International Journal of Latest Trends in Engineering and Technology
Special Issue April-2018, pp. 106-112
e-ISSN:2278-621X

SECURE AND PRIVATE DATA AGGREGATION FOR ENERGY CONSUMPTION SCHEDULING IN SMART GRIDS

G.Arul Kumar[1], Ms.Anilarose[2]

Abstract: The recent proposed solutions for demand side energy management leverage the two-way communication infrastructure provided by modern smart-meters and sharing the usage information with the other users. In this paper, we first highlight the privacy and security issues involved in the distributed demand management protocols. We propose a novel protocol to share required information among users providing privacy, confidentiality, and integrity. We also propose a new clustering-based, distributed multi-party computation (MPC) protocol. Through simulation experiments we demonstrate the efficiency of our proposed solution. The existing solutions typically usually thwart selfish and malicious behavior of consumers by deploying billing mechanisms based on total consumption during a few time slots. However, the billing is typically based on the total usage in each time slot in smart grids. In the second part of this paper, we formally prove that under the per-slot based charging policy; users have incentive to deviate from the proposed protocols. We also propose a protocol to identify untruthful users in these networks. Finally, considering a repeated interaction among honest and dishonest users, we derive the conditions under which the smart grid can enforce cooperation among users and prevents dishonest declaration of consumption.

1. INTRODUCTION:

A recent report from U.S. Department of Energy [1] states that, in the Unites States, almost two-fifths of the total electricity is consumed in households. However, the energy use is not efficient; the distribution of energy consumption rate in different hours of the day is not even. The peak usage of electricity is much higher than the offpeak periods. The peak value of electricity consumption data is extremely important for electric companies as the generation capacity of their power plants must be higher than the peak value. If some loads from the peak-periods can be shifted to the off-peak periods, the power company would be benefited by the reduction of the cost of power generation.

Controlling the energy usage at the customer side of smart meters has received a lot of attention. Some research (e.g., [2], [3], [4]) has been made to minimize the cost of production with the indirect interaction between the energy users (i.e., the customers) and the energy provider giving incentive for using energy at off-peak hours. The advent of smart meters gives the opportunity of two-way communication between the meters and the utility servers through the intelligent collectors [5]. This opportunity allows the researchers to rethink the optimal demand side management, which is also known as demand response. A direct load control solution for demand response is proposed in [6], where the utility remotely controls energy consumption for high-load household appliances like air conditioners and water heaters. In [7] and [8], electricity scheduling methods are proposed to reduce the peak-to average ratio (PAR) of the energy usage by introducing some flexible electricity price functions. These methods depend on the response of the users to the time-differentiated prices by shifting their load from the peak hours to the off-peak hours.

These research works focus on the household users, particularly the household appliances, which are flexible in their usage time; hence one can shift the usage time from peak time to off-peak time to reduce the cost. Mohsenian-Rad et al. in [9] proposed an autonomous and distributed demand-side energy management system among users that takes advantage of the communication infrastructure among the smart meters. The game-theory [10] is applied to formulate the energy consumption scheduling (ECS) problem, solution to which gives the maximum payoff to the users. Similar automated demand side management systems are also proposed in [11], [12], [13], [14], [15]. In these works, demand response solutions typically optimize the overall cost of power generation and, thereby, the usage cost of the customers. The distributed algorithm for the optimization of the energy consumption schedule requires a user to broadcast his hourly usage information to the other participating users; this algorithm interferes with the privacy problem. As the participating users possess various characteristics and they are mostly unknown to each other, privacy is an important matter. The algorithm is also susceptible to false data injection and replay attacks.

Due to these attacks, the optimization algorithm can come up with a result which is different from the actual optimal result. In this case, the participating users after optimization may not get the expected benefit; rather, they can end up paying much more than the

regular price. Moreover, some participating users may lie (i.e., defect) about their energy consumption behaviors.

[1] PG Scholar, Department of Computer Sciuence and Engineering, Rajiv Gandhi College of Engineering
[2] H.O.D,Department of Computer Sciuence and Engineering, Rajiv Gandhi College of Engineering

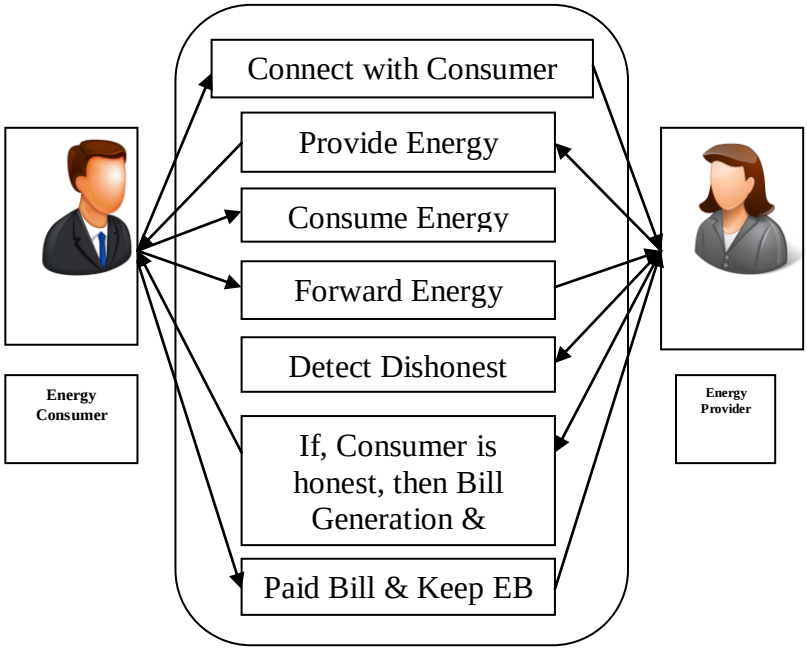

Fig:1 System Architecture Diagram

In this work, we propose some novel mechanisms for the distributed customer-side demand management in order to thwart security and privacy attacks by malicious outsiders or insiders in smart grids. We propose a mechanism for optimizing energy cost that meets the security challenges and performs efficiently that is developed on top of the typical energy consumption scheduling model. Our contributions in this paper are fivefold:

First, we propose an efficient secure multi-party computing (MPC) solution to preserve the privacy and security of the usage schedules. We have adopted the energy consumption scheduling model and management protocol proposed in [9] as a use case. Second, we enhance the efficiency of the distributed demand management protocol by clustering the participants and executing the optimization protocol over the clusters. Third, we demonstrate a scenario wherein a participating user can benefit by telling lies about its usage, if the price of electricity is computed based on consumers' usage in each slot (we call it per-slot billing mechanism in this paper). We also formally prove the incentive to deviate in such a scenario. Then we discuss assumptions for which there is no incentive for defecting. We also devise a truthful verifier-based solution in order to ensure the truthfulness of the participating users, where the verifier could be one of the users. Fourth, considering repeated interactions among users, we derive the conditions under which we can enforce cooperation among users and prevents dishonest declaration of consumption by a simple tit-for-tat mechanism. Finally, we evaluate the scalability and efficiency of our solution by executing simulation experiments.

Literature Review:

In this work, first we briefly discuss the research done so far for optimizing the energy usage cost. Then, we present a brief discussion on the research work that address the security and privacy problems related to this area.

Fahrioglu and Alvarado proposed a game [3] that models the interaction between a utility and its customers to let the customers help a utility solve a variety of problems. Herter in [4] proposed a mechanism to minimize the generation cost with the indirect interaction between the energy users and the energy provider by providing incentive for using energy at off-peak hours with the help of time-varying energy prices. Gomes et al. discussed a load control strategy in [25]. The paper implemented the elastic electrical price. The authors pointed out that the complexity is increased by the diversity and volatility in power systems, because the individuals have different aim.

Ruiz et al. in [7] introduced a direct load control algorithm based on linear programming to operate the virtual power plant composed of a large number of users with load reduction capabilities. The author in [26] made an investigation on relationship between the critical-peak pricing and the households with different income and usage in California State. This work justifies the need of a good cost function which can affect the behavior of users and their usage. However, the automation of the optimal demand side management solely by the interactions among the participating users (i.e., without an involvement of the utility) can offer an open, independent, and creative solution.

Mohsenian-Rad and Leon-Garcia proposed an optimal and automatic residential energy consumption scheduling framework in [27] that minimizes the electricity payment as well as the operational waiting time of each household appliance under a real-time pricing model. The authors addressed a similar problem in [9], [28] for autonomous demand side management within a neighborhood. They considered the deployment of energy consumption scheduling devices in smart meters, which can communicate with each other. The game theory is applied to distributive find the optimal consumption scheduling for all

the users. There are also other autonomous demand side management solutions presented by different researchers in [11], [12], [13], [14], [15]. In these solutions, the overall energy production or usage cost is minimized by controlling the energy consumption directly with optimal scheduling or indirectly with suitably chosen energy prices. Another demand response system is designed in [29] by minimizing the peak-to-average ratio of the aggregate load demand.

In [19], fairness in autonomous demand response is discussed based on the contribution that a user makes in achieving the system's global objective. However, none of these algorithms addresses the security problems introduced by their proposed algorithms. Li et al. presented a distributed data aggregation process for smart meters involved in transmitting data from a set of meters to the data collector [30]. To protect user privacy, they applied homomorphic cryptography. So, the meters participating in the aggregation cannot see intermediate results. However, their solution is costly and it cannot solve the security issues other than privacy found in our problem domain.

In [31], the authors showed that it is possible to extract the detail information about the household activities of a customer without any prior knowledge. In order to secure the customer's privacy, the authors also proposed a homomorphic encryption based zero-knowledge billing protocol for smart meters. Raj et al. proposed a privacy preserving approach by perturbing the usage data while meeting the utility needs [32].

Sankar et al. in [33] introduced the competitive privacy problem in distributed state estimation at the regional transmission organizations. Unlike above works, we proposed a lightweight MPC based data aggregation protocol that solves privacy as well as data integrity problems. In addition, with respect to the data integrity, we addressed the need of the participants' truthfulness in such protocols and proposed mechanisms to ensure this truthfulness by punishing for lying. Although we focused on the optimal scheduling of customers' energy consumption, our work is applicable to other problems in smart grids that need data aggregation among the participants.

2. RELATED WORKS

In this section, first we briefly discuss the research done sofar for optimizing the energy usage cost. Then, we present a brief discussion on the research work that address the securityand privacy problems related to this area. Fahrioglu and Alvarado proposed a game [3] that models the interaction between a utility and its customers to let the customers help a utility solve a variety of problems. Herter in [4] proposed a mechanism to minimize the generation cost with the indirect interaction between the energy users and the energy provider by providing incentive for using energy at off-peak hours with the help of time-varying energy prices. Gomes et al. discussed a load control strategy in [25]. The paper implemented the elastic electrical price. The authors pointed out that the complexity is increased by the diversity and volatility in power systems, because the individuals

have different aim. Ruiz et al. in [7] introduced a direct load control algorithm based on linear programming to operate the virtual power plant composed of a large number of users with load reduction capabilities. The author in [26] made an investigation on relationship between the critical-peak pricing and

the households with different income and usage in

California State. This work justifies the need of a good cost function which can affect the behavior of users and their usage. However, the automation of the optimal demand side management solely by the interactions among the participating users (i.e., without an involvement of the utility) can offer an open, independent, and creative solution. Mohsenian-Rad and Leon-Garcia proposed an optimal and automatic residential energy consumption scheduling framework in [27] that minimizes the electricity payment as well as the operational waiting time of each household appliance under a real-time pricing model. The authors addressed a similar problem in [9], [28] for autonomous demand side management within a neighborhood. They considered the deployment of energy consumption scheduling devices in smart meters, which can communicate with each other. The game theory is applied to distributively find the optimal consumption scheduling for all the users. There are also other autonomous demand side management solutionspresented by different researchers in [11], [12], [13],[14], [15]. In this solutions, the overall energy production or usage cost is minimized by controlling the energy consumption directly with optimal scheduling or indirectly with suitably chosen energy prices. Another demand response system is designed in [29] by minimizing the peak-to-average ratio of the aggregate load demand. In [19], fairness in autonomous demand response is discussed based on the contribution that a user makes in achieving the system's global objective. However, none of these algorithms addresses the security problems introduced by their proposed algorithms. Li et al. presented a distributed data aggregation process for smart meters involved in transmitting data from a set of meters to the data collector [30]. To protect user privacy, they applied homomorphic cryptography. So, the meters participating in the aggregation cannot see intermediate results. However, their solution is costly and it cannot solve

the security issues other than privacy found in our problem domain. In [31], the authors showed that it is possible to extract the detail information about the household activities of a customer without any prior knowledge. In order to secure the customer's privacy, the authors also proposed a homomorphic encryption based zero-knowledge billing protocol for smart meters. Raj et al. proposed a privacy preserving approach by perturbing the usage data while meeting the utility needs [32]. Sankar et al. in [33] introduced the competitive privacy problem in distributed state estimation at the regional transmission organizations. Unlike above works, we proposed a lightweight MPC based data aggregation protocol that solves privacy as well as data integrity problems. In addition, with respect to the data integrity, we addressed the need of the participants' truthfulness in such protocols and proposed mechanisms to ensure this truthfulness by punishing for lying. Although we

focused on the optimal scheduling of customers' energy consumption, our work is applicable to other problems in smart grids that need data aggregation among the participants.

3. PROPOSED WORK

In this system, first, we propose an efficient secure multi-party computing (MPC) solution to preserve the privacy and security of the usage schedules. We have adopted the energy consumption scheduling model and management protocol proposed as a use case. Second, we enhance the efficiency of the distributed demand management protocol by clustering the participants and executing the optimization protocol over the clusters. Third, we demonstrate a scenario wherein a participating user can benefit by telling lies about its usage, if the price of electricity is computed based on consumers' usage in each slot (we call it per-slot billing mechanism in this paper). We also formally prove the incentive to deviate in such a scenario. Then we discuss assumptions for which there is no incentive for defecting. We also devise a truthful verifier-based solution in order to ensure the truthfulness of the participating users, where the verifier could be one of the users. Fourth, considering repeated interactions among users, we derive the conditions under which we can enforce cooperation among users and prevents dishonest declaration of consumption by a simple tit-for-tat mechanism

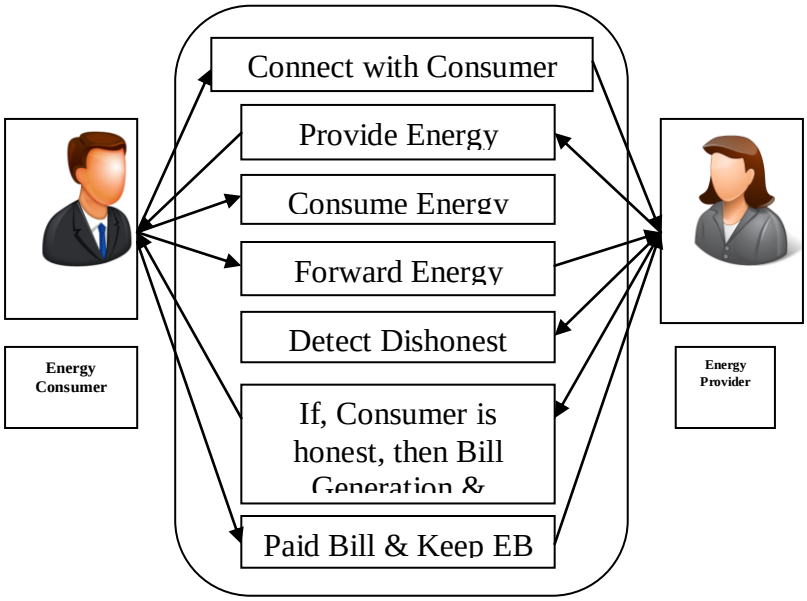

Fig:2 Architecture Diagram

Modules used in the application are

1. User Share Private Information
2. Energy Consumption model
3. Energy Consumption scheduling
4. Detect Dishonest user

3.1 User Share Private Informtion

In this module, many users are registered with smart grid.Here a user to broadcast his hourly usage information to the other participating users. While the integrity of the information is vulnerable to internal and external adversaries. To achieve this objective, in this work we consider the energy consumption scheduling model, in which users participate in a distributed protocol to optimize the energy usage cost.

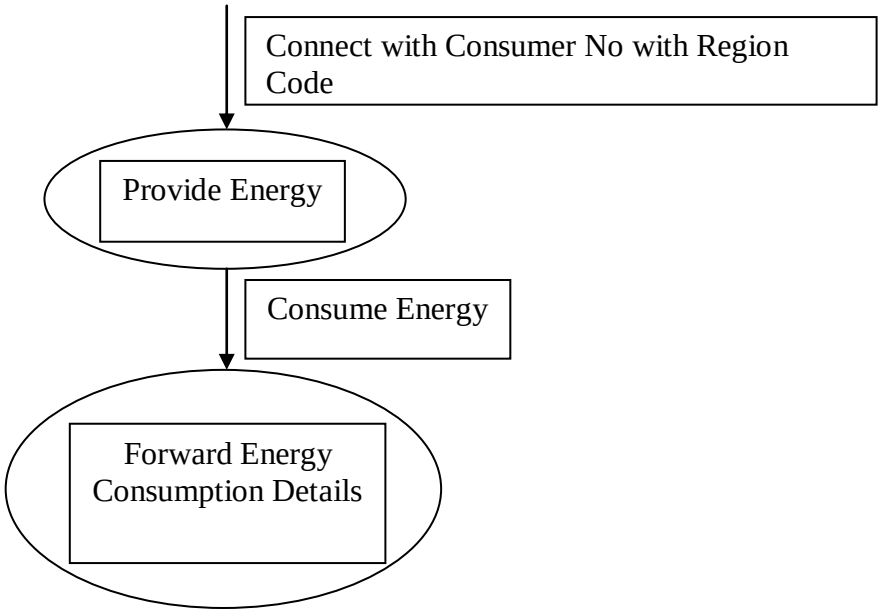

Fig 3.user share private information

3.2. Energy Consumption Model

In this module, the energy source provides the energy to the users by power lines. Each user is equipped with a smart meter. The smart meters are connected through the power line or Wi-Fi communication media, which forms a local area network (LAN). The energy provider is connected to this LAN through the wide area network (WAN).

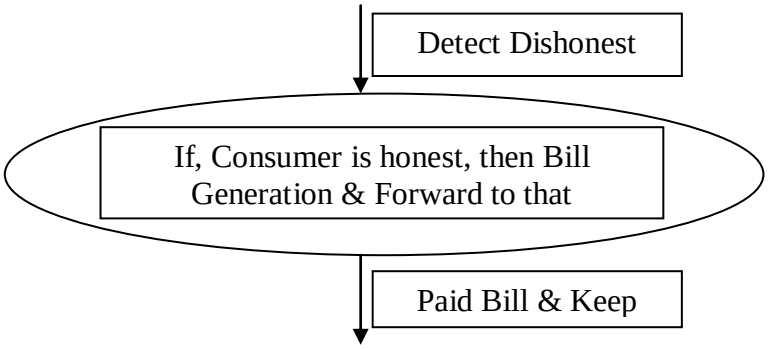

Fig.4.energy consumption model

3.3. Energy Consumption Scheduling

The strategy of each user x is its energy usage vector ux to maximize its payoff considering the other users strategies.In this module,we schedule the user's energy consumption.After Scheduling, we enhance the efficiency of the distributed demand management protocol by clustering the participants and executing the optimization protocol over the clusters.

3.4. Detect Dishonest User:

In this module, considering repeated interactions among users, we derive the conditions under which we can enforce cooperation among users and prevents

4. RESULT DISCUSSION

4.1 Evaluation

In this section, we present the evaluation results that we find by simulating our proposed solution for optimal and secured energy consumption scheduling. We also present the analytical results of applying the grim strategy with respect to the payoffs for different cases. 5.1 Simulation Results on Energy Consumption Scheduling We evaluate our proposed solution, especially its scalability, by running a simulation program written in Java. We run our experiment in Intel Core2-Duo 2:2 GHz Processor. Each user x 2 N has an arbitrary number of nonshiftable household appliances and an arbitrary number of shiftable household appliances. These arbitrary numbers are taken from a range between 10 to 20. Each nonshiftable appliance has a fixed operation schedule, while each shiftable appliance has a duration of operation and the possible time slots of operation (i.e., some consecutive time slots ranging from a starting slot to an ending slot). The number of possible

time slots must be larger than the usage duration. The properties of the appliances are chosen arbitrarily. We experiment using an arbitrary number of users (i.e., nodes). For the constants of the cost function Chð:Þ, we assume that both bh and ch are equal to 0 for all h 2 H, and the values of ah; h 2 H are an arbitrary value chosen between 0:5 to 0:6. The initial hourly cost of 15 users is depicted in Fig. 7a. In the experiment of our proposed solution, we use fixed size mutual exclusive clusters, while the number of clusters depends on the number of participating users. Our solution without clusters is almost similar to the algorithm of [9], except that the MPC algorithm (along with cryptographic measures) is executed by a node before each computation of the local optimization. We simulate MPC simply by the number of messages with a fixed processing overhead. The size of a cluster is taken as five users. We assume that the optimization process converges when the difference of cost reduction is less than 0:001 in the last consecutive rounds (e.g., 20) of local optimizations for each node.

In this section, we discuss about some points regarding our proposed solution for secure and private energy consumption scheduling

A Utility Collector Based Energy Consumption Scheduling Smart meters often forms a mesh network and they are connected to a data collector through this mesh network. A common framework for the communications often includes home area networks, building area networks, and neighborhood area networks, where we need many different communications between meters before sending data to the grid [23]. If we consider the usage data aggregation only, a smart meter needs to send its data to the collector through other meters, which does not preserve the privacy. Therefore, an aggregation scheme taking the help of a collector still needs to apply some privacy-preserving protocols.

A utility collector often sends collected usage data to the utility center by creating a secure channel with the utility server. However, in practice such secure channel is yet to be implemented in many places properly or fully, particularly for the communication among smart meters and collectors. For example, LonTalk is often used for communication among meters and collectors, which mainly ensures authentication of the two communicating parties [24]. After all, the privacy is not considered as a concern in this communication which is mainly taken place from a meter to a collector for reporting usage data to the utility center. On the other hand, the optimal scheduling protocol is executed among nodes (smart meters), where each node needs to know and use the received data for the optimal scheduling of energy consumptions. Therefore, the security, integrity, and privacy issues are required to be addressed together and comprehensively taking the protocol execution into consideration. In our work, we identify the potential threats of eavesdropping and false data injection with respect to the optimal energy usage scheduling protocol and thus provide a defense mechanism by ensuring data privacy along with the data authentication and integrity. We also provide security against semi-honest participating nodes, especially when they provide false information about their potential energy usage.

5. CONCLUSION

This work has presented a mutually exclusive cluster based solution for the optimal energy management problem, which can solve the security and privacy threats found in the earlier proposed solutions. Our solution provides data privacy, as well as protection from false data injection, i.e. data integrity. Comparing to the existing demand-side management solutions, the proposed approach is also highly efficient as in our proposed solution the running time increases almost linearly with the increase of the number of users. We have also presented an example which shows that a user participating in the optimization process can benefit by lying about his usage if the smart grid uses a per slot based charging mechanism. We have proved formally that a dishonest node can make benefit by lying about usage with per-slot based charging mechanism. We have proved that if a user cannot be untruthful about his total usage, then he cannot get any incentive by lying about the distribution of usage in different time slots. We have proposed a verifier based solution in order to detect malicious node who declared false information about its usage. We have also analyzed a grim trigger strategy solution for ensuring the truthfulness that can help smart grids to build incentive-based charging mechanisms. These mechanisms can be designed in future research works by choosing appropriate subscription period, reward and punishments values.

6. REFERENCES

[1] U.S. Department of Energy, 2010 renewable energy data book. (2011, Mar.) [Online]. Available: http://www.afdc.energy.gov/ pdfs/51680.pdf

[2] C. W. Gellings and J. H. Chamberlin, Demand-Side Management: Concepts and Methods, 2nd ed. Lilburn, GA, USA: Fairmont Press, 1993.

[3] M. Fahrioglu and F. L. Alvarado, "Designing incentive compatible contracts for effective demand management," IEEE Trans. Power Syst., vol. 15, no. 4, pp. 1255–1260, Nov. 2000.

[4] K. Herter, "Residential implementation of critical-peak pricing of electricity," Energy Policy, vol. 35, no. 4, pp. 2121–2130, Apr. 2007.

[5] R. Krishnan, "Meters of tomorrow [in my view]," IEEE Power Energy Mag., vol. 6, no. 2, pp. 96–94, Mar. 2008.

[6] B. Ramanathan and V. Vittal, "A framework for evaluation of advanced direct load control with minimum disruption," IEEE Trans. Power Syst., vol. 23, no. 4, pp. 1681–1688, Nov. 2008.

[7] N. Ruiz, I. Cobelo, and J. Oyarzabal, "A direct load control model for virtual power plant management," IEEE Trans. Power Syst., vol. 24, no. 2, pp. 959–966, May 2009.

[8] C. Triki and A. Violi, "Dynamic pricing of electricity in retail markets," Quart. J. Belgian, French Italian Operations Res. Soc., vol. 7, no. 1, pp. 21–36, Mar. 2009.

[9] [9] A.-H. Mohsenian-Rad, V.W.S. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand-side management based on game-theoretic energy consumptions scheduling for the future smart grid,"IEEE Trans. Smart Grid, vol. 1, no. 3, pp. 320–331, Dec. 2010.

[10] R. Gibbons, Game Theory for Applied Economics. Princeton, NJ, USA: Princeton Univ. Press, 1992.

[11] C. Ibars, M. Navarro, and L. Giupponi, "Distributed demand management in smart grid with a congestion game," in Proc. IEEE 1st Int. Conf. Smart Grid Commun., Oct. 2010, pp. 495–500.
[12] N. Gatsis and G. B. Giannakis, "Cooperative multi-residence demand response scheduling," in Proc. 45th Annu. Conf. Inf. Sci. Syst., Mar. 2011, pp. 1–6.
[13] S. K. Vuppala, K. Padmanabh, S. K. Bose, and S. Paul, "Incorporating fairness within demand response programs in smart grid," in Proc. IEEE PES, Innovative Smart Grid Technol., Jan. 2011, pp. 1–9.
[14] P. Samadi, R. Schober, and V. W. S. Wong, "Optimal energy consumption scheduling using mechanism design for the future smart grid," in Proc IEEE Int. Conf. Smart Grid Commun., Oct. 2011, pp. 369–374.
[15] M. Burcea, W.-K. Hon, H.-H. Liu, P. W.H. Wong, and D. K.Y. Yau, "Scheduling for electricity cost in smart grid," in Proc. 7th Int. Conf. Combinatorial Optim. Appl., 2013, pp. 306–317.
[16] M. A. Rahman, L. Bai, M. Shehab, and E. Al-Shaer, "Secure distributed solution for optimal energy consumption scheduling in smart grid," in Proc. IEEE 11th Int. Conf. Trust, Security Privacy Comput. Commun., Jun. 2012, pp. 279–286.
[17] A J. Wood and B. F. Wollenberg, Power Generation, Operation, and Control, 2nd ed. New York, NY, USA: Wiley, 1996.
[18] Y. Miyano and T. Namerikawa, "Load leveling control by realtime dynamical pricing based on steepest descent method," in Proc. SICE Annu. Conf., Aug. 2012, pp. 131–136.
[19] Z. Baharlouei, M. Hashemi, H. Narimani, and H. Mohsenian-Rad, "Achieving optimality and fairness in autonomous demand response: Benchmarks and billing mechanisms," IEEE Trans. Smart Grid, vol. 4, no. 2, pp. 968–975, Mar. 2013.
[20] O. Goldreich, Foundations of Cryptography: Volume 2, Basic Applications. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[21] M J. Atallah and W. Du, "Secure multi-party computational geometry," in Proc. 7th Springer-Verlag Int. Workshop Algorithms Data Struct., London, U.K., 2001, pp. 165–179.
[22] A C. Yao, "Protocols for secure computations," in Proc. 23rd Annu. Symp. Found. Comput. Sci., Nov. 1982, pp. 160–164.
[23] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 675– 685, Dec. 2011.
[24] Lontalk protocol specification. (1994).
[25] [Online]. Available: https:// support.dce.felk.cvut.cz/pub/hanzalek/_private/ref/LonTalk.PDF
[26] A Gomes, C.H. Antunes, and A.G. Martins, "A multiple objective evolutionary approach for the design and selection of load control strategies," IEEE Trans. Power Syst., vol. 19, no. 2, pp. 1173–1180, May 2004.
[27] P Centolella, "The integration of price responsive demand into regional transmission organization (RTO) wholesale power markets and system operations," Energy, vol. 35, no. 4, pp. 1568–1574, Apr. 2010.
[28] A-H. Mohsenian-Rad and A. Leon-Garcia, "Optimal residential load control with price prediction in real-time electricity pricing environments," IEEE Trans. Smart Grid, vol. 1, no. 2, pp. 120–133, Sep. 2010.
[29] A-H. Mohsenian-Rad, V. W. S. Wong, J. Jatskevich, and R. Schober, "Optimal and autonomous incentive-based energy consumption scheduling algorithm for smart grid," in Proc. Innovative Smart Grid Technol., Jan. 2010, pp. 1–6.
[30] H K. Nguyen, J. B. Song, and Z. Han, "Demand side management to reduce peak-to-average ratio using game theory in smart grid," in Proc. IEEE Conf. Comput. Commun. Workshops, Mar. 2012, pp. 91–96.