Volume: 9 Issue: VII Month of publication: July 2021

DOI: https://doi.org/10.22214/ijraset.2021.36734

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

Management of Smart Grids: A Review

Kshitij Singh
NITTTR Bhopal,

Abstract: Electrical power grid has witnessed continuous changes over the past century but phenomenal developments are visible in the last two decades or so. The demand of 24x7x365 power supply, and development in socio-economic status of individuals and nations the demand of electrical power hence grid complexity is rising. Moreover shifting to renewables has opened a whole new can of worms. The conventional approach of grid management is unable to cater the needs of such a complex demand and supply needs. The present work is an approach addressing various modalities, modes of operation and management of smart grids. This includes demand side management in household and non-household scenarios, ICT and cyber security concerns.

Keywords: Smart-grids, management of power, DSM, cyber attack.

I. INTRODUCTION

The growth and development of countries is measured in energy consumption. Power grid plays an imperative role in translation of electrical power from generating station to the retail consumer. With emergence of 24x7 power supplies, sophisticated appliances in household, heavy machinery in industries, bulk of transport including railways, mass rapid transit(metro-trains) and now electric vehicles, the complexity is ever increasing. The conventional approach of installing more generation and distribution capabilities is inefficient in achieving such needs. This has led to emergence, development and deployment of smart grids across the globe. The present paper reflects contemporary works in management of smart grids.

II. CONCURRENT WORKS

Derui Ding *et. al,* carried out a survey on security and attack detection of cyber-physical systems. They discussed robustness, security, resilience and stability of various systems. They found that several existing tools based on system models are far from meeting CPS design requirements. CPSs may be subject to multiple attacks at the same time. An adaptive strategy compensating different types of attacks has not received adequate attention. A large perturbation on system states could be caused by injected false data while a detection rate may suffer from a slightly increase. They proposed future works on, communication protocols, fusion of attack detection and resilience control. [2]

Giovanna and Roberta have elaborated the various threat sources for smart electric grid. Voltage controlled ICT architecture has been discussed. They specifically addressed the need of tools and measures mitigating the risks originated by intrinsically vulnerable ICT infrastructures. Security analysis have been performed to illustrate the parameters and the outcome of the risk analysis and their links with the security requirements and ongoing standards in smart grids. Their Voltage Control architecture is obtained by the experimental activity. This will be serve as benchmark for accurate modelling and simulations to obtain performance indicators of the grid. [3]

Maria *et. al* investigated the impact that a cyber-attack on the AGC loop may have in the power system. They employed an abstract of the detailed power system model and carried out a feasibility analysis based on reachability and optimal control theory. This gave an insight whether there exist an attack pattern that can disturb the power system. They carried out simulations on the IEEE-118 bus network. There work illustrated necessity of devising an attack detection scheme. Swings on a generator can be disastrous, as protection relays will have false tripping which can cascade into greater troubles onto to grid. [4]

Christopher *et. al.* seek to protect embedded control software by enhancing it with checks to find execution of unauthorized code in addition to regular application code. Their attack scenario included a network packet obtained from sensor data by a spoofed or compromised node, which we implemented on a MIPS ISA platform. They exploited a common library routine to trigger a buffer over-flow, as embedded system components have limited computing capacity. There detection system comprises micro-timing information to real-time systems. Their focus was on detecting an attack or intrusion rather than tackling or avoiding it. This may make system intrusion information available in real time but still system vulnerability cannot be avoided, with their proposed method. [5]

Jinsub Kim *et. al* presented an adversary model of data attack on power system topology and state estimation. They addressed unobservable attacks, which can pass the bad data detection at the control center. In addition, they reviewed security measure to be followed by a control center with limited security resource. Feasibility conditions for unobservable attacks were presented, and cost-effective attack mechanisms were discussed.

However, such countermeasures are not sufficient. It is because intruder may still mislead the control center with a biased state estimate, after launching an observable attack. In order to eliminate the attack effect, the control center needs to remove the bias in the state estimate introduced by the attack. They claim that not much effort has been made in this direction; hence, the present work will work towards filling this void. [6]

Cost for data management for a smart grid is found by Sandeep et. al. in a work. Monitoring data generated from a smart grid, has become so complex that traditional storage and computational methods, cannot suffice. They carried out simulations on CloudSim to calculate the cost of storage of smart grid data on cloud. The cost of managing the smart grid data on the cloud having one datacenter is $202560, which is $2430720 annually, they found. Their work claims that cloud data storage has advantages such as maximum optimization of energy, transmission and distribution automation, reduction in losses, minimizing theft. Also, demand-response through efficient storing and processing of smart grid data was obtained. Nevertheless, a serious concern with such an approach is loss of owner’s control over its data. Operators of any section be it generation or retail, cannot address confidentiality, accountability and privacy issues that may be exploited by attackers. Designing intrusion defense, detection and prevention systems for smart grid will be the future research direction in the areas of smart grid. [7]

Zubair *et. al* studied various classes of attacks on a smart grid. They found that such an attack does not affect the consumers alone, rather, the utility providers' business as well. They had categorized all such attacks into five distinct classes, for ease in identification and analysis. Their work included descriptions of various SCADA security threats, smart meter-specific attacks, physical layer attack, data Injection and replay attacks. They expect extensive research work to ensure that the smart grid is highly secure against the adversarial threat. However, counter measures against all such attacks have not been rigorously dealt in the paper. [8]

Wenye *et. al.* introduced the communication architecture and security requirements, analyzed security vulnerabilities through case studies, and discussed attack prevention and defense approaches in the smart grid. They first describe the objectives and requirements of cyber security in the smart grid, review cyber attacks in electric power systems, and vulnerabilities. They carried out an evaluation of the existing solutions, including network and cryptographic countermeasures, by considering case studies and applications in the smart grid. There were references on existing cyber security solutions, in combination with communication architectures and protocols in the context of real-time and non-real time scenarios for the smart grid. [9]

Anwar & Mahmood, in their study found that the numbers of cyber attacks are increasing rapidly, and only Bad Data Detection (BDD) algorithms are used for data security in the state estimation. However, an adversary can attack the cyber-physical grid through any of the entry point of the cyber system and impact direly on the physical assets. Cyber security is very crucial for the reliable and secured operation of a smart grid. The protection frameworks of smart grid against component-wise, protocol-wise and topology wise cyber-attacks are reviewed in this paper. For enhanced smart grid reliability and security, intrusion detection algorithms should be placed throughout system. [10]

In *SEGRID*, researchers have developed a concept for a SCADA system that is able to operate correctly even under intrusions. The key idea is to replicate the SCADA system, allowing replicas to execute the same sequence of requests (e.g., operator commands) in such a way that, despite the failure of a fraction of the replicas, the remaining ones have the same state and ensure correctness of the offered services. However, such a solution is very costly, as many SCADA replicas will have to be installed/simulated. SEGRID project has considered physical redundancy, which allows traffic to be rapidly rerouted from the affected parts. They have tried to avoid DOS attack by limiting *ClientHello* handshake before a TLS. Comment or extensive investigation of DOS counter-action could be carried out, as this project has proprietary technology involved, which was not available. [11]

David Chaum carried out one of the earliest research work on using cryptography to deliver messages. He presented a solution in which messages were delivered unconditionally or cryptographically secure technique, depending on whether it is based on one-time-use keys or on public keys. It can be adapted to address efficiently a wide variety of practical considerations. His work established that if many people wish to participate in an untraceable communication system, hierarchical arrangements might offer further economy of keys. The mix-net approach relies on the security of a true public-key system by using public-key distribution to provide a computationally secure system. His solution to the dining cryptographers problem demonstrates that unconditional secrecy channels can be used to construct an unconditional sender-intractability channel. Efficient use of many other practical communication techniques requires participants to group output bits into blocks. For example, in high-capacity broadcast systems, such as coaxial cable, surface radio, or satellites, more efficient use of channel capacity is obtained by grouping a participant's contribution into a block about the size of a single message. This forms the basis of block chain, wherein the size of block transmitted or stored between two nodes, is directly proportional to the amount of data taken into consideration. Use of such communication techniques could require an increase in bandwidth of the order of the number of participants. Hence, more the number of participants in a block chain heavier is the block. [12]

In a report of US Dept. of Energy, states that 10% of all generation assets and 25% of distribution infrastructure are required less than 400 hours per year, roughly 5% of the time. While Smart Grid approaches cannot completely displace the need to build new infrastructure, they will enable new, more persistent forms of demand response that will succeed in deferring or avoiding some new form of it. Demand response has been chronic since 1990, due to grave overlook to transmission expansion, noted the report. Not to forget that these were the same issues faced during the blackouts in 2000, 2001 and 2012 here in India. [13]

Khaled *et. al* examined how common security attacks such as the Denial of Service (DoS) attack and the Man-in-the-Middle attack (MiM) can be exploited against smart power meters within a Local Area Network (LAN). In a controlled lab, experiments were conducted using DOS and ARP cache poisoning attacks. Their work demonstrate that the tested smart meters were vulnerable to the ARP cache poisoning attack. Since the generated fake, ARP request packets succeeded to corrupt their ARP caches preventing them from communicating properly with the associate server. Smart meters may crash and disconnect from the network, when the rate of a DOS attack traffic increases considerably. They found that the tested smart meters lack needed security functionalities, such as firewall based packet filtering and Intrusion Detection/Prevention mechanisms. Overall, there is very wide scope to in cyber sector of smart grid. [14]

In an article, Otuoze, A.O., *et al.* identified threats to SGs deployment are classified and discussed based on technical and non-technical sources of threats. They highlighted the security challenges, mitigation of already identified threats in smart grid. A suggestive framework for achieving a secured smart grid is also presented. This is based on threat tracing to the source, through input to the Reference Control and Support System (RCISS). However, this system cannot be used for all cases before operations. [15]

Walstrom Michael reports that the US Industrial Control Systems – Computer Emergency Response Team (US ICS-CERT) has published numerous reports on vulnerabilities in software and hardware that are used in India, including SCADA. In India, the processes are underway to create strong institutions for information sharing and attack mitigation through sectoral CERTs and ISACs but there is much left to do. The Bureau of Indian Standards has created some standards for SCADA systems. But in order to create a mechanism for statutory control over the implementation of such standards state level electricity regulatory commissions need to pass smart grid regulations. In addition, the Central Electricity Authority (CEA) must issue guidelines that will apply to utilities across the country. [16]

In a *study conducted by the World Bank*, institutional focus on integrating grid and off-grid power sectors is emphasized. A utility can effectively recover cost of power, and ensure supply reliability through better metering infrastructure that is nearly impossible to tamper with. It should also be responsible for providing higher-quality service, charging a fair price to consumers and providers alike, focusing more on customer service, involving rural communities more in the process of electrification, and developing systems and technical standards more appropriate for rural levels of demand. Hence, for monitoring the quality of service and connection information, supporting local generation and supply smart grid is envisaged. [17]

Henderson Michael *et. al.* illustrated examples of disparate approaches to solar power by various pilot project model implemented in the USA. These clearly indicate a need for regulators to address how to monetize the use of the grid. Additional approaches will need to address both energy use and distribution system infrastructure costs for the continued success and growth of solar power installations. They discussed about IEEE 1547, Standard for Interconnecting Distributed Resources with Electric Power Systems. This is a key industry reference for interconnection, as standards & guidelines, recommended that cover a comprehensive set of aspects pertaining to distributed generation integration. Their article predicts IoTs to be cost effective systems ensuring a high level of reliability, security, and availability, even in catastrophic situations, to improve capacity and reliability with increased automation. They expect addressing standards and cybersecurity concerns should remain a high priority along with tackling consumer privacy and data ownership implications. [18]. Many analytical algorithms such as–regression, classification and clustering algorithms have been used in power sector to mitigate various issues related to smart grid. For example, Mirowsk *et al.* [19] analyzed the multi-year meter data to forecast the load demand in smart grid using data analytics. The authors developed a demand forecasting scheme to improve the overall accuracy and then they compared their model with various state-of-the-art short-term load forecasting schemes. Authors in [20] analyzed meter data by integrating cumulative sum and shewhart algorithms to identify the meters with irregular usage patterns for revenue protection. The authors preprocessed the data by normalizing the effect of temperature, analyzing unusual long missing or zero data and other outliers, and then applied these algorithms for change detection. Jokar *et al.* [21] used data analytics for electricity theft detection. The authors analyzed the electricity consumption patterns of the users and classified the users as normal or malicious by using support vector machine (SVM). Han *et al.* [22] used SVM to analyze the response of consumers under the various time of use electricity pricing policies. This analysis can further help the utilities to decide the optimal pricing policy in varying load demand scenarios.

Zhu *et al.* [23] proposed an exploratory tool to visualize the consumer data and provided the capabilities to the end users in order to interact with the power systems based on this visualization. The developed data-driven tool also helped the users to visualize the power system's configurations at different levels which could be used to plan the electricity usage in their homes. Wang *et al.* [24] used a differential evolution based SVM classifier to put forth an electricity price forecasting framework. For this purpose, the authors combined random forest algorithm and relief-F algorithm for hybrid feature selection on the basis of grey correlation analysis to remove duplicate features. After this step, principal component analysis was applied to extract the important features; on the basis of which, a differential evolution based SVM classifier was trained to accurately forecast the electricity prices.

Haben *et al.* [25] analyzed the smart meter data to make clusters of consumers for understanding their load demand and behavior. The four major time periods were identified for which the data was analyzed to form relevant attributes for clustering. Then, a finite mixture model was employed to cluster 10 distinct behavior groups attributed to various customers based on their demand and variability. All these aforementioned schemes are summarized in Table 1 in terms of their application area and a brief description.

Table I
Various Data Analytical Techniques Used In Smart Grid

S.no.	Scheme	Description	Application area
1	Haben *et al.* [25]	Made clusters of consumers for understanding their load demand and behavior.	Understanding consumer behavior
2	Zhu *et al.* [23]	An exploratory tool to visualize the consumer data and capabilities to the end users to interact with the power systems.	Interactive visualization
3	Jokar *et al.* [21]	Analyzed the electricity consumption patterns of the users and classified the users as normal or malicious.	Theft detection
4	Han *et al.* [22]	Analyzed the response of consumers under various time of use electricity pricing policies.	Understanding consumer behavior
5	Mirowsk *et al.* [19]	Developed a demand forecasting scheme that improved the overall forecasting accuracy.	Load forecasting
6	Wang *et al.* [24]	Differential evolution based SVM classifier was developed to put forth an electricity price forecasting framework.	Price forecasting
7	Wu *et al.* [20]	Identified the smart meters with irregular usage patterns for revenue protection.	Revenue protection

Therefore, managing the energy supply in the homes can help to stabilize the load demand in the smart grid. Fig. 1 shows the energy consumption of various appliances in a typical home of U.S. [26]. It is necessary to understand the demand of these appliances in order to manage their load requirements in the smart homes. These loads should be managed in such a way that the overall burden on the grid is reduced without compromising the user comfort in smart homes. For this purpose, the energy management systems in homes can be deployed in two fashions, i.e., distributed and centralized. In distributed, each HEMS is responsible for the energy consumption in its smart home, while in centralized HEMS, it is responsible for the energy consumption in multiple homes. Many authors proposed various home energy management systems in this regard which are discussed as follows and the summary of which is given in Table II.

Table II

Energy Management In Household Scenarios: A Comparative Analysis

S. No.	Type of load	Technique used	Objective of scheme	Use of DERs	Nature
1.	Smart homes	Inclining block model[27]	Efficient appliance scheduling scheme for reducing the peak to average ratio.	No	Centralized
2.	Residential units	Shared energy storage[28]	Energy storage at consumer end for reducing the energy prices and to support low voltage distribution networks.	Yes	Centralized
3.	Smart homes	Linear programming[29]	Device scheduling based on intermittent power generated from RES and the uncertainties involved in the system.	Yes	Distributed
4.	Smart homes	MILP [30]	Optimal appliance scheduling for shaping the load profile on the basis of day ahead pricing information.	Yes	Distributed
5.	Smart homes	Branch and bound[31]	Energy management system for managing heating and air-conditioning devices for enhancing consumer comfort.	No	Distributed
6.	Residential commu-nity	Game theory[35]	Auction pricing between shared energy resources and residential units for joint ownership of energy.	Yes	Centralized
7.	Residential commu-nity	Theory of maxima and minima[37]	Minimize the operational cost of shared energy storage facilities using RES.	Yes	Centralized
8.	Smart homes	Dynamic priority[36]	Tackle the issue of intermittent nature of RES to power loads in smart homes.	Yes	Centralized
9.	Smart home	MINLP[32]	Minimize the energy use while maintaining the comfort lifestyle of the users.	Yes	Distributed
10.	Smart homes	Energy storage[33]	Optimized the energy consumption in homes based on price when it is more than a threshold limit.	Yes	Centralized

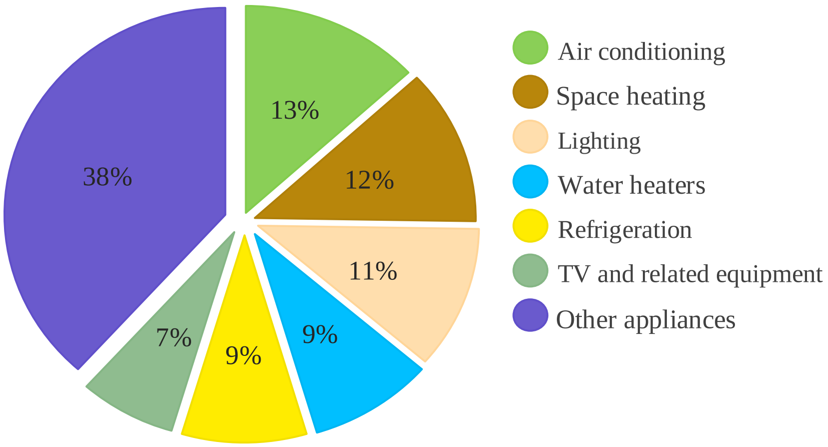

Figure 1: Energy usage in the homes of USA [26].

In centralized household energy management systems, Tushar *et al.* [35] proposed a game to control the joint ownership of energy between various residential units and the storage facility controller. An auction pricing concept was used to strike a deal between the stakeholders for determining the selling price of energy. In another similar scheme, use of Residential Energy System (RES) for the shared energy storage controller was devised by Tushar *et al.* [37] to reduce the operational cost. Byun *et al.* [36] presented a novel idea to make use of cloud-based home energy management system to tackle the intermittent issues of RES. This system assigned a real-time priority to a device in the home according to its type and present working status. The RES were then used to power the devices in accordance with their assigned priority.

Zhao *et al.* [27] proposed a system for efficient appliance scheduling in smart home so as to reduce the peak to average demand in smart grid. The authors combined real-time pricing and inclining block model for devising a power scheduling scheme which effectively reduced both the electricity cost and peak to average ratio. Chen *et al.* [28] presented an energy management system for managing the energy demand in buildings. This included the aggregated load demand of these building was matched with the desired load demand so as to maintain a balance between demand and supply. Authors Anvari *et al.* [29] proposed a system to reduce the energy usage in the homes to ensure that the thermal zone for the inhabitants remains within the comfortable limit. This was developed as a multi objective (MIN-LP)-based smart energy management system for home users to reduce their energy consumption while respecting the user comfort.

To support low voltage distribution networks when required, Wang *et al.* [30] proposed a strategy of shared energy storage at consumer end for reducing the overall energy prices in the network. The study aimed to catch an optimal point-of-balance between energy prices and demand response in residential homes so as to reduce the burden on the distribution network as well as increase the benefits of the consumers and network. Han *et al.* [31] designed a power line communication based distributed solution for controlling the energy consumption in smart homes. Using this information, the controller manages the usage of energy in such a way that it minimizes the total energy consumption cost in smart home. Shakeri *et al.* [32] proposed an energy management system which uses battery energy storage systems as well as managed the temperature of thermal appliances to ensure that the power consumption in a home was less than a certain set level. Their system used the utilities' pricing information to decide upon the storage of energy in batteries in off-peak hours and utilize the same to tackle peak loads.

In the distributed energy management system category, Chen *et al.* [33] considered the intermittent power generated from RES and the uncertainties involved in operating the devices while scheduling the devices in homes for the purpose of cost minimization. The initial schedule was prepared using linear programming while stochastic scheduling was used to handle the uncertainties. Paterakis *et al.* [34] modeled various appliances in the homes by using MILP technique to reduce household electricity bills. They achieved this by scheduling appliances day-ahead on the basis of features of each appliance and available pricing information. They presented an energy management system for managing the high power drawing loads of heating and HVAC (air conditioning) devices to reduce the energy consumption in homes.

III.CONCLUSIONS

The present work reviewed the concurrent literature about management of smart grids. Around 35 plus papers were classified and reviewed. This reflected various modalities, modes of operation and management of smart grids. The ICT, cyber security, demand side management in household and non-household scenarios were examined. Further studies can be done on modification and developing an entirely new model of smart grid based on the present work.

REFERENCES

[1] Duong Quoc Hung, Md Rakibuzzaman Shah and N. Mithulananthan "Smart Power Systems and Renewable Energy System Integration", Springer 2016

[2] Derui Ding, Qing-Long Han, Yang Xiang, Xiao hua Ge, Xian-Ming, Zhang "A survey on security control and attack detection for industrial cyber-physical systems", IEEE trans. on neuro computing, January 2018, DOI: 10.1016/j.neucom.2017.10.009.

[3] Giovanna Dondossola, Roberta Terruggia "Cyber Security of Smart Grid Communications: Risk Analysis and Experimental Testing", pp 169, Cyber Physical Systems Approach to Smart Electric Power Grid, Wiley 2017

[4] Maria Vrakopoulou, Peyman Mohajerin Esfahani, Kostas Margellos, John Lygeros, and Goran Andersson "Cyber-Attacks in the Automatic Generation Control", Springer, Berlin, Heidelberg, DOI: https://doi.org/10.1007/978-3-662-45928-7_11

[5] Christopher Zimmer, Balasubramany Bhat, Frank Mueller, and Sibin Mohan "Intrusion Detection for CPS Real-Time Controllers" In: Khaitan S., McCalley J., Liu C. (eds) Cyber Physical Systems Approach to Smart Electric Power Grid. Power Systems. Springer, Berlin, Heidelberg DOI: https://doi.org/10.1007/978-3-662-45928-7_12

[6] Jinsub Kim and Lang Tong "Against Data Attacks on Smart Grid Operations: Attack Mechanisms and Security Measures", pp 359-383 Springer, Berlin, 2018

[7] Sandeep Mehmi "Economic Viability of Smart Grid Cloud in India", Springer, Berlin. DOI: https://doi.org/10.1007/978-3-662-45928-7_13

[8] Zubair A. Baig and Abdul-Raoof Amoudi "An Analysis of Smart Grid Attacks and Counter measures", Journal of Communications Vol. 8, No. 8, August 2013

[9] Wenye Wang, Zhuo Lu,"Cyber Security in the Smart Grid: Survey and Challenges",Computer Networks Volume 57, Issue 5, 7 April 2013, Pages 1344-1371 Elsevier https://doi.org/10.1016/j.comnet.2012.12.017

[10] A. Anwar, A. Mahmood, "Cyber security of smart grid infrastructure", The State of the Art in Intrusion Prevention and Detection, CRC Press, Taylor & Francis Group, USA, January 2014, pp. 449-472.

[11] The European Commission "Security for smart electricity grids- A white paper", SEGRID Project, EU FP7 SEGRID project

[12] David Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability", Journal of Cryptology 1(1), 1988, pp. 65-75.

[13] U.S. Department of Energy, "The Smart Grid: An introduction" No. DE-AC26 04NT41817 Subtask 560.01.04

[14] Khaled Shuaiba , Zouheir Trabelsi , Mohammad Abed-Hafez , Ahmed Gaouda , and Mahmoud Alahmad, "Resiliency of Smart Power Meters to Common Security Attacks", , 6th International Conference on Ambient Systems, Networks and Technologies (ANT 2015) Elsevier 2015 doi: 10.1016/j.procs.2015.05.049

[15] Otuoze, A.O., et al., "Smart grids security challenges: Classification by sources of threats". J. Electr. Syst. Inform. Technol. (2017),https://dx.doi.org/10.1016/j.jesit.2018.01.001

[16] Michael Walstrom, "India's Electrical Smart Grid: Institutional and Regulatory Cybersecurity Challenges", - The Henry M. Jackson School of International Affairs

[17] A World Bank Study "Power for All- Electricity access challenge in India", http://dx.doi.org/10.1596/978-1-4648-0341-3

[18] Michael I. Henderson, Damir Novosel, and Mariesa L. Crow, "Electric Power Grid Modernization Trends, Challenges, and Opportunities", IEEE Power & Energy Society November 2017

[19] P. Mirowski, T. Kam Ho, and C.-N. Yu, "Demand forecasting in smart grids," Bell Labs technical journal, vol. 18, no. 4, pp. 135–158, 2014.

[20] Z. Wu, T. Zhao, and X. Shen, "Smart grid meter analytics for revenue protection," in International Conference on Power System Technology (POWERCON), 2014, pp. 782–787.

[21] P. Jokar, N. Arianpu, and V. Leung, "Intrusion detection in advanced metering infrastructure based on consumption pattern," in IEEE International Conference on Communications (ICC), 2013, pp. 4472–4476.

[22] W. Han, L. Zhange, and J. Liu, "Demand response model for characteristics analysis of electricity consumers," in IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia), 2012, pp. 1–5.

[23] J. Zhu, E. Zhuang, C. Ivanov, and Z. Yao, "A data-driven approach to interactive visualization of power systems," IEEE Transactions on Power Systems, vol. 26, no. 4, pp. 2539–2546.

[24] K. Wang, C. Xu, Y. Zhang, S. Guo, and A. Zomaya, "Robust big data analytics for electricity price forecasting in the smart grid," IEEE Transactions on Big Data, 2017.

[25] S. Haben, C. Singleton, and P. Grindrod, "Analysis and clustering of residential customers energy behavioral demand using smart meter data," IEEE Transactions on Smart Grid, vol. 7, no. 1, pp. 136–144, 2016.

[26] U.S. Energy Information Administration, Annual Energy Outlook 2016, Table A4.

[27] Z. Zhao, W. C. Lee, Y. Shin, and K.-B. Song, "An optimal power scheduling method for demand response in home energy management system," IEEE Transactions on Smart Grid, vol. 4, no. 3, pp. 1391–1400, 2013.

[28] Z. Wang, C. Gu, F. Li, P. Bale, and H. Sun, "Active demand response using shared energy storage for household energy management," IEEE Transactions on Smart Grid, vol. 4, no. 4, pp. 1888–1897, 2013. BIBLIOGRAPHY 175

[29] M. Shakeri, M. Shayestegan, H. Abunima, S. S. Reza, M. Akhtaruzzaman, A. Alamoud, K. Sopian, and N. Amin, "An intelligent system architecture in home energy management systems (HEMS) for efficient demand response in smart grid," Energy and Buildings, vol. 138, pp. 154–164, 2017. [104] X. Chen, T. Wei, and S. Hu, "Uncertainty-aware household appliance scheduling considering dynamic electricity pricing in smart home," IEEE Transactions on Smart Grid, vol. 4, no. 2, pp. 932–941, 2013.

[30] NG. Paterakis, O. Erdinc, A. G. Bakirtzis, and J. P. Catal˜ao, "Optimal household appliances scheduling under day-ahead pricing and load-shaping demand response strategies," IEEE Transactions on Industrial Informatics, vol. 11, no. 6, pp. 1509–1519, 2015

[31] Jo, S. Kim, and S.-K. Joo, "Smart heating and air conditioning scheduling method incorporating customer convenience for home energy management system," IEEE Transactions on Consumer Electronics, vol. 59, no. 2, pp. 316– 322, 2013.

[32] J. Wang, C. Chen, and S. Kishore, "A distributed direct load control approach for large-scale residential demand response," IEEE Transactions on Power Systems, vol. 29, no. 5, pp. 2219–2228, 2014.

[33] C.-S. Choi, J. Han, W.-K. Park, I. Lee, and S.-H. Kim, "Smart home energy management system including renewable energy based on ZigBee and PLC," IEEE Transactions on Consumer Electronics, vol. 60, no. 2, pp. 198–202, 2014.

[34] H. Monsef, and A. Rahimi-Kian, "Optimal smart home energy management considering energy saving and a comfortable lifestyle," IEEE Transactions on Smart Grid, vol. 6, no. 1, pp. 324–332, 2015

[35] W. Tushar, B. Chai, C. Yuen, S. Huang, D. B. Smith, H. V. Poor, and Z. Yang, "Energy storage sharing in smart grid: A modified auction-based approach," IEEE Transactions on Smart Grid, vol. 7, no. 3, pp. 1462–1475, 2016.

[36] J. Byun, I. Hong, and S. Park, "Intelligent cloud home energy management system using household appliance priority based scheduling based on prediction of renewable energy capability," IEEE Transactions on Consumer Electronics, vol. 58, no. 4, 2012.

[37] W. Tushar, J. A. Zhang, C. Yuen, D. B. Smith, and N. U. Hassan, "Management of renewable energy for a shared facility controller in smart grid," IEEE Access, vol. 4, pp. 4269–4281, 2016.