A_i \ge 0, B_i \ge 0} \| x - B_i A_i \|_F^2 + \lambda \sum_{p,q} (A_i)_{pq}$$

$\| Y \|_F$ represents the Frobenius norm of Y and the value of F is always set to two in sparse coding. C represents a constant. B_i^j denotes the jth column of matrix B_i. For a dataset $\hat{X}$ composed of v elements, the sparse coding can be shown as follows. λ denotes the weight of sparsity.

$$A_{1:v} = \arg \min_{A_{1:v} \ge 0} \left\| \hat{X} - [B_1...B_v] \begin{bmatrix} A_1 \\ ... \\ A_v \end{bmatrix} \right\|_F^2 + \lambda \sum_{i,p,q} (A_i)_{p,q}$$

III. FRAMEWORK AND ALGORITHM

A. Design Goal

In general, as shown in Figure 1, the objective of the attacker is to infer household activity from the power consumption data.

Specifically, the attack model is

(1) With the total energy consumption of all consumers in a region at a certain time, inferring the consumption of a certain consumer.

(2) With the total energy consumption of a consumer over a period of time, inferring the behavior of that consumer.

Inherited from Barbosa's [23] design goals, our schemes focus on the following aspects:

(1) Enabling the calculation of the total consumption of a consumer over a period of time (e.g., monthly billing);

(2) Enabling the calculation of the total consumption of all consumers in a region at a certain instant of time;

(3) Avoiding the measurement of the instantaneous consumption of an individual consumer at a certain instant of time.

Besides, we also propose two new design goals.

(4) Providing ε-differential privacy without generating a serious impact on the data-utility.

(5) The obfuscated data should not be far from the original data in case that the adversary removes the noise to get the real data.
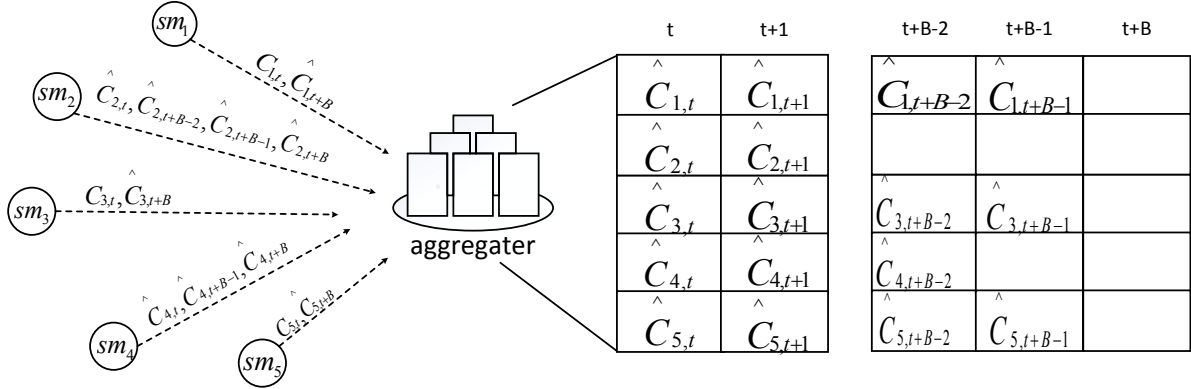
(a) attack model I from [30]
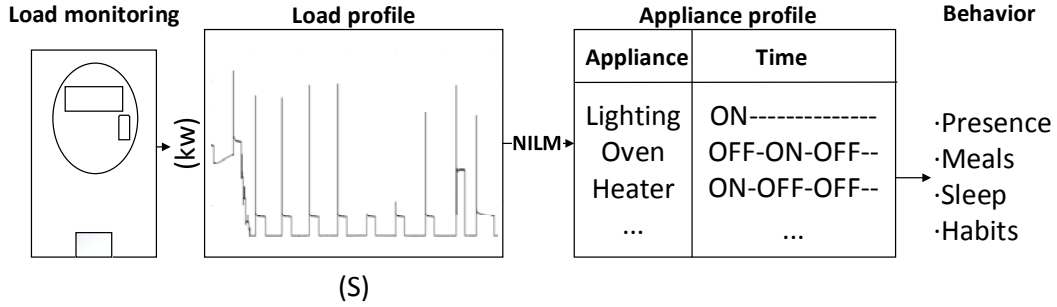
(b) attack model II from [31]

Figure.1. As shown in (a), for some consumers in a region at a certain instant of time, the adversary may learn a certain consumer's consumption data and then infer the consumer's behaviors and habits. As shown in (b), for a consumer over a period of time, the adversary may learn the switch states of each appliance by NILM and then infer the consumer's behaviors and habits.

B. System Framework

As shown in figure.2, the algorithm takes in the real energy consumption data, and performs the following steps:

(1) Train the dictionaries (basis functions)

This step can be complete by a trusted fog using historical data as the training set. If the electric utility data is trusted by customers, the dictionaries can be trained from electric utility data that are sent to the fog. Although the cost of training may be time-consuming, this work does not need to be carried out repeatedly, and it can be completed at the more powerful fog layer.

(2) Sparse coding

This step can be completed by the trusted fog regularly (e.g., 15 minutes), along with the data collected from the smart meter.

(3) Randomized response

This step can be completed by the trusted fog.

(4) Data re-aggregation.

This step can be completed by the trusted fog.

(5) Report. Send the generated report S to the server.

This step can be completed by the trusted fog. An end-to-end connection between the smart meter and the utility that could send noisy data.

C. Sparse coding

The energy consumption data $Y_{1 \times t}$ can be disaggregated by sparse coding as follows:

$$Y'_{t \times 1} = B_{t \times n} A_{n \times 1} \approx Y_{t \times 1} \qquad (2)$$

Here, t denotes the amount of time slots, which is one deal in whole date set. n is the number of basic functions b, which is larger than t. The dictionary $B_{t \times n} = [b_1 \ldots b_n]$ is related to the energy consumption dynamics corresponding to the different operation modes of a device. $A_{n \times 1}$ is the activation matrix.

Dictionaries are the critical factor to sparse coding. In IoT, efficient dictionary should be associated with the energy consumption data, Switch state of the appliance and the behavior signature. The switch state of an appliance is the appliance consumption patterns (ON/OFF) of a particular consumer [25]. The privacy-preserving requirement is that the application consumption patterns should not reflect a particular consumer's behavior at home, such as presence or absence, sleep-wake-cycles and other personal behaviors.

To achieve the desired goal using sparse coding, two important conditions must be satisfied:

- The combining error must small.

$$B_{t\times n}A_{n\times 1} - Y_{t\times 1} \to 0$$

- The Activations matrix $A_{n\times 1}$ is sparse

$$A_{n\times 1} = \{a_1, a_2, \ldots, a_i\}$$

Element a_i should be as close to 0 as possible.

It's obvious that the random initial dictionary B is far away from this goal, hence a continuous optimization process is required.
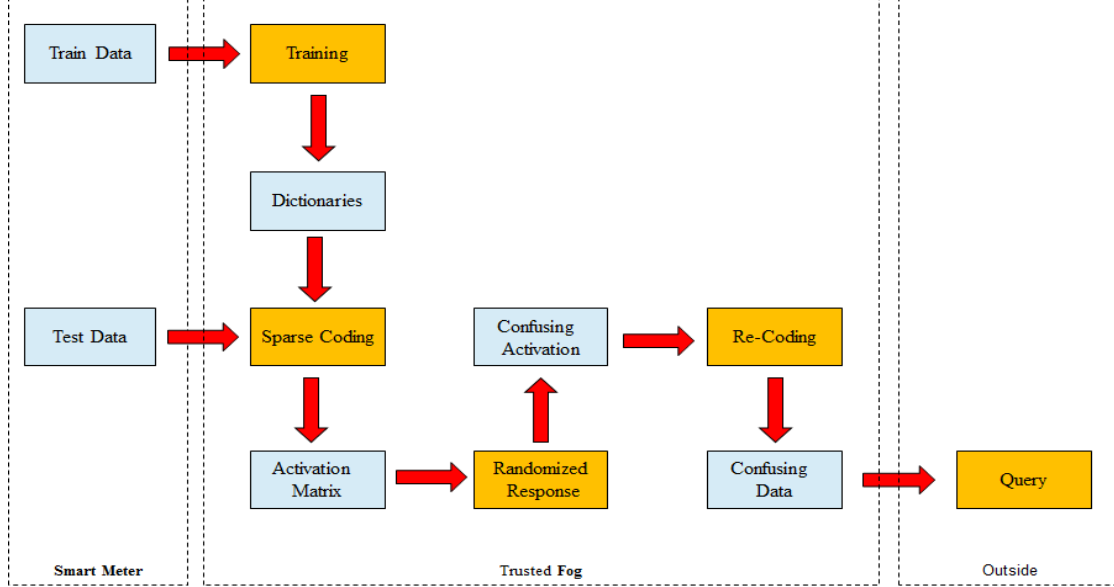

Figure.2. The process of our algorithm, training data, testing data and obfuscated data are represented by pale blue. The data processing like supervised learning, modified sparse coding, noise addition and data re-aggregation is represented by orange. Basic functions (dictionaries), aggregated activations and obfuscated activations belong to the intermediate data. Firstly, we train the basic functions based on supervised learning. Then, we predict the aggregated activations based on modified sparse coding from the testing data. At last, noise is added into activation and we get the obfuscated data by data re-aggregation.

D. Training dictionary

The process of training the dictionary is described as follows:

Firstly, define a suitable objective function with the dictionary B and activation A. Then, the objective function iterates, which solidifies and improves the dictionary B and activation A alternatively (solidifies the activation A and improves dictionary B, then solidifies the dictionary B and improve activation A). This process is repeated until convergence, in which dictionary B is appropriate.

The objective function is defined as follows.

$$\| Y_{t\times 1} - B_{t\times n}A_{n\times 1} \|_2^2 + \lambda f(A_{n\times 1}) \qquad (3)$$

Here, $\| Y \|_F$ represents the Frobenius norm of Y. C represents a constant. B_i^j denotes the *jth* column of matrix B_i. $\hat{X}$ is a dataset composed of v elements. λ denotes the weight of sparsity.

Here, $\| Y_{t\times 1} - B_{t\times n}A_{n\times 1} \|_2^2$ represents the cost of data-reconstruction.

$f(A_{n\times 1})$ is the restrictive condition of activation matrix $A_{n\times 1}$, where $f(A_{n\times 1})$ is a sparsity cost function which penalize a_i for being far from zero. A typical choice is:

$$f(A_{n\times 1}) = \| A_{n\times 1} \|_1 .$$

$\| A_{n\times t} \|_1$ captures the sparsity condition

The objective function based on sparse coding for the aggregated data sampling from v devices can be defined to be

$$\min \left\| Y_{t\times 1} - [b_1 \ldots b_n] \begin{bmatrix} a_1 \\ \ldots \\ a_t \end{bmatrix} \right\|_2^2 + \lambda \sum_{i=1}^{t} \| A \|_1 \qquad (4)$$

Given an energy consumption vector $Y_{t\times 1}$, to generate an acceptable dictionary, we train the dictionary as follows:

Firstly, we give an initial dictionary $\hat{B}_0$. According to the energy consumption profile of each appliance' state, we get vector set $\{b_1, b_2, \ldots b_n\}$. Each vector b_j corresponds to the energy consumption dynamics in a different operation mode of a given device. As shown in figure.3, for example, the energy consumption profiles of the fridge and washer dryer are intermittent and fluctuant even when they are at ON state. Additionally, the energy consumption profiles of a device in different operation models are not linear.

$$\hat{A}_j = \arg\min_{b_i, a_i} \left\| Y - \hat{B}_{i-1}A \right\|_F^2 + \lambda \sum_{j=1}^{t} f(A) \qquad (5)$$

To find the representative basis function, we combine several continuous data segments to serve as the initial dictionary denoted by $\hat{B}_0$

Secondly, we input the initial dictionary $\hat{B}_0$ to estimate the new activations and dictionary until convergence.

$$\hat{B}_j = \arg\min_{b_i, a_i} \left\| Y - B\hat{A}_{j-1} \right\|_F^2 + \lambda \sum_{j=1}^{t} f(A) \qquad (6)$$

$$\text{subject to } \|a_j\|^2 \leq \delta_0 \text{ and } \|Y - BA\| \leq \sigma$$

Here, δ_0 represents the upper bound of ratio 0 in Activation A

We also show the detailed process of dictionary training in **Algorihm1**.

TABLE.1 ALGORIHM OF DICTIONARY TRAINING

Algorithm1. Dictionary Training
Input: , $Y_{TrainDate}$, $\hat{B}_0$, ∂ , β
Sparse coding pre-training:
1 Initialize $\hat{B}_0$ randomly
2 $\hat{A}_0 \leftarrow \{Y_{TrainDate}, \hat{B}_0\}$
Dictionary training:
3. Iterate until convergence
a) $\hat{A}_i \leftarrow \arg\min \left\| Y - \hat{B}_{i-1}A \right\|_F^2 + \lambda_1 \sum_{i=1}^{t} f(A)$
b) $\hat{B}_j \leftarrow \arg\min \left\| Y - B\hat{A}_{j-1} \right\|_F^2 + \lambda_1 \sum_{i=1}^{t} f(A)$
subject to $\|a_j\|^2 \leq \delta_0$ and $\|Y - BA\| \leq \sigma$
Output: B

E. Randomized Response

For each energy consumption data batch Y, sparse coding is used to optimized Dictionary B through training. Then we can get a activations $A = \{a_1, a_2, \ldots a_n\}$,

Let

$$a_k' = \begin{cases} a_1, & \text{with probability } \frac{c_1}{i} f \\ a_2, & \text{with probability } \frac{c_2}{i} f \\ \quad \ldots\ldots \\ a_i, & \text{with probability } \frac{c_j}{i} f \\ a_k, & \text{with probability } 1 - f \end{cases}$$

where f is a user-tunable parameter controlling the level of longitudinal privacy guarantee that related to ε.

F. Data Re-aggregation

Based on the obfuscated activation and dictionary , we can generate the obfuscated energy consumption data Y' as follows:

$$Y' = BA'$$

Since the sparse coding is a linear mapping, the final obfuscated data Y' satisfies ε-differential privacy (proof is in the next section). However, the final obfuscated result may have a bad impact on the data-utility.

IV. PERFORMANCE ANALYSIS

In this section, using the REDD Data Set [32] and the Nilmtk toolkit [33], we measure the performance of our scheme in terms of the level of privacy preservation.

F1-score is an efficient metric to measure the privacy-preserving level, which can be calculated as follows:

$$F1-score = \frac{2 \times \Pr ecision \times \operatorname{Re} call}{\Pr ecision + \text{Recall}}$$

Here, Precision and Recall represent the positive predictive value and the recall sensitivity respectively. When the F1-score goes high, the application usage patterns can be tracked more accurately.

The commonality shares by Barbosa's scheme, Sankar's scheme and our scheme is the obfuscation of energy consumption data via noise addition. However, these schemes preserve consumer's privacy at different levels.

As shown in Table.3, we compare the F1-scores of our scheme with Barbosa [23], Sankar [34] and the classical NILM algorithm (FHMM). From the experiment results, we demonstrate that our scheme's F1-score is lower than the other schemes, which means that it is more difficult to extract the customer's behavior privacy from the noisy energy consumption data in our scheme. Therefore, compared to the other schemes, our scheme has a better privacy-preserving level.

TABLE.3 COMPARISON OF OUR ALGORITHM WITH OTHER TRADITIONAL ALGORITHMS

	Our Algorithm	Sankar's[34] Algorithm	Barbosa's[23] Algorithm	without noise
Fridge	0.53	0.64	0.65	0.65
Light1	0.58	0.65	0.64	0.71
washer dryer	0.44	0.50	0.49	0.54
Light2	0.19	0.23	0.23	0.23

As shown in Table3, we add noise into different schemes to generate the obfuscated data and then calculate the F1-scores of fridge, light, oven and washer dryer using different with FHMM algorithm. The lower F1-scoreamounts to lower precision rate, which means the behavior signatures are harder to extract in our scheme. Thus, by adding noise into the energy consumption signature, our scheme has a better privacy-preserving level.

V. CONCLUSION

In this paper, we proposed a Randomized Response Algorithm using the sparse coding to replace Boom filter. The algorithm can achieve differential privacy on batches of data. The algorithm is able to better fulfill the trade-off between privacy and utility in the fog environment. Therefore, the

appliance consumption patterns can be masked even if the adversary has obtained the near real-time load profile. At last, we analyzed the feasibility of our scheme and compared it with other traditional algorithms in IoT. Our algorithm can also be applied to other fields. In future, we will focus on extending the sparse coding to further preserve user's privacy without compromising the data-utility.

ACKNOWLEDGMENT

REFERENCES

[1] C. Dwork, "Differential Privacy," in the 31th International Colloquium on Automata, Languages and Programming, vol. 4052, pp. 1–12. 2006.

[2] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy". Foundations and Trends in Theoretical Computer Science, vol. 9(3-4), pp. 211-407, 2014.

[3] X. Du, M. Guizani, Y. Xiao and H. H. Chen, "A Routing-Driven Elliptic Curve Cryptography based Key Management Scheme for Heterogeneous Sensor Networks," IEEE Transactions on Wireless Communications, Vol. 8, No. 3, pp. 1223 - 1229, March 2009.

[4] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks," Journal of Computer Communications, Vol. 30, Issue 11-12, pp. 2314-2341, Sept. 2007.

[5] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, "An Effective Key Management Scheme for Heterogeneous Sensor Networks," Ad Hoc Networks, Elsevier, Vol. 5, Issue 1, pp 24–34, Jan. 2007.

[6] U. Erlingsson, P. Vasyl, and K. Aleksandra, "RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response." In Proceedings of the 2014 ACM Conference on Computer and Communications Security, pp. 1054–67, 2014.

[7] G. Fanti, V. Pihur and úlfar Erlingsson, "Building a RAPPOR with the Unknown: Privacy-Preserving Learning of Associations and Data Dictionaries" In Proceedings on Privacy Enhancing Technologies, pp. 41-61, 2016.

[8] S. Vinterbo, "A simple algorithm for estimating distribution parameters from n-dimensional randomized binary responses" arxiv:1803.0398 unpublished.

[9] L. Wu, X. Du, and X. Fu, "Security Threats to Mobile Multimedia Applications: Camera-based Attacks on Mobile Phones," IEEE Communications Magazine, Vol. 52, Issue 3, March 2014.

[10] L. Wu, and X. Du, "MobiFish: A Lightweight Anti-Phishing Scheme for Mobile Phones," in Proc. of the 23rd International Conference on Computer Communications and Networks (ICCCN), Shanghai, China, August 2014.

[11] X. Huang, X. Du, "Achieving big data privacy via hybrid cloud," in Proc. of 2014 IEEE INFOCOM Workshops, Pages: 512 – 517

[12] X.Fang, S. Misra, and G. Xue, "Smart grid—The new and improved power grid: A survey," IEEE communications surveys & tutorials, vol. 14(4), pp. 944-980, 2012.

[13] W. Wang, Y. Xu, M. Khanna, "A survey on the communication architectures in smart grid," Computer Networks, vol. 55(15), pp. 3604-3629, 2011.

[14] NIST, "National institute of standards and technology –guidelines for smart grid cybersecurity: Vol. 2 - privacy and the smart grid," 2010.

[15] R. Lu, X. Liang, and X. Li, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," IEEE Transactions on Parallel & Distributed Systems, vol. 23(9), pp.1621-1631, 2012.

[16] X. Du and H. H. Chen, "Security in Wireless Sensor Networks," IEEE Wireless Communications Magazine, Vol. 15, Issue 4, pp. 60-66, Aug. 2008.

[17] Zhang Z, Qin Z, Zhu L, et al. Toward practical differential privacy in smart grid with capacity-limited rechargeable batteries. arXiv preprint arXiv:1507.03000, 2015.

[18] Ács G, Castelluccia C. I Have a DREAM!(differentially private smart metering)[C]//Information hiding. 2011, 6958: 118-132.

[19] Eibl G, Engel D. Differential privacy for real smart metering data[J]. Computer Science - Research and Development, 2017,32(2): 173–182

[20] C. Dwork, F. Mcsherry, and K. Nissim, "Calibrating noise to sensitivity in private data analysis" In the Proceedings of 3rd Theory of Cryptography Conference, pp. 265-284, 2006.

[21] F. McSherry. "Privacy integrated queries: an extensible platform for privacy-preserving data analysis," In Proceedings of the ACM SIGMOD International Conference on Management of data. Pp. 19-30,2009 .

[22] V. Rastogi, and S. Nath, "Differentially private aggregation of distributed time-series with transformation and encryption," In Proceedings of the International Conference on Management of Data, pp. 735-746, 2010.

[23] P. Barbosa, A. Brito, and H. Almeida, "A Technique to provide differential privacy for appliance usage in smart metering," Information Sciences, pp.355-367, 2016.

[24] Kolter J Z, Batra S, Ng A Y. Energy disaggregation via discriminative sparse coding[C]// International Conference on Neural Information Processing Systems. Curran Associates Inc. 2010:1153-1161.

[25] Grosse R, Raina R, Kwong H, et al. Shift-Invariance Sparse Coding for Audio Classification[J]. Computer Science, 2012, 9.

[26] Roweis S T. One microphone source separation[C]//Annual conference on neural information processing systems. 2001: 793-799.

[27] Elhamifar E, Sastry S. Energy disaggregation via learning 'Powerlets' and sparse coding[C]// The 29th AAAI Conference on Artificial Intelligence, 2015:629-635.

[28] Jenatton R, Mairal J, Obozinski G, et al. Proximal Methods for Hierarchical Sparse Coding[J]. Journal of Machine Learning Research, 2010, 12(7):2297-2334.

[29] Singh S, Majumdar A. Deep Sparse Coding for Non-Intrusive Load Monitoring[J]. IEEE Transactions on Smart Grid, 2017.2:1-10

[30] Jongho Won, Y. T. Chris, and K.Y. David, "Privacy-Assured Aggregation Protocol for Smart Metering: A Proactive Fault-Tolerant Approach," IEEE/ACM Transactions on Networking, vol. 24(3), pp. 1661-1674, June 2016.

[31] G. Hart. "Nonintrusive appliance load monitoring," In Proceedings of the IEEE, vol. 80(12), pp.1870-1891,1992.

[32] J. Kolter, M. Johnson. "REDD: A Public Data Set for Energy Disaggregation Research". Workshop on Data Mining Applications in Sustainability, vol. 25, pp. 59-62, 2011.

[33] N.Batra, J. Kelly, O. Parson, H. Dutta, K. William and et al, "NILMTK: an open source toolkit for non-intrusive load monitoring" In Proceedings of 5th International Conference on Future Energy Systems, pp. 265-276, 2014.

[34] L. Sankar, R.Rajagopalan, S. Mohajer, and S.Mohajer. "Smart Meter Privacy: A Theoretical Framework". IEEE Transactions on Smart Grid, vol. 4(2), pp. 837-846, 2013.