

Communication challenges in Smart Grid

Eleftherios Tsampasis ^a, Dimitrios Bargiotas, Charalambos Elias, Lambros Sarakis

Technological Educational Institute of Sterea Ellada, Electrical Engineering Department, Psachna 34400, Greece

Abstract. Smart grid is not a system, application, network, or single device. It is no surprise that there is no unique definition of the Smart Grid (SG): ABB says is an evolved grid system that manages electricity demand in a sustainable, reliable and economic manner, built on advanced infrastructure and tuned to facilitate the integration of all involved elements. However, the definitions from authoritative organizations follow a common theme: Smart grids utilize information and communication technologies to manage the energy distribution and optimize the transmission from suppliers to consumers and vice versa. Capacitor banks and reclosers need the intelligent control to appropriately adapt the supply to the demand. In this paper, we discuss communication systems and the requirements they have to fulfill in the smart grid applications.

1 Introduction

A smart grid (SG), also called intelligent grid, intelligrid, futuregrid, intergrid, or smart electrical/power grid, is an enhancement of the 20th century power grid. The traditional power grids (as shown in Figure 1) are generally used to carry power from a few central generators to a large number of users or customers.

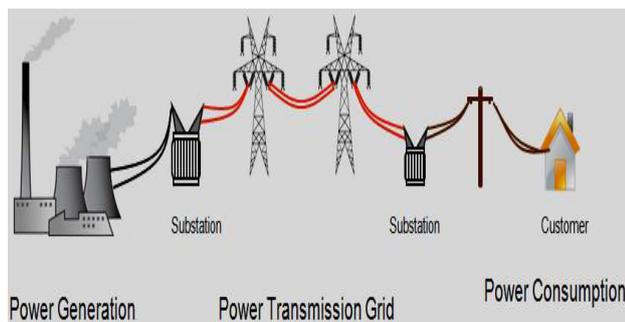


Figure 1. Example of the traditional power grid

In contrast, the SG (an example of which is shown in Figure 2) uses two-way flows of electricity and information to create an automated and distributed advanced energy delivery network utilizing modern information technologies and thus it is capable of delivering power in more efficient ways and responding to widely ranging conditions and events. For example, once a medium voltage transformer failure event occurs in the distribution grid, the SG may automatically change the power flow and recover the power delivery service immediately.



Figure 2. Example of smart grid

Electric power systems are very complex physical networks. According to NIST's conceptual model [1] [2], the Smart Grid consists of seven logical domains: Bulk Generation, Transmission, Distribution, Customer, Markets, Service Provider and Operations. The first four feature the two way power and information flows. The last three feature information collection and power management in the Smart Grid.

A Smart Grid is an upgraded energy grid which enables sensing, monitoring, communication and control of middle and low voltage grids. Against this background, the communication infrastructure must address the following:

- Match the technical requirements.
- The technology must be securing a stable environment to attract investments in Smart Grid.
- The costs to achieve the required coverage, installation and operation should be low.

The remainder of the paper is organized as follows. Section 2 discusses various communications technologies available for smart grids while section 3 describes the communication requirements in smart grids. Finally Section 4 concludes the paper.

^a Corresponding author: etsampasis@teiste.gr

2 Communication technologies available for smart grids

The communication is one of the most critical elements that enable smart grid applications. Different communication technologies supported by two main communications media, wireless and wired, can be used for data transfer between smart meters and electric utilities. The information flow can be considered as the concatenation of a flow from the sensor to the smart meters and of another flow between smart meters and the utility's data centers. L. Wenpeng suggests in [3], the first data flow can be accomplished through wireless communications or power line communication, such as ZigBee, and Z-wave; both technologies are ideal for home-area networks (HANs).

A smart metering communication system [4] consists of the following components:

- Smart meter which is a two-way communicating device that records consumption of electric energy.
- Home Area Network (HAN) which is an information and communication network formed by appliances and devices within a home to support different distributed applications
- Neighborhood Area Network (NAN) that collects data from multiple HANs and deliver the data to a data concentrator; and finally
- Wide Area Network (WAN) which is the data transport network that carries metering data to central control centers.

Based on the data rate and coverage range, smart grid applications are grouped by their data rate and coverage range required for their successful deployment. We now turn our attention to the above mentioned technologies.

2.1 ZigBee

ZigBee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios. The technology defined by the ZigBee specification is intended to be simpler and less expensive than other wireless personal area networks (WPANs), such as Bluetooth or Wi-Fi. Applications include wireless light switches, electrical meters with in-home-displays, traffic management systems, and other consumer and industrial equipment that requires short-range low-rate wireless data transfer.

2.2 Wireless Mesh network (WMN)

In this network, nodes are comprised of mesh routers and mesh clients. Each node operates not only as a host but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations. A WMN is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves (creating, in effect, an ad hoc network).

2.3 Powerline Communication

Powerline communications (PLC) uses the existing power line infrastructure to transmit high-speed (2–3 Mb/s) data signals from one device to the other for communication purposes. This allows utility companies to use a single infrastructure for power and data transmission. As a result of this, PLC systems have been suggested as a cost-effective and painless solution to grid communication needs. PLC technologies utilize existing power cables for information exchange [5]. The majority of automatic meter readings deployments around the world are using PLC technologies for transmitting metering data. However, the use of power lines to provide reliable data transmissions has to face a number of technical challenges due to the signal propagation characteristics of typical power cables, such as high signal attenuation, disruptive interference from other power signals, including nearby electric appliances or external electromagnetic sources [6]. It must be noted that there are two major categories of PLC technologies that operate in different bands and have different capabilities. More specifically, there are narrowband PLC (NB-PLC) technologies that operate in transmission frequencies of up to 500 kHz; on the other category, broadband PLC (BB-PLC) technologies, target significantly higher bandwidth performance than the first one (up to 200 Mbps).

2.4 Digital Subscriber Lines

Digital Subscriber Line (DSL) provides digital data transmission over the telephone lines. DSL connections are dedicated point-to-point circuits which are always connected and need no dial up. The phone line is used for transmitting both the voice and Internet data requests while keeping them separate. A DSL modem hooks up the computer to the phone line on the subscriber's side. A DSL access multiplexer on the service provider's side takes requests from multiple users and sends them through a single connection to the internet. There are different types of DSL services ranging in speeds from 16 kbps to 52 Mbps.

2.5 Cellular Network Communication

A cellular network is a radio network distributed over land through cells where each cell includes a fixed location transceiver known as base station. These cells together provide radio coverage over larger geographical areas. These networks can be a good option for communicating between smart meters and the utility and between far nodes.

Cellular network solutions also enable smart metering deployments spreading to a wide area environment. 2G, 3G, WiMAX, and LTE are the cellular communication technologies available to utilities for smart metering deployments.

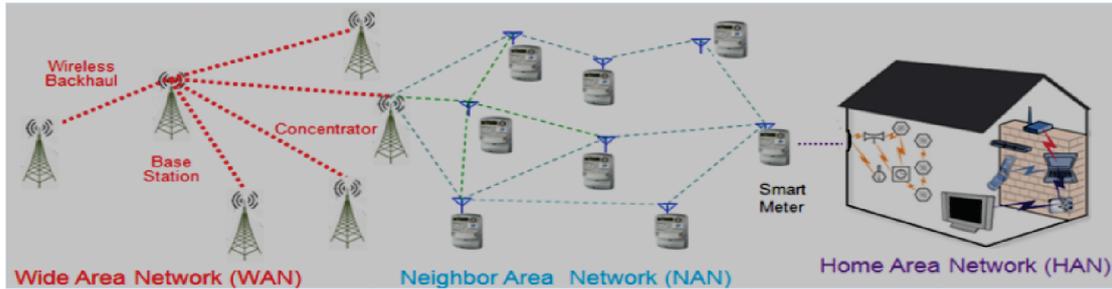


Figure 3. Communications Layer

3 Communication requirements in smart grids

3.1 High Level Security Requirements

Electric Power Research Institute (EPRI) states, one of the biggest challenges facing the smart grid deployment is related to cyber security of the systems [1]. Cyber security is a critical issue due to their increasing potential of cyber-attacks [7], and incidents against this critical sector as it becomes more and more interconnected. Cyber security must address not only deliberate attacks, such as industrial espionage, or terrorists, but inadvertent compromises of the information infrastructure due to human errors, equipment failures, and natural disasters.

3.2 Quality- of- Service related requirements (QoS)

The communication between the power supplier and power customers is a key issue of the smart grid it is necessary to guarantee Quality of Service (QoS) [6] for the communication and networking technology in all of the stages of the Smart Grid, ranging from power generation, transmission, distribution, to the customer applications. How to ensure the monitoring data, emergency response and control command can be reliably delivered within required time frame, but would not be affected by the number of cell phone customers and their data traffic. To tackle this challenge, Wei Sun [8] proposes to use a private wireless network dedicated for power distribution system monitoring.

3.3 Privacy

Privacy becomes an important concern when collecting energy usage data with the deployment and adoption of smart grid technologies. To protect such sensitive information it is imperative that privacy protection mechanisms be used to protect the privacy of smart grid users. Electricity usage information stored at the smart meter and distributed thereafter acts as an information-rich side channel, exposing customers' behaviors and habits. History has shown that where economic or

political motives alignment, behavioral data mining techniques will evolve quickly to match the desires of those who will take advantage of this information [9].

The definition of privacy tends to vary among different societies and cultures and as such, there is no clear list of categories of privacy that can be applicable for all. However, four major types of privacy are generally recognized

- Personal Privacy: this includes mainly body privacy and territorial privacy
- Information Privacy: this kind of privacy is mainly related to passing of information over various media and could also be called communications privacy
- Organization Privacy: this includes the confidential information about an organization such as loss and profit statistics, current trend in the market, future products, potential customers, transaction details etc.
- Spiritual and Intellectual Privacy: this kind of privacy includes a person's spiritual nature, of his feelings and his intellect [10].

3.4 Integrity

Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity is the main aspect for computer and network security design [11]. By nature, it is still crucial for securing the smart grid refers to preventing undetected modification of information by unauthorized persons or systems. For smart grid communication systems, this applies to information such as product recipes, sensor values, or control commands. This objective includes defense against information modification via message injection, message replay, and message delay on the network. Violation of integrity may cause safety issues, that is, equipment or people may be harmed. The risk of attacks targeting data integrity in the power networks is indeed real. An example is in the article [12], which proposed attack, called false data injection attack, against the state estimation in the power grid. Confidentiality is the concealment of information or resources. The need for keeping information secret arises from the use of computers in sensitive fields such as smart grid, government and industry integrity and

confidentiality are two, main aspects for computer and network security design

3.5 Reliability and Availability

System reliability has become one of the primary requirements for power utilities. Growing old power infrastructure, peak demand and increasing energy consumption are some of the causes that create unreliability issues for the power grid [7], [11]. Exploiting the potential of the secure and modern communication protocols, the communication and information technologies faster and more robust control devices, embedded intelligent devices (IEDs) for the entire grid from substation and feeder to customer resources, will significantly strengthen the system reliability and robustness. Availability is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all. Availability refers to the ability to use the information or resource desired For smart grid systems availability refers to all the information technology (IT) elements of the plant such as control systems, safety systems, operator workstations, engineering workstations, manufacturing execution systems, as well as the communication systems between these elements and to the outside world. Wireless technologies with constrained bandwidth and security and reduced installation costs can be a good choice for large-scale smart grid deployments. Then again, wired technologies with increased capacity, reliability and security can be costly [6]. To provide system reliability, robustness and availability simultaneously with appropriate installation costs, a hybrid communication technology combined with wired and wireless solutions can be an ideal solution

4 Conclusions

Cyber security and privacy issues in the smart grid are new areas in the fields of power industry, electrical engineering, and computer science. More in-depth research is required to develop such a promising power grid in the near future. At this paper, we made a brief description in communication technologies which are available for the operation in Smart Grids and safety requirements that need to be met to ensure the reliable operation of next generation electric power system. The success of future smart grid depends heavily on the communication infrastructure, devices, and enabling services and software. As communication is an underpinning technology for this huge development, we envisage that smart grids will be an exciting research area for communication engineers for many years to come.

References

1. Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI, Jun. 17, 2009 [Online]. Available:

- http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf
2. M. Bauer, W. Plappert, C. Wang, K. Dostert, Packet-oriented communication protocols for smart grid services over low-speed plc, in: Proc. of IEEEISPLC'09, 2009, pp. 89–94.
3. L. Wenpeng, D. Sharp, and S. Lancashire, “Smart grid communication network capacity planning for power utilities,” in Proc. IEEE PES, Transmission Distrib. Conf. Expo., Apr. 19–22, 2010, pp. 1–4.
4. G. Kalogridis, C. Efthymiou, S.Z. Denic, T.A. Lewis, and R. Cepeda, “Privacy for smart meters: towards undetectable appliance load signatures,” in: The First IEEE International Conference on Smart Grid Communications (Smart Grid Comm), Gaithersburg, MD, Oct. 2010, pp. 232-237.
5. S. Galli, A. Scaglione, Z. Wang, For the grid and through the grid: the role of power line communications in the smart grid, Proceedings of the IEEE 99 (6) (2011) 998–1027.
6. Vehbi C. Güngör, Member, IEEE, Dilan Sahin, Taskin Kocak, Salih Ergüt, Concettina Buccella, Senior Member, IEEE, Carlo Cecati, Fellow, IEEE, and Gerhard P. Hancke, Senior Member, IEEE. Smart Grid Technologies: Communication Technologies and Standards.
7. K. Moslehi and R. Kumar, “Smart grid—A reliability perspective,” Innovative Smart Grid Technologies (ISGT), pp. 1–8, Jan. 19–21, 2010.
8. Wei Sun*†, Xiaojing Yuan†, Jianping Wang*, Dong Han† and Chongwei Zhang Quality of Service Networking for Smart Grid Distribution Monitoring
9. P. McDaniel and S. McLaughlin, “Security and Privacy Challenges in the Smart Grid,” in Security & Privacy, IEEE, vol.7, no.3, pp.75-77, May-June 2009.
10. S. Zeadally, A. Pathan, C. Alcaraz, and M. Badra, “Towards Privacy Protection in Smart Grid”, Wireless Personal Communications, vol. 73, pp. 23-50, 2012.
11. Ye Yan, Yi Qian, Hamid Sharif and David Tipper “A Survey on Cyber Security for Smart Grid Communications”.
12. Q.Yang, J. “Afor distributed control of power distribution networks,” IEEE Trans. Barria, and T. C. Green, “Communication infrastructures Ind. Inform., vol. 7, no. 2, pp. 316–327, May 2011.