Cyber Security Issues in Smart Grid Technology

Sikha Sharma[1], Sherovani.B[2], Dr A.P.Nirmala[3]
[1, 2] Dept of MCA
[3] Assistant Professor, Dept of MCA
[1, 2, 3] New Horizon College Of Engineering

Abstract- *Smart Grid is Information and Communication Technology (ICT) enabled Power grid. It is efficient, secure, reliable and self-healing power grid. Integration of micro grids, electric vehicles and other utilities make it more interesting. The deregulation of electricity sector has necessitated the use of many advanced software and embedded technologies to handle the size and complexity of power network. Smart grid needs to be supported by efficient and secure communication architecture design and implementation. At the same time it is necessary to ensure the security and solitude of data and information stored in the smart grid system to have a complete uptime of the power grid. This paper presents a comprehensive analysis of the various communication and cyber security issues involved with the successful operation of Smart Grid. Specifically, we focus on reviewing and discussing network vulnerabilities and architectures in the Smart Grid.*

Keywords- Smart grid, Cyber Security, Communication, Generation, Transmission, Distribution, Advance metering, restructuring.

I. INTRODUCTION

The Smart Grid, generally referred to as the next-generation power system, is considered as a revolutionary and evolutionary regime of existing power grids. Smart grids provide electricity demand from the centralized and distributed generation stations to the customers through transmission and distribution systems. The grid is operated, controlled and monitored using information and communications technologies (ICT). These technologies enable energy companies to seamlessly control the power demand and allow for an efficient and reliable power delivery at reduced cost. Via digital two-way communications between consumers and electric power companies, the smart grid system provides the most efficient electric network operations based on the received consumer's information.

II. SMART GRID NETWORK ARCHITECTURE

Smart grid network is the necessary communication platform for monitoring and controlling the grid operation. To date, the architectural framework and implementation standards of the smart grid are still under investigation by the academic [9], [5], [11], industrial [1], [12], [6], [8], and government sectors. Although there are various designs for the grid architecture, almost every case follows the common reference model [17] proposed by the U.S. National Institute of Standards and Technology (NIST). Data storage devices may additionally be included in the network to support networked storage, local fault diagnosis, and distributed decision making. There is a communication gateway in each community network. It manages the communication among the network elements, performs data aggregation, and bridges the bottom and top layers to allow data exchange. An example of a community network is the network in a smart community [18]. At the top layer are *regional networks*. Dedicated hub nodes may be deployed in the network to build a multiple-hop overlay structure for efficient and reliable data communication. A control center is implemented in each regional network. It provides supervisory control and data acquisition (SCADA) functionalities in the regional grid: collecting electricity usage data and grid operation status, detecting and responding to anomalies, and optimizing power generation, transmission, and distribution. To interconnect these domains, Cisco [1] argued that the whole system should use an independent "network of net-works." It also claimed that the best standard suite of protocols for the smart grid is the Internet Protocol (IP) [1]. Since IP has already achieved great success in the current Internet in terms of flexibility, security, and interoperability, Cisco believes that the interoperability standards of the smart grid should use IP architecture as reference [1]. In addition, several researchers have proposed their own opinions on how to implement this model. Clark and Pavlovski [9] studied the pros and cons of wireless network applications for the smart grid and then suggested adopting 3G/4G technology for the architectural design.

As shown in Fig. 1, NIST's model consists of seven logical domains [17]. Each one of the above four (Bulk Generation, Transmission, Distribution, and Customers) can generate, store, and deliver electricity in two-way. The bottom three (Markets, Service Providers, and Operations) mainly manage the movement of electricity and provide relevant information or services to power consumers and utilities.

Three types of customers are present in this model: HAN (Home Area Network), BAN (Building Area Network), and IAN (Industrial Area Network). Within those areas, AMI (Advanced Metering
Infrastructure) is deployed to monitor all incoming and outgoing electrical and communication flow.

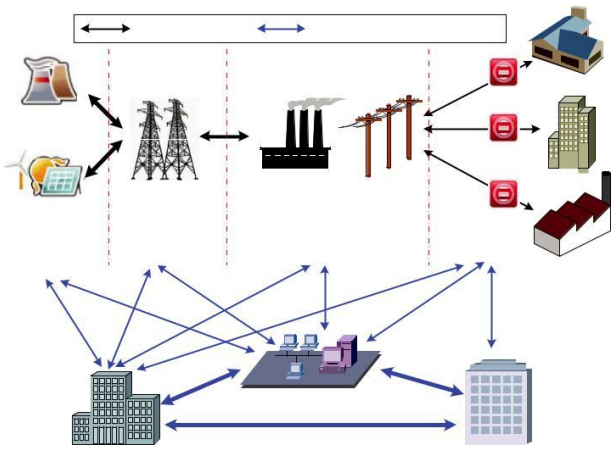

Fig 1 NIST reference model for the smart grid [4]

III. CYBER SECURITY ISSUES IN SMART GRID

Increasing interconnection of smart grids additionally will increase the exposure of grid to potential attackers and/or unintentional errors. Networks that connect more often to totally different networks introduce most common vulnerabilities which will span multiple smart Grids and increase the possibilities of failures. Different variety of interconnections invites additional denial of service attacks, malicious code, compromised system and intrusions. Because the variety of nodes will increase within the network, the amount of entry points increase which can be used by potential adversaries for exploitation. Extensive information & data collection their flows might broaden the potential for compromises of information and data and breach of confidentiality and client privacy. Components of good grid security includes physical elements and management applications, cyber infrastructures needed to support necessary designing, operational and market functions, cyber-attacks and its impact on the system, actions and measures to mitigate risks from cyber threats.

A. Cyber Security issues in Generation Power generation management primarily involve managing the generator power output and terminal voltage by applying local automatic transformer (AVR) and governor control (GC) schemes. AVR and governor control don't rely on the supervisory control and data acquisition (SCADA) transmission infrastructure for its operations as each the terminal voltage and rotor speed are detected locally. Albeit these applications are susceptible to malware that would enter the station local area network (LAN) through different entry points like USB keys. Additionally associates working in company may compromise plant cyber security mechanisms to gain an entry point into the native local network and may disrupt normal operation by corrupting the logic or settings within the digital controllers. The automatic generation control (AGC) is a secondary frequency management that's involved with fine controlling the system frequency to its nominal value [10] and [2]. The AGC depends on tie-line and frequency measurements provided by the SCADA mensuration system. . An attack on AGC may have direct impacts on system frequency, stability and operation. Denial of service (DoS) style of attacks might create a big impact on AGC operation once supplemented with another attack that needs AGC operation.

B .Cyber Security issues in Transmission Power system state estimation [15] is used as a technique by that estimates of system variables like voltage magnitude, phase angle (state variables) and power flows on totally different sections are calculated based on likely faulty measurements from field devices. The control center application performs computations by making use of large no. of measurements it receives via wide-area network. False information injection attacks, that escape detection by existing faulty measurement identification algorithms, could also be dangerous. The reactive (VAR) compensation with FACTS devices [10] is the method of controlling reactive power injection or absorption in a power grid to boost the performance of the transmission network FACTS devices interact with each other to exchange operational data via communication link. It can face Denial of cooperative operation that may be a DoS attack. During such attack, the the communication to some or all the FACTS devices might be stopped by flooding the network with unwanted packets. This may end in the loss of vital data and therefore have an effect on semi-permanent and dynamic management capabilities. De-synchronization (timing-based attacks) might disrupt steady operation of Cooperative FACTS devices (CFDs).

C .Cyber security and distribution system Modern relays are internet protocol (IP) capable and support various communication protocols [13]. Cyber-attack on the communication set up or malicious amendment to the control logic might end in unexpected tripping of distribution feeders, resulting in load segments not served Advance metering Infrastructure primarily depends on the deployment of good smart meters to supply real-time meter readings. Smart meters offer utilities with the flexibility to implement load management & control (LMC) to disable control devices once demand spikes. The capability to remotely disable smart meters through load management shift provides potential threats from attackers. Embedded systems are used heavily in

the grid to support observance and management functions. Intelligent electronic devices (IEDs) are placed to control relays throughout the grid [4]. Recent events have shown that IEDs are often maliciously reprogrammed to halt intended management functions. Deployments of embedded devices at large scale in smart grid additionally incentivize the employment of cheaper hardware leaving very little computing capability to support varied security functions like malware or intrusion observance. The deployment of secure computation within embedded platforms provides a key challenge to cyber security.

D .Cyber security in communication network of Smart grid Cyber security [10] inside the communication network is known as protection of data and systems from unauthorized access, disclosure, modification, destruction or disruption. The objectives of Cyber security are confidentiality, integrity and availability These 3 objectives need to be ensured altogether in various stages of data processing (i) storage state in storage media (ii) processing state in RAM and (iii) transmission state in communication media. Three Objetives of Cyber-security in Smart Grid Confidentiality is outlined in literature as protection of data from unauthorized access or revelation. The authorized users only ought to get access to data and un-authorized ones ought to be prevented from doing this. Integrity is defined as protection of data from unauthorized modification or destruction. . It's necessary to make sure that the data and information and system containing information is correct, non-corrupted and complete. Availability refers to the protection of data and information systems from unauthorized disruption. It is important to make sure the timely and reliable access to and use of data and information systems

IV. CYBER SYSTEM VULNERABILITIES OF SMART GRID

Consumers' Lack of Awareness: a comprehensive andstrong security architecture for the SGs, including all important features required to analyze and detect the attacks, needs a huge investigation that might not be affordable for utilities alone. Therefore, the customers need to learn adequately about the risks, costs, and advantages of the SG systems, because of the demand for a higher level of security, and support the utilities, both for themselves and the society.

Young and Unknown Technologies: many new technologies are adding to the SG which could be eye-catching to hackers and opponents for the reason that their point of weaknesses and security regulations has not been recognized yet. Therefore, finding a gap to exploit the vulnerabilities would be simple.

Scalability: is defined as a system ability to update itsscale based on the growth in the size of demand. The SG technologies are considered as potential solutions for controlling the complex electrical power systems, which are widely growing in population and technology. It is obvious that the growth in the quantity of circulating data and energy flows, the SG protocols, and the size of network structure directly affect the size and complexity of the SGs. This volume of information and complexity might cause data accumulation, and control efficiency destruction, if not handled and accommodated properly in the SG. Therefore, efficient data flow construction solutions are required to prevent these problems in the system [14].

The Weaknesses Received from Joined Communication Technologies: applying existing ICTs in the structure of the SGs can lead to inheriting almost all the susceptibilities and unresolved problems (e.g., routing problems, IP spoofing, Denial of Service attacks, etc.) from these technologies to the SG system.

Lack of Standards and Regulations: interoperability of a SG refers to the ability of various systems to work cooperatively, interchange equipment or data from each other, and use the harmonious parts to perform a task. To achieve interoperability, standards and regulations must include each part of the SG. It is also worthy to mention that novel protocols publishing continuously, sometimes cause security missing in the SGd (e.g., Distributed Network Protocol).

V. CONCLUSION

Many countries in the world have moved towards making their power grid smarter and others are in the process. With increasing integration of many regional grids across the globe would make it possible to form power cloud where power can be drawn from the cloud in any amount at any time and place. This would necessitate storage and movement of large chunk of data, high speed network connectivity of various systems in power grid, use of smart devices and high speed computing techniques to handle the complexity and size of the smart grid. Many new scalable communication architecture, protocols and software need to be designed and developed to handle the real time requirements of operation and control of smart grid. It would also require that policy, procedures and technologies are identified and implemented to operate the smart grid in a secure and reliable manner. Estimation of potential risk and its impact assessment on the business continuity of smart grid system would decide the appropriate tools and technologies to be put in place for mitigation of potential cyber-attacks on the smart grid. By making correct choices it is possible to run the future smart

grid in an efficient, secure and reliable manner as it is important for sustainable growth.

REFERENCES

[1] Cisco Systems, Inc., "Internet protocol architecture for the smart grid," White Paper, Jul. 2009.

[2] Siddharth Sridhar, and Manimaran Govindarasu," Model-Based Attack Detection and Mitigation for Automatic Generation Control" IEEE Transaction on Smart Grid, Vol. 5, No. 2, March 2014.

[3] A Review on Cyber Security Issues and Mitigation Methods in Smart Grid Systems Maneli Malek Pour, Arash Anzalchi, and Arif Sarwat Florida International University.

[4] A. M. Gaouda, Ahmed Abd-Rabou and Abdul Rahman Dahir, "Developing Educational Smart Grid LaboratorY", IEEE.

[5] J. Gadze, "Control-aware wireless sensor network platform for the smart electric grid," IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 1, Jan. 2009, pp. 16-26.

[6] W.Y. Chu and Dennis J.H. Lin, "Communication strategies in enabling smart grid development," in: The 8th International Conference on Advances in Power System Control, Operation and Management (APSCOM 2009), Hong Kong, China, Nov. 2009.

[7] Cyber Security and Privacy Issues in Smart Grids Jing Liu and Yang Xiao, *Senior Member, IEEE*, Shuhui Li, Wei Liang, C. L. Philip Chen, *Fellow, IEEE*.

[8] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in: Innovative Smart Grid Technologies (ISGT 2010), Gaithersburg, MD, Jan. 2010, of Engineers and Computer Scientists 2010 Vol II (IMECS 2010), Hong Kong, Mar. 2010.

[9] A. Clark and C.J. Pavlovski, "Wireless networks for the smart energy grid: application aware networks," in: Proc. International MultiConference.

[10] Siddharth Sridhar, Adam Hahn and Manimaran Govindarasu, "Cyber–Physical System Security for the Electric Power Grid" Proceedings of the IEEE | Vol. 100,No. 1, January 2012.

[11] C. Wei, "A conceptual framework for smart grid," in: Power and EnergyEngineering Conference (APPEEC 2010), Chengdu, China, Mar. 2010.

[12] A.R. Metke and R.L. Ekl, "Smart grid security technology," in: Innovative Smart Grid Technologies (ISGT 2010), Gaihersburg, MD, Jan. 2010, pp. 1-7.

[13] Higgins, N.; Vyatkin, V.; Nair, N.-K.C.; Schwarz, K.; "Distributed Power System Automation with IEC 61850, IEC 61499, and Intelligent Control," Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on , vol.41, no.1, pp.81- 92, Jan. 2011.

[14] C. D. Cameron, P. Taylor, and C. Patsios, "Scalability in smart grid data flow architectures," in 2014 49th International Universities Power Engineering Conference (UPEC), Sept 2014, pp. 1–6.

[15] Saman Zonouz, Katherine M. Rogers, Robin Berthier, Rakesh B. Bobba, William H. Sanders, Thomas J. Overbye" SCPSE: Security-Oriented Cyber-Physical State Estimation For Power Grid Critical Infrastructure"IEEE Transactions on Smart Grid..

[16] M. Kezunovic, "Automated fault analysis in a smart grid," in: IEEE Asia and Pacific Transmission & Distribution Conference & Exposition, Seoul, Oct. 2009, pp. 1-3.

[17] U.S. NIST, "NIST framework and roadmap for smart grid interoperability standards, release 1.0," NIST Special Publication 1108, Jan. 2010

[18] U.S. NETL, "Advanced metering infrastructure," White Paper, Feb.2008.

[19] Lanchao Liu, Mohammad Esmalifalak, Qifeng Ding, Valentine A. Emesih, and Zhu Han, "Detecting False Data Injection Attacks on Power Grid by Sparse Optimization" IEEE Transaction on Smart Grid, Vol. 5, No. 2, March 2014.