TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 12, No. 12, December 2014, pp. 8022 ~ 8027
DOI: 10.11591/telkomnika.v12i12.6725

Guidelines to Establish Secure Structure in Communication Networks used in the Smart Grid

Siamak Rezaei
Department of Electrical Engineering, Najaf Abad Branch, Islamic Azad University, Najaf Abad, Iran
email: siamakrezaei50@yahoo.com

Abstract

Currently, an extensive worldwide movement to implement electrical Smart Grid and replacing traditional grids has been started. In the past, since each electrical grid was usually using its specific systems and protocols, the possibility of system penetration and consequently security concerns was in low levels. But in recent years, with implementation of electrical Smart Grid, using open standards and popular network protocols, such as the technology which is used in the Internet (Internet Protocol), in electrical Smart Grids has been considered. This is due to advantages like efficiency, accessibility and low cost of these technologies. But, on the other hand, this increases the security concerns. Thus, selecting the appropriate communication mechanism for Smart Grid, is one of the most important challenges. Therefore, in this paper we introduce and study traditional communication networks in Smart Grids and discuss security capabilities of them.

Keywords*: grid security, IP, standards, protocols, communication networks*

1. Introduction

Smart Grid is the title usually used to describe the elements which can be connected to the power grid and have advanced communication infrastructure and provide many advantages and benefits for power sets. Reliable and secure communication infrastructure is the basis of the smart grid. The management of such a communication infrastructure which establishes the connections between the elements of the smart grid, should be based on open standards. The purpose of creating the smart grid is an electrical power transmission from production to consumer using digital technologies in order to increase energy efficiency, reduce costs, enhance reliability and clarity of the production, transmission and consumption.

The growing awareness of energy and the environment, the demand for reliable and stable power grid and the need for high quality and high reliability resources led smart grid to become common goal in developing power grid in the whole world. Smart grid should be implemented as soon as possible so that it could desirably affect the current trends of power delivery, reliability and taking advantage of renewable energies. But the success of this project is dependent on a number of implementation factors such as consumer collaboration, capability of equipments to take advantage of the information technology advances, adopting generalizable standards and enhancing efficiency of the energy transmission system [1].

Power distributors have been seeking ways of economically reading customers' meter for a while. This is possible by installing a device which is only able to monitor. The meter reading device can be programmed to report if its read number exceeds a predicted value. On AMR (Automatic Meter Reading) system, reading and tariff of the customers' meters are done automatically remotely which is done through the spread spectrum communication system with UNB (Ultra Narrow Bandwidth) and it sometimes uses PLC. Information is transmitted to the receiver in the distribution substation using RTU.

The second generation GSM mobile phone provides a standard in which, the connection is based on the circuit or Circuit Switch. In this system connection to the meter is performed via public communication network and there is no need for data collection unit or specific transmitters and receivers any more and data communication can be done easily via every meter. The third generation mobile phone is UMTS that provides broadband communication (bandwidth of several hundred kilobits per second). Advanced meters could be equipped with GSM or UMTS modems to establish a connection with communication network

Received June 6, 2014; Revised September 21, 2014; Accepted October 19, 2014

and data collection unit. Since there is no guarantee of the network availability in the location of the meter, this network could be used alongside with other communication substrates. On the UMTS network, various services are supported, which include voice services, data services such as videophone and video conferencing with up to 8 participants, download capability, multimedia content and email, internet services and also mobile commerce [2].

Therefore, knowledge about the present telecommunication networks in Smart Grid and their security structure could be of a key importance for correct management of events in occurrence of security problems in the network and reducing security damages in order to increase the reliability of the network. In this paper, we first review the overall performance of communication networks in Smart Grid in section 2. Then in sections 3 and 4, security challenges in present communication networks in Smart Grid and security solutions for exchanging information in these networks is discussed.

2. Overall Review of Implementation of Communication Networks

Standards are protocols which are defined on industrial scale not restricted to a particular manufacturer. With standard protocols, components made by different manufacturers could be used with complete compatibility. As long as a part follows particular standards, it could be placed and operate within the network. By taking advantage of the standards, guidelines and best trends in this area, an electric company can establish its smart security management system. So, in this stage one should try to review and examine the available standards of the various components of the monitoring data transmission system in power grid [3, 4].

2.1. Technical and Economical Comparison of Optimal Solutions from Different Directions

Based on technical and economical data obtained from different brands of data monitoring systems, a technical and economical comparison between them should be made. Some of the important parameters in this comparison, in addition to technical factors, are factors such as the final cost of the system, efficiency and quality, maintenance costs, development costs, system reliability and others.

2.2. Selection of the Solution, Company and Final Product

Based on meetings with companies that are selected as final candidates and frequent communication with them, appropriate product and company would be selected.

2.3. Documentation of All Requirements of the Security and End-user

To complete the requirements and finalizing the design, the all requirements of the security and end-users should be documented.

2.4. Locating the Exact Sites of the Installation

Since the location of the data transfer devices usually changes during the design process, with the presence of security experts and end-users, different heights and angles are examined and tested for data transmission to determine precise locations of angles for installation.

2.5. Implementing all Affairs Related to the Installation

At this stage, making infrastructure for the system is also done, including carving, making ready the routes, intubation for the cable laying and etc. In addition, the tower should be designed using specialized softwares. Also deployment of the other devices such as a communication platform, UPS, arrester and etc. should be done in parallel to this stage.

2.6. Test and Setup of the System

At this stage, all of the related equipment such as antennas, cameras, communication systems, main software, control room and etc. should be designed and installed and possible problems should be solved.

2.7. Preparing all Schematics and Documentation of the System

For continuous, correct and accurate operation of the project, final schematics and all steps and information which is obtained during the project should be documented.

2.8. Providing Principles of using the System

One of the most effective issues is rules, structure and usage of the system. So, at this step, all of rules and guidelines related to the optimal usage of the system are provided and the necessary information is given to system users.

2.9. Providing Structure and Maintenance Plans

One of the issues which is really effective on the reliability and stability of the system, is maintenance of the system that includes a variety of methods. At this step, determining the structure of maintenance, plans and strategies, the method for documenting changes and repairs are done and maintenance personnel is instructed [5].

2.10. Documentation and Updating Collected Information during the Project

To record any changes or to develop the system and also to be aware of the different enhancements of the system, this documentation and updates should be done regularly.

2.11. Network Platform

Communication links.

3. Security Challenges in present Communication Networks

The aim of the security of the access network is providing security in radio interface and in the access network sector. This sector is one the most important parts of security, because due to air interface and lack of physical security, many attacks such as eavesdropping or modifying messages are applied to this sector.

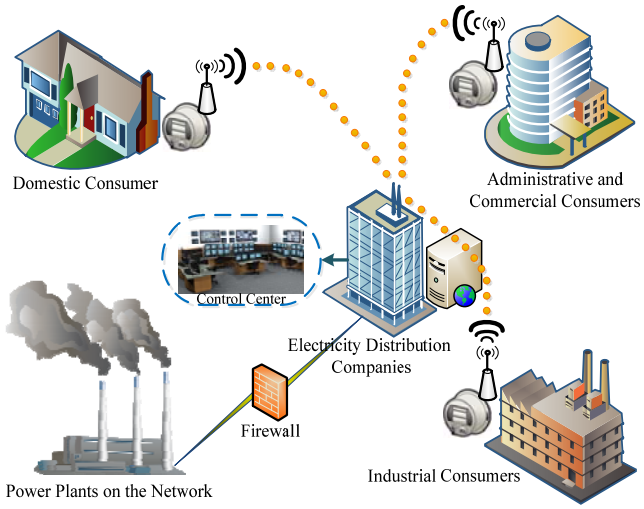

Figure 1. A structure indicating data transmission in the Smart Grid

Three different security methods are used in wireless networks:

a) WEP (Wired Equivalent Privacy): this method, in which eavesdropping of the users who are not permitted on the network are prevented, is suitable for small networks. Because it requires manual setting (KEY) for each client. Encryption of WEP is based on the RC4 algorithm using RSA [4].
b) SSID (Service Set Identifier): WLAN networks have several local networks that each of them has a unique identifier (ID). These identifiers are inserted at multiple

Access Points. Each user must make corresponding SSID identifier setting to access the network.

c) MAC (Media Access Control): a list of the used MAC addresses in a network is inserted into the corresponding Access Point (AP). Therefore, only the computers with these MAC addresses have the access permission. In other words, when a computer sends a demand, its MAC address would be compared with the corresponding MAC address list in the AP and the permission of access will be evaluated. This security method is suitable for small networks since entering these addresses to AP in large networks would be very difficult [6-10].

A complete set of standards, whose main aim is secure and errorless transmission, had been provided for wireless network which include 802.15 for Personal Area Networks (PAN), 802.11 for Local Area Networks (LAN), 802.16 for Metropolitan Area Network (MAN) and 802.20 for Wide Area Networks (WAN).

One of the most successful wireless standards is IEEE802.11 which is a selected technology for most of the Wireless LANs in public places and companies and provide HotSpot as a big business for wireless internet service providers.Currently an association of manufacturers and service providers who are known as Wi-Fi are tracing developments of commercial achievements of the 802.11.

IEEE 802.16 protocol is developed for large wireless metropolitan networks or in the other words WMAN. At first this standard has been designed to provide broadband wireless access in metropolitan networks. In January 2003, IEEE introduced 802.16a, a new version of wireless technologies, which works in 2 to 11 gigahertz radio frequencies, while the initial standard had been designed for working in 10 to 66 gigahertz. The greatest result of this change is solving “direct sight restriction” problem.

It is worth noting that the properties of radio waves with frequencies above 10GHz cause absorption of these waves by natural and artificial obstacles (e.g. trees and buildings) and some kind of direct sight should be provided by installing the transmitter and receiver antennas on high points and communication towers. With solving this problem, 802.16 significantly reduces the costs of the development of a wireless metropolitan network.

4. Information Security in the Exchange of Information in Communication Networks of Smart Grid

For the security of the network, providing security in communication between network elements is one of the main goals and it has nothing to do with mobile terminal. Both elements could belong to a network or two different networks. If these elements are on different networks, security mechanisms must be standardized. In the past, the security mechanisms for communication between two network elements doesn’t seem so necessary, because it was only available for specific institutes and entering an SS7 network was difficult for an attacker. But nowadays, this is not true due to two reasons: first, the number of operators and service providers is increasing and secondly, most of the networks tend to replace SS7 signaling protocol with IP network protocol. Though using IP protocol has numerous benefits, but most of the hacking tools available on the internet are applicable to this network. So, protecting messages between signaling networks should be considered as a serious security target. For this purpose, in the third generation network, security mechanisms related to the core have been developed, including IPsec and MAPsec.

Each interface in communication network has one or several unique IP addresses. A network interface could have one or several IP addresses, but an IP address cannot be attributed to several interfaces in a network. With increasing demand for IP based services, the need for a new method of technology, which could support large number of the users and provide a large number of IP addresses for users, is highlighted.

Although the performance of IPv4 protocol is great, but it has its own limitations. Since in IPv4 security is not provided, other protocols like IPSec is implemented with security approach. The main challenge for IPv4 is its addressing space limitation. After several years of popularity of the internet, the lack of variety of IP addresses became one of the major concerns in the internet. NAT (Network Address Translation) was developed to overcome the limitations of IP addresses. This technology lets the computers in a private (local) network to use specific addresses in order to communicate with each other, but use a public shared IP for all

connections to the internet. IPv4 protocol supports 3.4 billion IP addresses, while IPv6 protocol can support 50×10^{48} IP addresses.

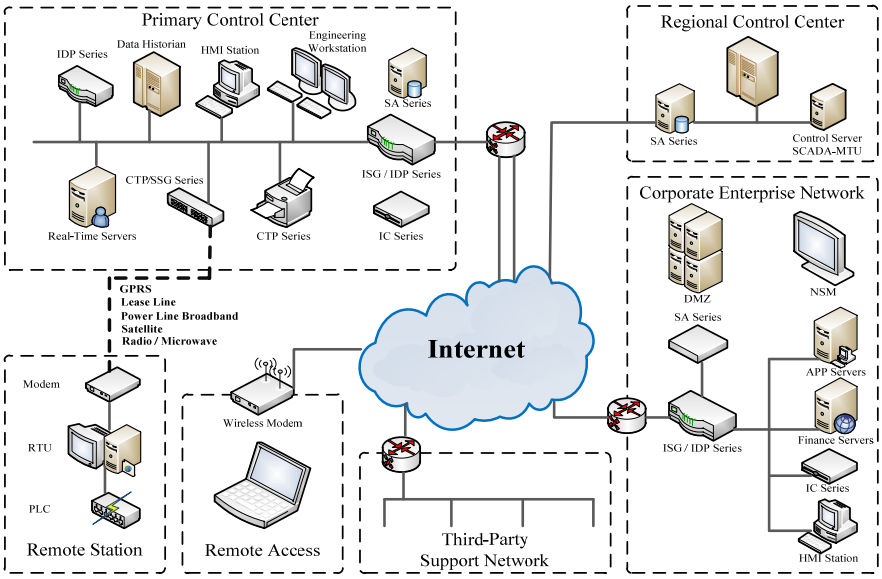

Figure 2. Block Diagram of transmit and receive encrypted data in the secure Smart Grid

IPv6 has been designed so that it is possible to provide various IP services to a large number of users, in terms of numbers and in terms of geographic area, via IPv6. Using IPv6, addressing space increases several times, as a result lot of unique addresses could be created in this way. Despite these unique addresses, access and security mechanisms are also altered [10-14].

5. Conclusion

Increased usage of digital information and control technologies in Smart Grids leads to rise in reliability, security and efficiency of power grids and rise in the integration of distributed generation, demand response and energy efficiency as well. As a result, the creation of a secure environment for information exchange and privacy in Smart Grid is crucially important. Studies show that IP-based networks are not sufficient alone to respond to quality of service requirements of applied applications in Smart Grid and requires approaches to guarantee quality of service. Since in the IPv4-based networks, security is not included, in third generation network network core related security mechanisms have been created which includes MAPsec and IPsec. Therefore, according to what has been said, in order to create an efficient space in Smart Grids and also maintaining existing investments and minimizing risks, paying attention to structures and security of communication infrastructures of Smart Grid is of vital importance.

References

[1] El-hawary ME. The Smart Grid—State-of-the-art and Future Trends." *Electric Power Components and Systems*, 2014; 42(3-4): 239–250. Accessed March 19, 2014. Available http://www.tandfonline.com/doi/abs/10.1080/153250082013.868558.
[2] Baghar-Nasrabadi S, Shahinzadeh H. Evaluation of Existing Protocols to Improve Information Exchange Security in the Smart Grid. *Journal of Basic and Applied Scientific Research (JBASR).* 2013; 3(1): 558–563.
[3] Ericsson GN. Cyber security and power system communication essential parts of a smart grid infrastructure. *Power Delivery. IEEE Transactions on*, 2010; 25(3): 1501–1507.
[4] Ghorbani J, et al. 2013. Investigation of communication media requirements for self healing power distribution systems. In *Energytech.* IEEE. 2013 1–7.

[5] Goel S, Negi R. Guaranteeing secrecy using artificial noise. *Wireless Communications, IEEE Transactions on*. 2008; 7(6): 2180–2189.
[6] Hasanalizadeh-Khosroshahi A. Sensor Networks in Demand Side of Smart Grid. *8th International Conference on Technical and Physical Problems of Power Engineering*. Norway, Fredrikstad, Ostfold University College. 2012: 5–7.
[7] Julkunen H, Chow CE. Enhance network security with dynamic packet filter. *Computer Communications and Networks. Proceedings 7th International Conference on*. IEEE. 1998. : 268–275.
[8] Shahinzadeh G, Shahinzadeh H, Paknejad A. Infrastructure Evaluation for using Smart Metering System (AMI & AMR) in Power Distribution Networks. *International Journal of Computing and Digital Systems (IJCDS)*. 2013; 2(3): 181–186.
[9] Shahinzadeh H, et al. Evaluation of SCADA Security in smart grids. *3rd International Conference on Computer Technology and Development (ICCTD)*. 2011.
[10] Shahinzadeh H. Technical Guidelines for Creating Smart Cyber Security of Information Technology in Power Systems. *1st Iranian Conference on Smart Grid*. 2010.
[11] Wang X, Yi, P. Security framework for wireless communications in smart distribution grid. *Smart Grid, IEEE Transactions on*, 2011; 2(4): 809–818.
[12] Wang W, Lu Z. Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*. 2013; 57.
[13] Shahinzadeh H, Hasanalizadeh-Khosroshahi A. Implementation of Smart Metering Systems: Challenges and Solutions. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2014; 12(7).
[14] Wang W, Xu Y, Khanna M. A survey on the communication architectures in smart grid. *Computer Networks*. 2011; 55(15): 3604–3629.