A Privacy Preserving Multiagent System for Load Balancing in the Smart Grid*

Extended Abstract

Shangyu Xie
Illinois Institute of Technology
Chicago, Illinois
sxie14@hawk.iit.edu

Yuan Hong
Illinois Institute of Technology
Chicago, Illinois
yuan.hong@iit.edu

Peng-Jun Wan
Illinois Institute of Technology
Chicago, Illinois
wan@cs.iit.edu

ABSTRACT

To improve system economics and reliability, microgrids (viz. power consumers equipped with local generators) can cooperatively utilize their local energy to facilitate load balancing on the power grid (balancing the regional supply and demand) via a multiagent system. However, due to the privacy concerns on continuously revealing each microgrid's local data (e.g., demand and supply at different times) for deriving real-time optimal balancing decisions, the application of such multiagent cooperation is still limited. In this paper, we design a novel privacy preserving multiagent system via an efficient cryptographic protocol for cooperatively balancing the regional supply and demand, as well as each microgrid's local supply and demand without disclosing their local data.

KEYWORDS

Privacy; Multiagent System; Smart Grid; Secure Computation

ACM Reference Format:
Shangyu Xie, Yuan Hong, and Peng-Jun Wan. 2019. A Privacy Preserving Multiagent System for Load Balancing in the Smart Grid. In *Proc. of the 18th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2019), Montreal, Canada, May 13–17, 2019,* IFAAMAS, 3 pages.

1 INTRODUCTION

Load balancing on the power grid is essential for both energy saving and stability of the power system [13]. The goal is to *balance supply and demand within a tight margin* in real time: if supply exceeds demand, besides storing the extra energy (may result in huge energy loss), voltage spike would occur in the power system; when the supply lags behind demand, the voltage sags. Both of these unbalanced situations would be detrimental to power grid operations and devices connected to the grid [23]. In recent smart grid infrastructure, the deployed microgrids (which are both power suppliers and consumers) could facilitate the main grid to further obtain load balancing via a multiagent system (MAS) – ensuring better *system economics* and *reliability* [18].

However, the above multiagent cooperation requests all the agents (e.g., main grid and microgrids) to jointly compute the real time optimal energy allocation for load balancing with their private local data (*most of which are generated in real time*), such as the regional supply, each microgrid's demand load and maximum local supply (at diffent times) as well as the maximum tolerable gap between its supply and demand. Clearly, disclosing these data for optimizing the multiagent load balancing decisions would explicitly compromise their privacy [3, 6, 8, 10, 17, 19]. Although numerous privacy preserving schemes [1, 5, 16, 17] have been proposed in literature to address the privacy concerns in the smart grid, most of them focus on the smart metering data and propose relevant privacy preserving metering applications (e.g., regional statistics [2], billing [6], and aggregation [11]). None of such existing techniques can be applicable to private multiagent load balancing in real time. To address this deficiency, we propose a novel light-weight cryptographic protocol under Secure Multiparty Computation (SMC) [4, 22], and implement our privacy preserving multiagent system (namely, Pairing) based on the cryptographic protocol.

2 PROBLEM FORMULATION

Given n microgrids $\forall i \in [1, n], M_i$, we denote the main grid G's regional supply allocated for all the n microgrids at time t as S^t, each microgrid M_i's local demand load and supply as d_i^t and s_i^t, respectively, and its external demand as x_i^t. The energy transmission efficiency [9] can be defined as $\eta_i \in [0, 1]$. Specifically, at time t, a cooperative model is to find the *optimal external demand* $\bar{x}_i^t$ of individual microgrids $M_i, 1 \le i \le n$ such that the overall deviation between the regional demand and supply is minimized. Meanwhile, the deviation between each microgrid M_i's overall supply (local s_i^t and external x_i^t) and local demand (d_i^t) should be bounded by a tight balancing margin ξ_i (which can be specified by itself as a ratio or value) [15, 21]. Hence, the cooperative load balancing problem at time t can be mathematically formulated:

$$\min : |\sum_{\forall i=1}^{n} \frac{x_i^t}{\eta_i} - S^t| \text{ (at time t)}$$
$$s.t. \begin{cases} |x_1^t + s_1^t - d_1^t| \le \xi_1 \\ \vdots \quad\quad \vdots \quad\quad \vdots \\ |x_n^t + s_n^t - d_n^t| \le \xi_n \\ 1 \le i \le n, x_i^t \ge 0, \eta_i \in [0, 1] \end{cases} \tag{1}$$

Since we aim at proposing a multiagent system running continuously over any period, the above nonlinear programming (NLP) problem should be iteratively solved at any time (w.l.o.g., over any period $t \in [1, m]$) with limited information disclosure, where each party's excessive energy (both regional and local) at time t will be stored and rolled over to its supply at time $(t + 1)$.

*This work is partially supported by the National Science Foundation (NSF) under Grant No. CNS-1745894 and the WISER ISFG grant.

Proc. of the 18th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2019), N. Agmon, M. E. Taylor, E. Elkind, M. Veloso (eds.), May 13–17, 2019, Montreal, Canada.

3 PROTOCOL DESIGN FOR PAIRING

3.1 overview

Figure 1 outlines the major components of the protocol for our PAIRING system. In initialization, main grid G and all the microgrids generate their own key pairs (pk, sk) and $\forall i \in [1, n], (pk_i, sk_i)$, and share the public keys pk and $pk_1, \dots, pk_n$ to all the parties (keys are generated per Homomorphic Encryption, e.g., Paillier Cryptosystem [14]). At each time $t \in [1, m]$, all the parties jointly call sub-protocol Secure Categorization (SC) and possibly call sub-protocol Secure Approximation (SA) to derive the optimal external demands $\forall i \in [1, n], \bar{x}_i^t$ (SA is only called in a certain output case of SC). Then, each microgrid $M_i, 1 \leq i \leq n$ requests the energy with amount $\bar{x}_i^t$ from G at time t. Finally, all parties call the sub-protocol Secure Rollover (SR) to locally store the excessive energy for the next time slot.

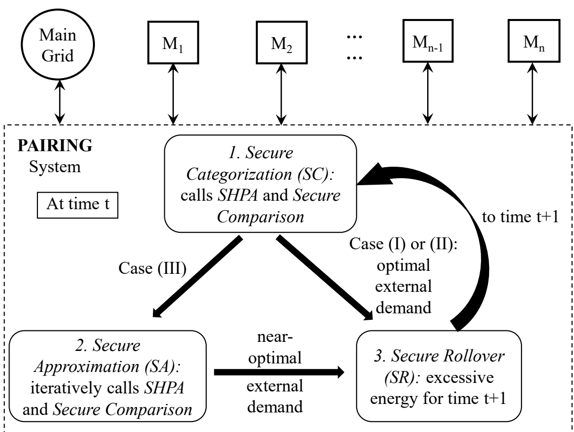

Figure 1: PAIRING System

3.2 Secure Optimization at Time t

Intuitively, the objective function $|\sum_{i=1}^{n}(x_i^t/\eta_i) - S^t|$ can be minimized to 0 if the variables $\forall i \in [1, n], x_i^t$ can make $\sum_{i=1}^{n}(x_i^t/\eta_i) = S^t$ hold. Thus, we have:

LEMMA 3.1. *The optimal solution of the supply and demand balancing problem at time t can be derived as below:*

- *Case (I): if* $S^t \geq \sum_{i=1}^{n}[(d_i^t - s_i^t + \xi_i)/\eta_i]$, *then external demands* $\forall i \in [1, n], \bar{x}_i^t = (d_i^t - s_i^t + \xi_i)/\eta_i$ *are optimal;*
- *Case (II): if* $S^t \leq \sum_{i=1}^{n}[(d_i^t - s_i^t - \xi_i)/\eta_i]$, *then external demands* $\forall i \in [1, n], \bar{x}_i^t = (d_i^t - s_i^t - \xi_i)/\eta_i$ *are optimal;*
- *Case (III): if* $\sum_{i=1}^{n}[(d_i^t - s_i^t - \xi_i)/\eta_i] < S^t < \sum_{i=1}^{n}[(d_i^t - s_i^t + \xi_i)/\eta_i]$, *then* $|\sum_{i=1}^{n} x_i^t/\eta_i - S^t| = 0$ *hold with multiple optimal solutions.*

The optimal solutions for Case (I) and (II) are constants. In Case (III), PAIRING securely approximates one of the multiple optimal solutions. The proposed cryptographic protocol provides *strong security* and better *parallelization* of computation for higher efficiency and scalability, compared to securely solving the exact solution [7, 20]).

3.2.1 Secure Hierarchically Paired Aggregation (SHPA). SHPA is invoked to aggregate shares of the data from all the parties for *"Two Rounds"* in which both aggregated results will be securely compared later. For instance, while comparing $\sum_{i=1}^{n}[(d_i^t - s_i^t - \xi_i)/\eta_i]$ and S^t, each microgrid M_i will generate a random nonce r_i such that $\sum_{i=1}^{n}[(d_i^t - s_i^t - \xi_i)/\eta_i + r_i]$ (Round A) and $S^t + \sum_{i=1}^{n} r_i$ (Round B) are aggregated for comparison (to securely obtain an *equivalent result* as the original comparison). SHPA primarily utilizes the homomorphic encryption building block (e.g., Paillier Cryptosystem [14]) for summing up the distributed shares via *hierarchical pairing* in a random order, which can also mitigate the collusion threats. Specifically, at the beginning, a microgrid (say $M_r, 1 \leq r \leq n$) is randomly picked to utilize its public key pk_r for encryption in Round A. The main grid G's public key pk will be used in Round B.

3.2.2 Secure Categorization (SC). At each time $t \in [1, m]$, Secure Categorization (SC) only executes once to securely decide the case of the current load balancing (per Lemma 3.1). To decide Case (I), (II) or (III), two secure comparisons (by leveraging the FAIRPLAY [12], a Secure Function Evaluation system) should be executed: (1) $S^t + \sum_{i=1}^{n} r_i$ (held by G) and $\sum_{i=1}^{n}[(d_i^t - s_i^t + \xi_i)/\eta_i + r_i]$ (held by a random microgrid M_r); (2)$S^t + \sum_{i=1}^{n} r_i'$ (held by G) and $\sum_{i=1}^{n}[(d_i^t - s_i^t - \xi_i)/\eta_i + r_i']$ (held by a random microgrid M_r'). Each of the above comparisons calls sub-protocol SHPA once to aggregate the two random numbers for G and M_r, respectively.

3.2.3 Secure Approximation (SA). If Case (III) is identified in the SC, another sub-protocol Secure Approximation (SA) will be called by all the parties (including G) to jointly approximate a near-optimal solution for minimizing the deviation between the regional supply and demand. SA is established by performing λ-round secure *distributed binary search* by all the microgrids (which also calls SHPA and secure comparison with the main grid G for locating each microgrid's upper/lower bounds of the search).

THEOREM 3.2. *A λ-round Secure Approximation (SA) approximates the optimal solution with a bounded error* $\sum_{i=1}^{n}[\xi_i/2^{(\lambda-1)}]^2$.

3.3 Real-time Cryptographic Protocol

The substations (as main grid) or microgrids are generally equipped with a battery that can store excessive energy [18] (the capacity of the battery is generally greater than the excessive energy after balancing). We design our sub-protocol Secure Rollover (SR) to store the excessive energy for next time slot if the (local or regional) supply exceeds the demand (still balanced with a tight margin) at time t. Note that sub-protocol Secure Rollover is locally executed by each agent, and does not result in information leakage.

4 CONCLUSION

We have designed a multiagent system PAIRING based a novel efficient cryptographic protocol for privately balancing real-time regional supply and demand on the power grid as well as microgrids' local supply and demand. We also implemented the PAIRING system that integrates secure computation, communication and power transmission. High accuracy and efficient system performance would enable smooth deployments of PAIRING in the emerging smart grid infrastructure.

REFERENCES

[1] Gergely Ács and Claude Castelluccia. 2011. I Have a DREAM! (DiffeRentially privatE smArt Metering). In *Information Hiding*. 118–132.

[2] Cheng-Kang Chu, Joseph K. Liu, Jun Wen Wong, Yunlei Zhao, and Jianying Zhou. 2013. Privacy-preserving smart metering with regional statistics and personal enquiry services. In *ASIACCS*. 369–380.

[3] Sanjay Goel, Yuan Hong, Vagelis Papakonstantinou, and Dariusz Kloza. 2015. *Smart Grid Security*. Springer Publishing Company, Incorporated.

[4] Oded Goldreich, Silvio Micali, and Avi Wigderson. 1987. How to Play any Mental Game - A Completeness Theorem for Protocols with Honest Majority. In *Proceedings of the 19th ACM Symposium on the Theory of Computing*. ACM, New York, NY, 218–229. http://doi.acm.org/10.1145/28395.28420

[5] Yuan Hong, Sanjay Goel, and Wen Ming Liu. 2016. An Efficient and Privacy-preserving Scheme for P2P Energy Exchange Among Smart Microgrids. *International Journal of Energy Research* 40, 3 (2016), 313–331.

[6] Yuan Hong, Wen Ming Liu, and Lingyu Wang. 2017. Privacy Preserving Smart Meter Streaming Against Information Leakage of Appliance Status. *IEEE Trans. Information Forensics and Security* 12, 9 (2017), 2227–2241. https://doi.org/10.1109/TIFS.2017.2704904

[7] Yuan Hong, Jaideep Vaidya, and Haibing Lu. 2012. Secure and efficient distributed linear programming. *Journal of Computer Security* 20, 5 (2012), 583–634.

[8] Yuan Hong, Han Wang, Shangyu Xie, and Bingyu Liu. 2018. Privacy Preserving and Collusion Resistant Energy Sharing. In *2018 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2018, Calgary, AB, Canada, April 15-20, 2018*. 6941–6945. https://doi.org/10.1109/ICASSP.2018.8462202

[9] Zhichuan Huang, Ting Zhu, David Irwin, Aditya Mishra, Daniel Menasche, and Prashant Shenoy. 2016. Minimizing Transmission Loss in Smart Microgrids by Sharing Renewable Energy. *ACM Trans. Cyber-Phys. Syst.* 1, 2, Article 5 (Dec. 2016), 22 pages. https://doi.org/10.1145/2823355

[10] Akhtar Hussain, Van-Hai Bui, and Hak-Man Kim. 2018. A Resilient and Privacy-Preserving Energy Management Strategy for Networked Microgrids. *IEEE Trans. Smart Grid* 9, 3 (2018), 2127–2139. https://doi.org/10.1109/TSG.2016.2607422

[11] Klaus Kursawe, George Danezis, and Markulf Kohlweiss. 2011. Privacy-friendly aggregation for the smart-grid. In *PETS'11*. 175–191.

[12] Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella. 2004. Fairplay - Secure Two-Party Computation System. In *Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA, USA*. 287–302. http://www.usenix.org/publications/library/proceedings/sec04/tech/malkhi.html

[13] V. Mathew, R. K. Sitaraman, and P. Shenoy. 2012. Energy-aware load balancing in content delivery networks. In *2012 Proceedings IEEE INFOCOM*. 954–962. https://doi.org/10.1109/INFCOM.2012.6195846

[14] P. Paillier. 1999. Public key cryptosystems based on composite degree residuosity classes. In *Advances in Cryptology - Eurocrypt '99 Proceedings, LNCS 1592*. 223–238.

[15] A. Ricci, B. Vinerba, E. Smargiassi, I. De Munari, V. Aisa, and P. Ciampolini. 2008. Power-Grid Load Balancing by Using Smart Home Appliances. In *2008 Digest of Technical Papers - International Conference on Consumer Electronics*. 1–2. https://doi.org/10.1109/ICCE.2008.4588081

[16] Cristina Rottondi, Giacomo Verticale, and Antonio Capone. 2013. Privacy-preserving smart metering with multiple data Consumers. *Computer Networks* 57, 7 (2013), 1699–1713.

[17] Lalitha Sankar, S. Raj Rajagopalan, Soheil Mohajer, and H. Vincent Poor. 2013. Smart Meter Privacy: A Theoretical Framework. *IEEE Trans. Smart Grid* 4, 2 (2013), 837–846.

[18] Jochen Schwill. 2016. How to balance supply and demand on new electricity markets. *Gencom's Newsletter* (2016).

[19] Onur Tan, Deniz Gündüz, and H. Vincent Poor. 2013. Increasing Smart Meter Privacy Through Energy Harvesting and Storage Devices. *IEEE Journal on Selected Areas in Communications* 31, 7 (2013), 1331–1341.

[20] Jaideep Vaidya. 2009. A Secure Revised Simplex Algorithm for Privacy-Preserving Linear Programming. In *AINA '09: Proceedings of the 23rd IEEE International Conference on Advanced Information Networking and Applications*. 347–354.

[21] Reinier A.C. van der Veen and Rudi A. Hakvoort. 2016. The electricity balancing market: Exploring the design challenge. *Utilities Policy* 43 (2016), 186 – 194. https://doi.org/10.1016/j.jup.2016.10.008

[22] Andrew C. Yao. 1986. How to generate and exchange secrets. In *Proceedings of the 27th IEEE Symposium on Foundations of Computer Science*. IEEE, IEEE Computer Society, Los Alamitos, CA, USA, 162–167.

[23] Mengmeng Yu and Seung Ho Hong. 2016. Supply and demand balancing for power management in smart grid: A Stackelberg game approach. *Applied Energy* 164 (2016), 702 – 710. https://doi.org/10.1016/j.apenergy.2015.12.039