Review of System Architecture and Security Issues for Smart Grid

Sunguk Lee

Research Institute of Industrial Science and Technology
Pohang,Gyeongbuk, South Korea
Sunguk@rist.re.kr

Abstract

The smart grid has received high interest for improving efficiency and reliability of power system. It adopts Information and System Technology for this purpose and several technologies are considered as system architecture of the smart grid. Consequently security issues of system should be considered for the smart grid. In this paper system architecture for the smart grid is presented. Requirements of security and solutions for cyber attack in the smart grid also discussed.

Keywords: *Security, Authentication, Intrusion Detection, Power line communication*

1. Introduction

The Smart grid [1, 2] is an intelligent next-generation power system that adopts Information and Communication Technology (ICT) to improve efficiency and reliability of power system. Most of power systems use fossil fuel like as oil, coal and gas as energy resources. However fossil fuel is consumed rapidly and it seems to be run out in the near future. Also emission of carbon dioxide (Co_2) by fossil fuel is big threat to protect environment. Renewable energy resource is considered as attractive energy resource for replacing fossil fuel. Wind and solar are promising renewable energy resources however these resources product electric power intermittently. Hence new power system is necessary to cope with these challenges.

The smart grid is an ideal way for integrating renewable resources to current power grid and ideal way for customer participation in the electricity enterprise [3]. The smart grid has distinct components and functions comparing with current power grid as below:

- Real time communication infrastructure
- Monitoring and Management system
- Advanced Metering Infrastructure(AMI)
- Energy Storage System
- Renewable Energy Generator

The Energy Storage System can improve efficiency and reliability of power system with renewable energy generation. The smart grid control center may have functions of monitoring and interaction with generators and devices in customer side. The fast and reliable bi-directional communication infrastructure may play important role for real time monitoring and managing of smart grid system.

Generally the Advanced Metering Infrastructure (AMI) [2] consists of bi-directional communication infra and smart meter. The smart meter gathers the metering data at customer side and sends this data to intermediate node called "local concentrator" to central control center. The AMI provides several services as follows.

- Dynamic Pricing
- Demand Response
- System monitoring
- Power Quality Measurement

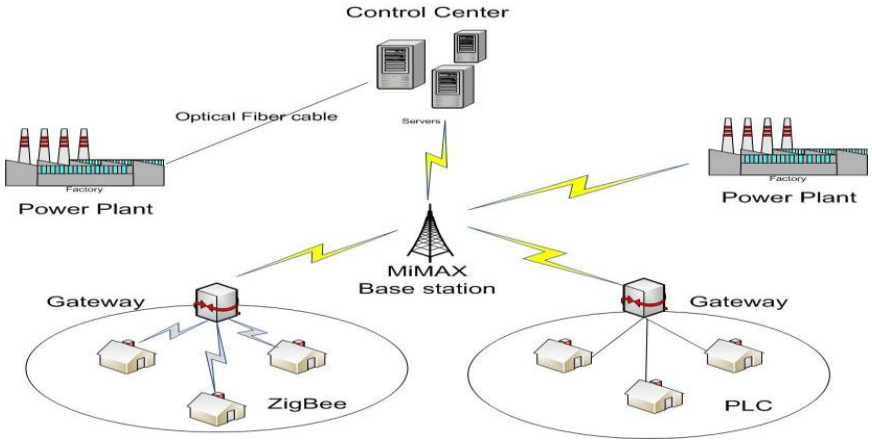

Figure 1. Communication Infrastructure for Smart Grid

Figure 1 shows an example of communication architecture for the smart grid. The control center receives real time status information from subsystem and smart meters. The control center plays vital roles of monitoring and managing the power system. Commonly Supervisory Control And Data Acquisition (SCADA) system [4] is used for these purpose in the industrial field.

The electrical power generators and subsystems of the smart grid may be distributed geographically within large area. Therefore combination of several communication technologies is used to cover the whole smart grid area. As shown in the figure 1 communication infrastructure of smart grid is composition of 2 kinds of communication network: Wide Area Network (WAN) and Local Area Network (LAN). The critical monitoring and managing messages are exchanged between central center and subsystem through communication network. The smart grid covers geographically large scaled area therefore vulnerability to cyber attack is increased. Also the latency requirement for monitoring and operating message should be considered for selecting communication infrastructure for the smart grid [5].

The remainder of the paper is organized as follows. In the section 2 communication technologies for smart grid is explained. In the next section security issues are described. Finally section 4 concludes this paper.

2. Communication Infrastructure for Smart Grid

The communication infrastructure should provide continuous connectivity between control center and all units in the smart grid. Also a huge amount of data from all application in the smart grid is generated continuously therefore requirement of bandwidth and latency should be met by communication channel.

The information flow of the smart grid can be divided in 2 parts. The first information flow is between smart meters and sensors. For this data exchange LAN technology is used. The second data flow is between smart meters and central control center. In some case local concentrator relays data from smart meter to control center. WAN is used for this data flow.

2.1. Wide Area Network for Smart Grid

The WAN connects several subsystem and smart meters with control center which is far from subsystem and customer side network. Power Line Communication (PLC) uses power cable as a communication medium therefore new cable deployment is not needed. However low data rate and significant signal attenuation limit its usage for WAN. The dedicated copper or fiber optic cable support reliable and secure communication however it is very costly to deploy new cable for long distance. Cellular communication like as WiMAX, 3G and LTE is also considered for WAN in the smart grid. Cellular network already exist so cost for building infrastructure is not needed. However user should pay licensing /subscription fee. Also the shared medium can cause congestion and low performance at sometimes. Table 1 shows technologies of WAN for the smart grid.

Table 1. Technologies of WAN for the smart grid

Technology	Max. Data Rate	Coverage range	Frequency Band	Band Licensed
GSM	800 Kbps	1-10 Km	900-1800MHz	Licensed
3G	2 Mbps	1-10Km	1.92-1.98GHz, 2.11-2.17 GHz	Licensed
WiMAX	75 Mbps	1-5 Km	2.5,3.5,5.8 GHz	Licensed
PLC	2-3 Mbps	1-3 Km	1-30MHz	Free

2.2. Local Area Network for Smart Grid

For communication between smart meters and electric load several kinds of communication such as Home Area Network (HAN) and Building Area Network (BAN) are used in the smart grid. The power line communication (PLC), Ethernet and several wireless technologies like as Bluetooth, Wi-Fi (IEEE802.11) and Zigbee (IEEE802.15.4) are considered for HAN or BAN in the smart grid.

Ethernet can support high data rate and more secure communication than other technologies. However the Ethernet need costly cable deployment and has less flexibility than wireless technologies. The PLC can provide high data rate and secured communication using existing power cable for short range communication. The PLC can be good communication choice between electric devices and smart meter in home or building environment. ZigBee also can be ideal communication technology for AMI with acceptable data rate, easy implementation, low bandwidth requirement and mobility. Wi-Fi provide high data rate but it consumes more electric power than other

wireless technology. Bluetooth is limited for implementing HAN because of its limited capability. Table 2 describes characteristics of LAN for the smart grid.

Table 2. Technologies of LAN for the smart grid

Technology	Data Rate	Coverage range	Band Licensed	Cost
Ethernet	10-100 Mbps	100 M	Free	High
PLC	10-100 Mbps	10-10M	Free	Medium
Wi-Fi	5-100 Mbps	30-100M	Free	Medium
ZigBee	0.02-0.2 Mbps	10-75M	Free	Low
Bluetooth	0.7-2.1 Mbps	10-50M	Free	Low

3. Security Issues for Communication Infrastructure in the Smart Grid

The communication network in the smart grid takes charge of exchanging information among distributed power device including generators for managing power system. Therefore reliability and security of communication infrastructure has direct relation with those of power system. The Internet Protocol (IP) is widely used communication protocol. The smart grid is also expected to adopt IP and this may give several benefits to the smart grid [6]. However this has vulnerability to cyber attacks like as DoS attack. The smart grid may consist of several kinds of communication networks. Therefore comprehensive security solution to protect cyber attacks is essential for communication infrastructure for the Smart Grid.

3.1. Security Requirement for Communication

The essential security requirements for communication are availability, confidentiality, integrity and authenticity [1, 2, 7].

- Availability

  The communication network should guarantee the delivery of data at any time. The network has to survive against possible cyber attacks and failure. A denial of service (DoS) attack is to disturb or block the data transmission by consuming significant amount of communication resources with useless data. To protect the DoS attack system should have filtering function to discriminate the suspicious traffic.

- Confidentiality

  The information delivered through communication network should be confidential. The information like as user account is very sensitive information to be kept in secret from unauthorized parties. In wired network eavesdropper should be in the communication path. However wireless network can be suffer from eavesdrop attack at multiple point within transmission range. Encryption with a secret key can support confidentiality of information.

- Integrity

  The data from sender must be not altered during transmission by attacker. Malicious attacker can add or manipulate the information. If the information concern with measurements, monitoring and operating of system is altered by attacker it can cause a wrong operation and malfunction of management system of the smart grid.

- Authenticity

  Authentication is used for identifying another node and source of data in the communication network. Malicious data can be injected in the network by attacker to interrupt the system. Therefore receiver has to know that the information especially for managing and control of smart grid is from correct sender.

3.2. Solutions for cyber attacks

To achieve privacy information or injecting malicious data in the communication network attacker must intrude network firstly through a legal node with authentication by any means. Strong authentication protocol is required to guarantee secure communication in the smart grid however this protocol has to have minimum communication overhead and computation cost considering limited resource of power devices like smart meter [7]. Cryptographic algorithm can be used to keep data privacy. The sender encrypts message with encryption key and transmits it to receiver. Then receiver can decrypt received message with decryption key. Intrude detection and firewall also can enhance security of smart grid communication [8].

4. Conclusion

The smart grid is an intelligent power system to improve efficiency and reliability with automated control, sensing and measurement and energy management based on data of generation and demand of power. The communication infrastructure plays a vital role for efficient energy management by supporting continuous interaction among members in the smart grid.

In this paper communication infrastructure and its security issues have been discussed. Conventional wired communication technologies can support high data rate and secured communication however costly new cable deployment is essential. Therefore PLC which used existing power cable and Zigbee can be ideal communication technologies for LAN in the smart grid. Cellular network like as MiMAX and LTE can support wide area communication between control centre and subsystems. Security requirement and solutions for cyber attack are also discussed in the paper.

References

[1] W. Wang and Y. Xu and M. Khanna, "A survey on the communication architectures in smart grid", Computer Networks, **(2011)** July, pp. 3604-3629.
[2] V. Namboodiri, V. Aravinthan and W. Jewell, "Communication Needs and Integration Options for ANI in the Smart Grid", white paper, **(2012)** May.
[3] What are Smart Microgrids?, http://www.galvinpower.org/microgrids.
[4] N. Cai, J. Wang and X. Yu, "SCADA system security: Complexity, history and new developments", IEEE International conference on Industrial Information, **(2008)**, pp. 569-574.

[5] V. C. Gungor, D. Sahin, T. Kocak and S. Ergut, "Smart Grid Technologies; Communication Technologies and Standards", IEEE Transaction Industrial Information, vol. 7, no. 4, **(2011)**, pp. 529-539.
[6] V. K. Sood, D. fischer, J. M. Eklund and T. Brown, "Developing a Communication Infrastructure for the smart grid", IEEE Electrical power and energy conference, **(2009)** October, pp. 1-7.
[7] M. M. Founda and Z. M. Fadlullah, "A Lightweight Message Authentication Scheme for Smart grid Communication", IEEE Transaction Smart Grid, **(2011)** December, pp. 675-685.
[8] Z. Lu, X. Lu and W. Wang, "Review and evaluation of Security Treats on the Communication Networks in the Smart Grid", MILCOM, **(2010)** October, pp. 1830-1835.