International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 2
ISSN: 2454-4248
56 – 59

Modelling for Improved Cyber Security in Smart Distribution System

Sumit Saini
Electrical Engg. Dept.
DCRUST, Murthal
Sonipat, India

Rajender Kr.Beniwal
Electrical Engg. Dept.
DCRUST, Murthal
Sonipat, India

Rinku Kumar
Electrical Engg. Dept.
DCRUST, Murthal
Sonipat, India
rinkukumar721@gmail.com

Ram Paul
Com. Sci. Engg. Dept.
Amity S. of Engg. &
Tech., New Delhi, India

Sunita Saini
Management Dept.
DCRUST, Murthal
Sonipat, India

Abstract—Information technology is the backbone of the smart grid, where all networks like generation, transmission, distribution, and customer components are connected to each other. Connectivity between these components offers many advantages including consumer's ability to manage their electricity consumption rates and electricity bills etc. Smart grid also provides operators great extent of system visibility and control over electricity services, supervision and control of generating units, power quality improvements and reduced fuel cost etc. Highly connected infrastructure in smart grid threats the reliable operation of grid, especially in terms of cyber security. In automated system, where control actions can be generated by a single command even from a great distance may lead complete shutdown of the whole system. Failure/disoperation of power service suspends all critical services. Therefore, the electrical grid becomes the most significant target for acts of vandalism and terrorism. So an extensive security against the cyber-attacks is required in smart grid environment as compare to traditional electricity grid, where almost all control actions were taken manually or with little use of local controllers. Therefore, with control atomization modulation of traditional energy supply system into a smart network requires a huge investment to develop security strategies as a safeguard for this critical infrastructure.

Keywords-*cyber security; protection; smart grid; control; critical infrastructure*

*****

I. INTRODUCTION

Energy management is a great task to deal in a vast and complex power system network [1-3, 13, 24], if every time data for energy uses and power flow is available to the service provider (utility), then this will improve the management, energy security, better asset utilization, congestion management [4, 14-19, 21, 23, 24, 25] etc. in Smart Grid operation. Smart Grid is the combination of modern information technology and power grid assets. Cyber security of the smart grid network means to secure the communication network, where the control action i.e., information is contained. 1) The data that transferred on a network must not be illegally invaded, transferred to unauthorized location, modified, patched or deleted; 2) confidentiality of the content must not be revealed to someone else; 3) the security measures must be selected according to nature of information i.e., sensitive data such as alarms, settings of different control valves, equipment management etc. Data collection in smart grid is accomplished by information exchange between controller and control center and vice versa, so two communication is necessary for that [5]. The main tasks performed by smart grid are:

1. Helps the customer to manage consumption and use electricity wisely.

2. Enables customer to respond to utility that help minimize the period of surpluses, bottlenecks, and outages.

3. Helps utilities in improving their performance and controlling costs by timely availability of information.

There are a lot of components associated in the smart grid for achieving its goals [6]. These components are connected to each other via a common communication network to provide real time data flow at each end of the smart grid for satisfactory operation of the system, from utility as well as consumer point of view [20, 22, 26]. This property of the smart grid enables it to perform real time actions to avoid [7] any malfunctioning, to have complete observability, to avoid severe black outs situations, to supports its self-healing capability, for contingency analysis and many more [27-29]. At the same time this two way network exploits a large number of vulnerabilities in the system which may cause severe effects in the power system [8]. For example, a circuit breaker can be controlled electronically by sending signal to its controller. An unhorsed person could target the sensor control and maloperate the device from a distant computer. It could harm the supply network in many ways such as increased losses, electricity theft, power quality issues, service interruption and power management problems [30, 32-36].

Synchrophasors are employed in the smart grids to measure

 ISSN: 2454-4248
56 – 59

the streaming voltage and other parameters in much faster way than the previously employed devices [9]. This data streams over the network to take necessary actions. The data is collected approximately from each device of the smart grid in real time. Between the points of data collection and reception, the data protection is required. With the basic knowledge fundamentals and little investment a hacker could interfere with the network and could get control and access the information of the grid equipment that are essential for maintaining the communication. An intruder, after gaining control on the devices can operate the whole structure and could create imbalance voltage [31], power imbalance, or shut down the power plant without knowledge of the service provider. So, there is no smartness in the smart grid without a smarter security.

Rating of the data corresponding to its importance can be done and accordingly the level of cyber-attack can be categorized in small, medium and high level. This segregation helps to decide the cyber security measures respectively. The high rating indicates highly sensitive data and highest level of security. The data security relates with the technical skills and expertise is required to access it. A person with almost no knowledge of system can exploit with the help of exploiting tools. So, the extant of data up to which a user can access it at a time must go through some manual information exchange.

II. SECURE SMART GRID

The smart grid highly dependent on the data, which is transferred though communicating network and poses its own security risks, so smart grid communication network should be structured in such a way that it can provide a greater security for data theft and gird equipment as any malicious act not only harms the software it can also harm the sensing and controlling components, generators, meters, CB's, remote terminal units and many other sensitive parts of the grid. Intruder can hold in power as a whole to support terrorism which can harm the nation too, so cyber security of smart grid should be sound enough. Some models that can provide greater cyber security to the smart grid are given below:

A. Laying Down an Independent Communication Network

Proper security measures can increase the security level of the World Wide Web but some hidden vulnerabilities even when great care is taken, can't be avoided.

This is due to the various unknown links in communication network and operating system susceptibility. Thus network structure can provide the maximum security from the security attackers. If network is independent and no external links are provided by the server, no one can interrupt the operation of the utility. The security and reliability of the network depends upon the following factors:

- Network architecture
- Area covered by server
- Security level
- Type of the operating system
- Interdependency of the different servers
- Continuity of the network

Although this structure provides maximum security but this is the most expensive one. A lot of capital investment is required to build up such a network. This is very complicated task as wiring for independent network will be very typical in nature. Huge land requirement is there, large workforce requirement etc.

B. Using PLCC and LAN

Power Line Carrier Communication and Local Area Network together can provide a great flexibility and security to the smart grid network. Localized data can be collected and processed through the local area network for the use in that area and data required for the central unit can be made available through PLCC network. This architecture also provides maximum security level for the smart grid. It reduces the capital cost requirements to build up a new communication network.

C. Customer Care or Call Center Architecture

This is same as in case of mobile communication, companies provide information to their users through customer care center. The requested information and help is given through online communication via handset to the user and their

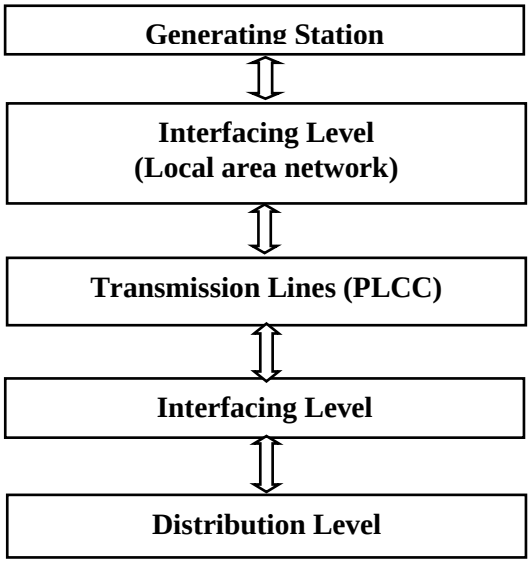

Figure1. Block diagram of PLCC and LAN architecture

quarries solved by the agents of the service provider and complete assistance and satisfaction of the customer is assured. Even the access level to the agents also predefined no one can go outside their premises, so the data is available as per the authenticity of the customer and agent position in the company.

 ISSN: 2454-4248
56 – 59

All the information to the customer and information provided by the agent is recoded for various futuristic events. This architecture will reduce the intrusion effect and will provide greater flexibility and security. This architecture may be implemented in co-ordination with power line carrier communication network as shown below:

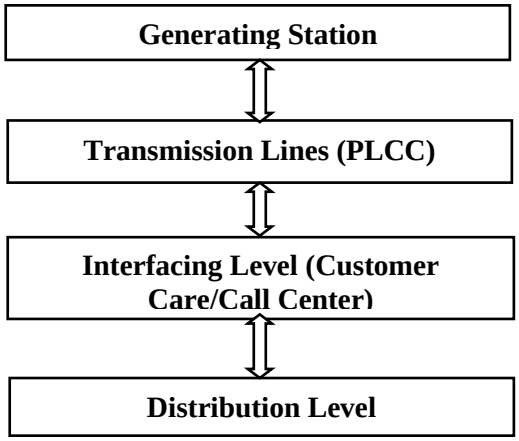

Figure 2. Customer care or call center architecture

D. Strong Passwords

The security of the online information can be improved by selecting a password which cannot be guessed easily. The password must contain a highly complex structure and some special characters too. A two or more level security steps may be involved to make it more secure. A frequent change of the password further increases the reliability of the communication system. The passwords which are completely different in pattern and order can't be breached easily. The passwords must be remembered by the user.

E. Put up a Strong Firewall and Install Intivirus Protection

Firewall and antivirus software are essential tools for a communication based control system. These software can detect the unauthorized access, different type of viruses that can harm the data and take action automatically. Antivirus must be updated time to time to keep you protected. The security applications are good if they are updated recently.

F. Secure Your Computers/Mobiles

Most of the data is stored in computers and control actions/supervision is also done by computers. These computers/mobiles must be protected from unauthorized elements. Data encryption and password protection are the most common techniques to prevent data theft.

G. Regular Data Backup

Scheduling regular data backups to an external storage, is an effective, safe and secure way to be confirmed that all your data is secure. To avoid any error in data saving, automatic data backups can be scheduled by the operator.

H. Educate and Communicate Cyber Security Policies to Employees

Security breach may be the result of the lack of knowledge of the employees. It must be a regular practice to teach the employees about safe and secure online habits. The employees should be aware about the criticalness of the data and how severe it can be if accessed by someone who wants to attack the whole structure. The different policies of cyber security and rules can be dispersed to all employees It must be ensured that it is understood by all workers, so that things can be in practice.

I. Access Limit to Critical Data

The critical data must be kept within the reach of the safe hands. The all critical data must not be available at one desk irrespective of the authority level as it can be a weakest point of the secure network.

III. Conclusion

In smart grid network, information technology plays a vital role in atomization and control. Cyber security measures must be embedded in the network architecture as a part of the design process. Starting from the utility end consumers should also be aware about the security issue of the smart grid communication network. Cyber awareness programs can decrease the vulnerability of the system. With the advancement in the communication system and security measures the security threats are evolving continuously. For use of the new technological parts in smart grid architecture, a common testing and implementing lab may be constructed by various service providers to avoid capital investment and for experimental purposes. The architectures described above can provide much better security levels for smart grid without much modification.

References

[1] "Smart Grid - enabling electricity networks of the future TODAY," Smart Grids for Distribution, 2008. IET-CIRED CIRED Seminar, vol. no.1, 23-24 June 2008, pp.1-1.

[2] Koponen P., Seesvuori R., Böstman R. (1996).

[3] "Adding power quality monitoring to the smart kWh meter," Power Engineering Journal (IEE), August 1996, 10, (4), pp. 159-163.

[4] "Critical Infrastructure Protection Challenges in Securing Control Systems", General Accounting Office

[5] (GAO) Report, GAO-04-140T, October 1, 2003.

[6] M.C. Macduff, R.C. Eagan, U.S. Department of Energy report for "ACRF Data Collection and Processing Infrastructure," December 2004, pp. 1-20.

[7] Marihart, D.J., "Communications Technology Guidelines for EMS/SCADA Systems," Power Delivery, IEEE Transactions on, Volume: 16, Issue: 2, April 2001 pp. 181–188

[8] Liting Cao; Jingwen Tian; Yanxia Liu; "Remote Real Time Automatic Meter Reading System Based on Wireless Sensor Networks," 3rd International Conference on Innovative Computing Information and Control, June 2008, pp. 591 – 591.

[9] "Phasor Technology and Real-Time Dynamics Monitoring System," Available at www.phasorrtdms.com/downloads/guides/ RTDMSFAQ.pdf

[10] V. Kumar, J. Srivastava, and A. Lazarevic, "Editors, Managing Cyber Threats: Issues, Approaches and Challenges,".

[11] G.Phadke, "Synchronized phasor measurements in power systems", IEEE Computer Applications in Power, April 1993, pp. 10-15.

[12] R. Singh, Satpal and S. Saini, "Power Sector Development in Haryana," International Journal of Science," Technology and Management, vol. 5, no. 3, pp. 278-285, 2016.

[13] S. Saini, "Social and behavioral aspects of electricity theft: An explorative review," International Journal of Research in Economics and Social Sciences, vol. 7, no. 6, pp. 26-37, 2017.

[14] S. Saini, "Scenario of Distribution Losses – A Case Study from Haryana", International Journal of Research in Economics and Social Science, vol. 8, no. 1, pp. 163-175, 2018.

[15] S. Saini, "Malpractice of Electricity Theft: A major cause of distribution losses in Haryana," International Research Journal of Management and Commerce, vol. 5, no. 1, pp. 284-313, 2018.

[16] S. Saini, "Expectancy-disconfirmation based assessment of customer Satisfaction with electric utility in Haryana," International Research Journal of Human Resources and Social Sciences, vol. 5, no. 1, pp. 320-335, 2018.

[17] S. Saini, "Electricity Theft – A primary cause of high distribution losses in Indian State," International Research Journal of Management and Commerce, vol. 8, no. 1, pp. 163-175, 2018.

[18] S. Saini, "Service quality of electric utilities in Haryana – A comparison of south and north Haryana," International Journal of Research in Engineering Application & Management, Accepted, 2018.

[19] S. Saini, "Rationale behind developing awareness among electricity consumers," International Journal of Research in Engineering Application & Management, Accepted, 2018.

[20] S. Saini, "Analysis of service quality of power utilities," International Journal of Research in Engineering Application & Management, Accepted, 2018.

[21] S. Saini, "Difference in Customer Expectations and Perceptions towards Electric Utility Company," National Journal of multidisciplinary research and management, Accepted, 2018.

[22] S. Saini, "Appraisal of Service Quality in Power Sector of NCR," National Journal of multidisciplinary research and management, Accepted, 2018.

[23] S. Saini, "Evolution of Indian Power Sector at a Glance," National Journal of multidisciplinary research and management, Accepted, 2018j.

[24] S. Saini, R. Singh, Satpal, "Service quality assessment of utility company in Haryana using SERVQUAL model," Asian Journal of Management, Accepted, 2018.

[25] S. Saini, "Influence of gender on service quality perceptions", Kaav International Journal International Journal of Economics, Commerce & Business Management, Accepted, 2018.

[26] R. Kumar, S. Saini, A. Aggarwal, R. Paul, R. Saini and S. Saini, "Complete management of smart distribution system," International Journal of Engineering Sciences & Research Technology, Submitted, 2018.

[27] R. K. Beniwal, A. Aggarwal, R. Saini and S. Saini. "Detection of anomalies in the quality of electricity supply," International Journal on Future Revolution in Computer Science & Communication Engineering, Accepted, 2018.

[28] M. K. Saini, R. Dhiman, A. N. Prasad, R. Kumar and S. Saini, "Frequency management strategies for local power generation network," International Journal on Future Revolution in Computer Science & Communication Engineering, Accepted, 2018.

[29] R. K. Beniwal, A. Aggarwal, R. Saini and S. Saini, "Analysis of electricity supply in the distribution network of power sector," International Journal of Engineering Sciences & Research Technology, Submitted, 2018.

[30] R. Kumar, A. Aggarwal, R. K. Beniwal, S. Saini, R. Paul and S. Saini, "Review of voltage management in local power generation network." International Journal of Engineering Sciences & Research Technology, Submitted, 2018.

[31] M. K. Saini and R. Kapoor, "Multiwavelet transform based classification of PQ events," International Transactions on Electrical Energy Systems, 2012; 22(4):518-532.

[32] R. Kapoor R and M. K. Saini, "A new signal processing technique for power system disturbance detection and classification," Institution of Engineers India Part-EL, 2007; 88: 9-14.

[33] M. K. Saini et al., PQ events classification and detection – a survey, 2nd IEEE International Conference on Sustainable Energy and Intelligent system, Chennai, 2011; 490-495.

[34] M. K. Saini and R. Kapoor, Classification of nonlinear power quality events based on multiwavelet transform, International Journal of Nonlinear Science, 2010: 10(3): 279-286.

[35] M. K. Saini and R. Beniwal, Recognition of Multiple PQ issues using Modified EMD and Neural Network Classifier, Iranian Journal of Electrical and Electronics Engineering, 2018, In Press.