고객 정보의 개인 정보 보호를 고려한 멀티 마이크로그리드 시스템의 최적 운영

후세인 아크타르[*], 부이 반하이[*], 김학만[*]
[*]인천대학교 전기공학과
e-mail : hmkim@inu.ac.kr

Optimal Operation of Multi-Microgrid Systems Considering Privacy of Customer Information

Akhtar Hussain[*], Van-Hai Bui[*], Hak-Man Kim[*]
[*]Dept of Electrical Engineering, Incheon National University, Incheon, Korea

Abstract

Information security and preservation of customer's data privacy are key factors for further wide spread adoption of microgrid (MG) technology. However, strong coupling between the operation cost of multi-microgrid (MMG) system and privacy of customer data makes it more challenging. A nested energy management system (EMS) has been proposed in this paper. The surplus/shortage information from the inner level MGs is included in processing the optimal operation of outer level MGs. This type of optimization ensures a layered privacy-preservation to customer at each MG level. The proposed EMS architecture is a better trade-off architecture between the operation cost of the MMG system and customer privacy-preservation at each level of MG.

1. Introduction

Microgrids (MGs) have an enormous potential to bring various advantages in terms of flexibility, reliability, efficient usage of energy, integration of renewable energy sources, environmental protection, and many more [1]. However, various challenging issues related to information sharing like security of data, privacy-preservation of customers need to be addressed to get maximum benefit from this technology [1]. In order to minimize the effect of uncertainties, several MGs are interconnected to form a multi-microgrid (MMG) system [2].

Operators at energy management system (EMS) receive information from all the components of an MG, and schedules them in-accordance to the objective of the optimization algorithm. Such type of management might reveal the personal habits/behaviour of individual customers, the type of equipment being used by a specific customer and their time of usage, presence/absence of customer at home, and many more [3]. The customer privacy problem is different from the data security. Customer privacy may not be preserved, even if the data is transmitted over a secured link and is received securely at the EMS center [4].

Various researches have been carried out in the literature to address the issues related to information sharing and information processing of MG/MMG systems. Various security and privacy challenges faced by modern smart and microgrids have been analyzed by [5]. A framework for tackling the privacy issues in smart grids during the development process has been presented by [6]. Cyber-physical attack detection methodology for smart and microgrids has been proposed by [7], which is based on distributed agents. A privacy preserving energy scheduling algorithm for microgrids has been proposed by [1]. Decentralized EMS has been used by [8] for ensuring the privacy of customers in MGs.

Decentralized EMSs can ensure the customer privacy only when they are owned by a single owner. An MG with multiple loads; owned by different owners, may not want to share their personal information with their local EMS also. Secondly, operation cost for decentralized EMSs is very high as compared to the centralized EMS architectures. In order to create a tradeoff between the operation cost and preservation of customer privacy in MMGs, nested EMS architecture has been proposed in this paper. The privacy increases progressively from inner to outer MGs in nested EMS.

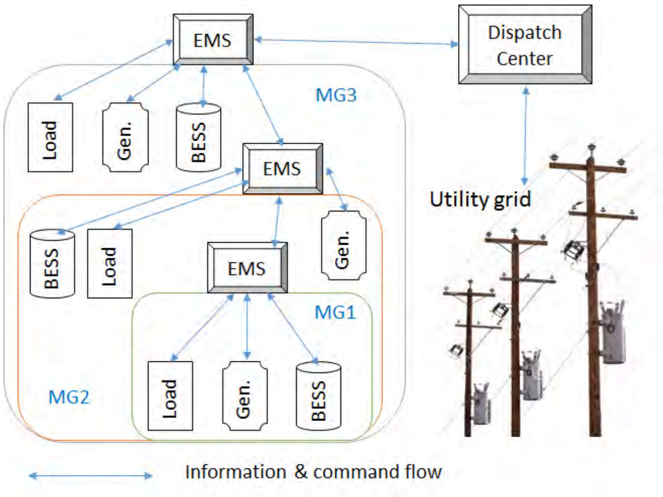

Fig. 1 Data flow in Nested EMS Architecture

2. Nested EMS Architecture

In nested EMS architecture, scheduling of resources is carried out sequentially from the innermost MG to the outermost MG. In this way, the surplus amount of inner MG serves as a source and shortage as a load for the outer level MG. Due to the inclusion of surplus/shortage information from the inner level MGs, the privacy of data increases and it becomes difficult for the outer level EMS operators to reveal the load pattern of inner level MG's customers. The information and command flow in the proposed nested EMS architecture is shown in Fig. 1.

It can be observed from Fig. 1 that each MG contains load, generation sources, and battery energy storage system (BESS). The innermost level MG (MG1) will do local optimization by using the market price signals (buying and selling prices). Interval-wise shortage/surplus will be calculate and informed to its adjacent upper level MG (MG2). MG2 will optimize its local resources while including the shortage/surplus information from MG1. All the intermediate MGs will do their optimization in a similar way. The outermost level MG (MG3) will decide the amount of power to be traded with the utility grid. The nesting of MGs is primarily logical, but it may be physical also in some cases, i .e. A campus microgrid with each department as an inner level MG.

There could be various loads with different ownerships in each MG level. In that case, the load owners may not want to share their load patterns directly with the local EMS. Various researches have been carried out to address this issue. The concept of sharing aggregated load with the local EMS has been proposed by[4]. The EMS may not need to know the loads of individual customers, rather an accumulated load information is enough for scheduling the resources. It has been suggested by [4] that encrypted values of individual loads will sent to the energy supplier. The energy supplier will not bale to decrypt individual values. The encrypted values will be summed to form an aggregated load data. Once the load aggregation has been performed, the energy supplier should be able to decrypt the aggregated data values. Details of this privacy-preservation technique can be found in [4]. This type of information sharing model can be incorporated in the proposed nested EMS architecture to share the information with the local EMS. The conceptual model for sharing information by using the proposed method of [4] is shown in Fig. 2.

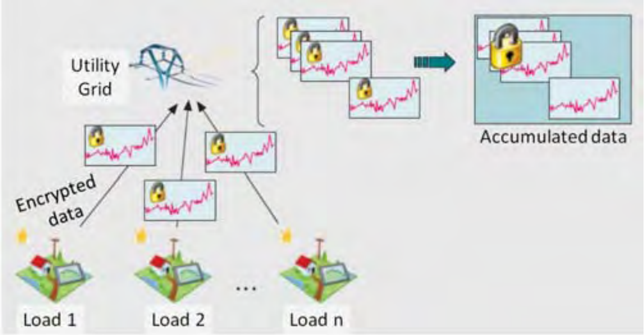

Fig. 2 Conceptual model for information sharing [4]

Another method for collecting data from smart meters in an aggregated way, while ensuring privacy of individual customers has been proposed by [3]. Firstly, each client node is assigned a unique integer ID between 0 and n, where n is the total number of nodes in the system. Utility's central server is responsible for this ID assignment [3]. Before sending the data signal, the sending node encrypts the data with its private key and signs it with the public key of receiver. Random gossip concept has been used for realizing the proposed information sharing model. The information flow for node 0 using the proposed model of [3] is shown in Fig. 3. It can be observed from Fig. 3 that every process sends and receives one message per round. The clutter can be reduced by omitting the extra messages. It can be observed from Fig. 3 that, at the second set of log n rounds produces a different pattern of communication than the first set, so nodes do not repeat gossip partners in the entire n rounds [3]. Similar type of process can also be incorporated in the proposed nested EMS architecture to ensure customer privacy while sharing data with local EMSs.

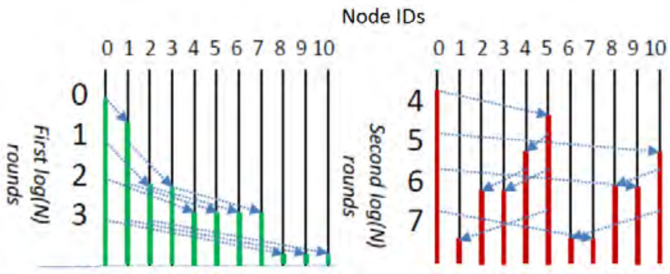

Fig. 3 Information flow for node 0 [3]

3. Problem formulation

A mixed integer linear programming (MILP) model has been used to realize the proposed nested EMS architecture-based scheduling of MMG systems. The objective of the model is to minimize the cost of MMG operation as shown in equation (1). The major constraints associated with this function are the load balancing, capacity of BESS, and generation limits of controllable distributed generators (CDGs) as shown in equations (2)-(5). The innermost MG has to optimize its own resources only, i .e. there is no lower level MG for MG at level 1. The outermost MG has to decide the amount of electricity to be traded with the utility grid. Therefore, buying and selling prices in equation (1) will be replaced by trading prices for all intermediate level MGs.

$$\mathbf{min}\ (\sum_{t=1}^{T} C_{MG}(t))$$

$$C_{MG}(t) = \sum_{i=1}^{I} (C^{e}_{CDG_i}(t).M^{e}_{CDG_i}(t)) + \sum_{i=1}^{I} (P^{e}_{BUY}(t).M^{e}_{BUY_i}(t)) - \sum_{i=1}^{I} (P^{e}_{SELL}(t).M^{e}_{SELL_i}(t)) \qquad (1)$$

Subject to:

$$M^{e}_{Load_i}(t) = M^{e}_{REN_i}(t) + M^{e}_{CDG_i}(t) + M^{e}_{BUY_i}(t) - M^{e}_{SELL_i}(t) + M^{e-}_{ESS_i}(t) - M^{e+}_{ESS_i}(t) \qquad (2)$$

$$\min[M^{e}_{CDG_i}] \le M^{e}_{CDG_i}(t) \le \max[M^{e}_{CDG_i}] \qquad (3)$$

$$\min[M^{e}_{ESS_i}] \le M^{e}_{ESS_i}(t) \le \max[M^{e}_{ESS_i}] \qquad (4)$$

$$BESS\ Constraints \qquad (5)$$

Where:

t : Identifier of the operation intervals.

T : Total number of the operation intervals.

i : Identifier of MGs.

I : Total number of the MGs in the MMG network.

C_{MG} : Cost of operation of MMG network.

$C^{e}_{CDG_i(t)}$: Production cost of the ith MG's CDG unit.

$P^{e}_{BUY}(t), P^{e}_{SELL}(t)$: Price for buying and selling electricity from/to utility grid or adjacent MGs respectively.

$M^{e}_{CDG_i}(t)$: Amount of electricity generated by CDG unit.

$M^{e}_{BUY}(t), M^{e}_{SELL}(t)$: Amount of electricity bought and sold from/to utility grid or adjacent MGs respectively.

$M^{e+}_{ESS}(t), M^{e-}_{ESS}(t)$: Amount of electricity charged and discharged to/from ESS of the ith level MG.

4. Conclusion

An architecture for optimal scheduling of MMGs while preserving customer privacy has been proposed in this paper. The proposed nested EMS architecture provides a better trade-off between the operation cost, and preservation of customer privacy in MMG systems. In order to ensure privacy for loads with different ownerships in an individual MG, existing information sharing mechanisms available in literature can be used.

Acknowledgements

This work was supported by the Power Generation & Electricity Delivery Core Technology Program of the Korea Institute of Energy Technology Evaluation and Planning (KETEP), granted financial resource from the Ministry of Trade, Industry & Energy, Republic of Korea. (No. 20141020402350)

References

[1] Wang, Z., Yang, K., & Wang, X. "Privacy-preserving energy scheduling in microgrid systems". IEEE Transactions on Smart Grid, 4(4), 1810-1820, 2013.

[2] Nguyen, D. T., & Le, L. B. "Optimal energy management for cooperative microgrids with renewable energy resources". In: IEEE International Conference on Smart Grid Communications, pp. 678-683, 2013..

[3] Birman, K., Jelasity, M., Kleinberg, R., & Tremel, E. "Building a secure and privacy-preserving smart grid". ACM SIGOPS Operating Systems Review, 49(1), 131-136, 2015.

[4] Marmol, F. G., Sorge, C., Ugus, O., & Pérez, G. M. "Do not snoop my habits: preserving privacy in the smart grid". IEEE Communications Magazine, 50(5), 166-172, 2012.

[5] McDaniel, P., & Laughlin, S. "Security and privacy challenges in the smart grid". IEEE Security & Privacy, (3), 75-77, 2009.

[6] Fhom, H. S., & Bayarou, K. M. "Towards a holistic privacy engineering approach for smart grid systems". In IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 234-241, 2011.

[7] Amin, S. M. "Smart grid security, privacy, and resilient architectures: Opportunities and challenges". In IEEE Power and Energy Society General Meeting, pp. 1-2, 2012.

[8] Shi, W., Xie, X., Chu, C. C., & Gadh, R. "A distributed optimal energy management strategy for microgrids". In IEEE International Conference on Smart Grid Communications, pp. 200-205, 2014.