International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2016 IJSRCSEIT | Volume 1 | Issue 3 | ISSN : 2456-3307

A Security approach for Smart Grid on Review

Santosh Kumar Suman, Mohd. Aqib, Sumit Kumar Singh

Department of Electrical Engineering, Rajkiya Engineering College, Kannauj, Uttar Pradesh, India

ABSTRACT

Aim of this paper the infrastructure for the traditional grid & smart grid. Together depend upon management and control system but the main modification is in the security system because it activities the benefits of the cyber world for realizing its objectives, it also faces security attacks. Therefore, security of the smart grid becomes foremost concern. Even the best smart grid infrastructure along with best management and control mechanisms will prove to be ineffective if security of the smart grid is not taken care of. In this discusses about the importance of protection in smart grid. It presents a review of progress made by researchers and governments and the technologies used in the area. It identifies the security issues involved with the current infrastructure. It points out about the areas in security where the research is still needed and discusses some observations regarding improvement of security in smart grid.

Keywords : Smart Grid, Smart Protection, Security, Smart Management, Smart Infrastructure

I. INTRODUCTION

Smart Grid in is an integration of communication infrastructure with full digital technology (Information and Communication technology) and power system infrastructure with real time power and data (information) flow (in a two-way exchange) between consumers and utilities in a dynamic way. Moreover, power markets are run on real time pricing. Smart Grid consists of many components like smart meters, smart appliances, advanced sensors etc. It will give consumers to choose their power distributor according to their power price. Smart Grid will make the existing grid intelligent, smarter, reliable and more flexible to handle threats. The power system grid or grid is used to support electricity generation, transmission, distribution, operate and control [1]. Though it is can be considered one of the greatest achievements of 20th century but now it seems to be overburdened, technologically outdated, which leads to various troubles including costly blackouts and burnouts [2]. Due to these reasons, the efforts are going on to make the current grid to smart grid. Hence, the term smart grid is an intelligent and smart version conventional power grid. The smart grid is also called smart power grid, smart electrical grid, intelligent grid, future grid, intergrid or intragrid [1]. Smart grid is a concept for transforming an electric power grid with the help of automated controls, advanced communications and other forms of information technology. The purpose is to integrate new innovative technologies, advanced equipment and tools from generation, transmission and distribution all the way to consumer appliances [3]. The key characteristics of the smart grid include enhanced power quality, optimizing asset utilization, minimizing operations & maintenance expenses, accommodating a wide variety of generation, self-healing, tolerating security attacks, empowering the consumers and fully enabling electricity markets [4]. For incorporating these characteristics the overall structure of the smart grid is divided into three components including Smart Infrastructure System, Smart Management & Control System and Smart Protection System [1].As shown in the Table-I, smart infrastructure system comprises smart energy subsystem, smart information subsystem, and smart communication subsystem. For two way benefit for consumer as well as energy producer, the smart management and control system has several objectives including improvement in energy efficiency, demand profiling, utility maximization, cost

reduction and emission control etc. The smart protection system focuses on reliability and security of the smart grid either physical or cyber. This third component of the smart grid is considered to be the most important in terms of preserving confidentiality, integrity and availability of the smart system [5]. The reason behind is dependency of the entire system on cyber word.

Table-I : Smart Grid main Components

Smart Grid		
Smart Infrastructure System	**Smart Management and Control System**	**Smart Protection System**
• Smart energy subsystem • Smart information subsystem • Smart communication subsystem	• Improvement in energy efficiency • Demand profiling • Utility maximization • Cost reduction • Emission control	• Reliability • Security & privacy

The rest of the paper is organized as: the next section discusses about role of security in successful implementation of smart grid. Section 3 presents systematic review of available approaches in the area. Section 4 discusses about security issues in present grid infrastructure. Section 5 identifies about security challenges of smart grid yet to be addressed. Section 6 suggests recommendations for security enhancement of smart grid. The paper concludes at last section

II. METHODS AND MATERIAL

A. Smart Grid

The Smart Grid has come to describe a next generation electrical power system. It is typified by the increased use of communications and information technology in the generation, delivery and consumption of electrical energy. Another definition of Smart Grid can also be considered. According to Wikipedia it delivers electricity from suppliers to consumers using digital technology to control appliances at consumer's premises to save energy, reduce cost and increase reliability and transparency. As said by Green Energy Act (Canada) it is a nickname for an ever widening palette of utility applications that enhance and automate the monitoring and control of electrical distribution. DOE: The Smart Grid transforms the current grid to one that functions more cooperatively, responsively and organically [3]. A Smart Grid is an electricity network that can intelligently integrate the actions of all users connected to it - generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies[4]. The smart grid is intelligent as it is capable of sensing system overloads and rerouting power to prevent or minimize a potential outage;of working autonomously when conditions require resolution faster than humans can respond and cooperatively in aligning the goals of utilities, consumers and regulators .It is capable of meeting increased consumer demand without adding infrastructure which shows its efficiency. Accepting energy from virtually any fuel source including solar and wind as easily and transparently as coal and natural gas; capable of integrating any and all better ideas and technologies energy storage technologies. This grid enables real-time communication between the consumer and utility so consumers can tailor their energy consumption based on individual preferences, like price and/or environmental concerns. This creates new opportunities and markets by means of its ability to capitalize on plug-and-play innovation wherever and whenever appropriate. A new technique for 'scheduling' energy in electric grids has been developed. It moves away from centralized management by tapping into the distributed computing power of energy devices. The approach advances the smart grid concept by coordinating the energy being produced and stored by both conventional and renewable sources.

Figure 1. advances smart grid concept

B. Necessity & Significance of smart protection system

Aim of earlier grid is to afford electricity to the consumer in enhanced way. Therefore it has only one

way communication concerning uncertain communication technologies. The necessity of development in grid can be satisfied by usage of digital technology. Transformation from analog to digital electricity infrastructure introduces the challenge of communication security. Earlier, role of protection system is limited to infrastructure and equipments but smart grid system is more complex, fast and handles bulk data hence requires much more pointed protection arrangement than earlier. As shown in figure-1, earlier for supporting grid infrastructure, protection and control was applied in adhoc manner but with smart grid "safeguard" safety has occurred in far great role. To overcome the security threat, protection part is widely increased.

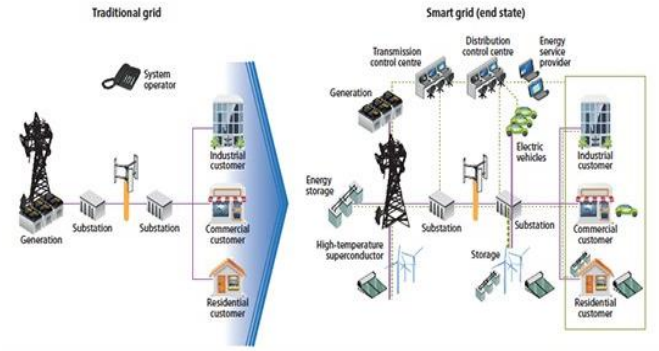

Figure 2. Towards "smart" energy grids

In recent years, attacking methods and incidents especially for industrial control systems has gradually increased. Recently on 21st October 2013, New York Times reported that two software engineers Crain and Sistrunk were able to hack and compromise entire national power grid and water utility systems from remote locations [6]. In 2011, L. Auriemma, an ethical hacker proposed means to attack the control automation system components and the underlying devices [7]. The first-ever control system malware called Stuxnet was found in July 2010. This malware, targeting vulnerable SCADA systems, raises new questions about power grid security [8]. In 2008, there was evidence of computer intrusions into some European power utilities [9]. In 2009, a researcher of IOActive Inc. demonstrated the worms infecting the smart meters. The worm could infect 25,000 meters in 24 hours and could cut the power supply of 15,000 houses [10].

In view of the above, it can be easily understood that smart protection is the major component of smart grid. It does not matter, how smart is the infrastructure or how smart is the management and control. Everything depends upon how smartly we can protect the smart grid. Any breach especially in security of the smart grid can dump the entire system. If smart protection fails then the smart grid would be the most awful. Nothing will stay smart. Even traditional power system shall work better than the smart grid. Then what is the benefit of introducing smart grid. Hence to realize all the benefits of smart grid, the grid must be made attack resistant. Though it is true that hundred percent securities cannot be achieved. But security enhancement must be the foremost issue to protect the entire system from attacks [10].

C. Literature review on Smart Grid Security

The smart grid field is very new and so its security. Smart Electricity generation, transmission and distribution system, in which Electricity suppliers and consumers are connected though safe, is the core of Smart Future. Following is the relevant research in smart grid security:

Jeena Joy et al (2013) by a Smart Grid have been evolved as the innovative idea universally as a solution for the power demand problems. Countries worldwide are looking for an efficient implementation of the same. A lot of research is now going on the various issues and challenges on the implementation and real time operation of the various components of Smart Grid. This paper presents a review on different challenges of electric power system in smart grid aspects. This also gives an insight into the current status of the research and developments in the field of smart grid. Authors strongly believe that this survey article will be very much useful to the researchers for finding out the relevant references in the field.

Anwar et al (2014) raised the issue of cyber-attacks in smart grid and presented a study of cyber attack impact on power system. They reviewed Smart Grid protection frameworks against component-wise, protocol-wise and topology-wise cyber-attacks. They emphasize on cyber security not on physical security. They discussed about security requirements of smart grid, which affects 'availability', 'integrity', and 'confidentiality' [14].

B. Vaidya et al (2013) emphasized on the severe short coming of Supervisory Control and Data Acquisition (SCADA) Systems. They raised the issue that the devices in SCADA systems are configured with default

password. Hence unobserved access via dial up and corporate information technology can be made to compromise the system. For restricting the unauthorized access to the devices they proposed lightweight and efficient security solution for Substation Automation Systems (SAS). Their approach provides multilevel and multifactor authentication and attribute based authorization by deploying public key certificates .The problem with this approach is that it is complex in nature and cover only a small domain for security [5].

K. C. Sou et al (2013) discussed that SCADA systems are increasingly dependent on the cyber world/ Internet. Because of the reason, more access points are exposed to malicious attackers. Hence more SCADA functionalities are subject to threat. They took the issue that the data communicated to SCADA can be attacked. Their research was focused to false data attacks. They took a security index problem which is attack construction and proposed an efficient solution to the security index (i.e. attack construction). They also proved and numerically demonstrated their results. The limitation of the method is being applicable only on infrastructure security [15].

E. Bou-Herb et al (2013) discussed that cyber vulnerabilities need to be addressed in order to increase the security of the smart grid. To increase the security of the smart grid they focused on the communication security aspect which was dealing with the distribution component of smart grid. They addressed the security concerns of Advance Metering Infrastructure (AMI) by correlating vulnerabilities in these systems and their associated risk. The aim was to mitigate the vulnerabilities in order to improve cyber security of the future smart grid. Again they focused on a very small component of power system application security i.e. metering system and the approach is vague in nature [16].

J. Wafler et al (2013) discussed about mutual dependency of Information and Communication Technologies and smart gird. They emphasized that the failing of either the power grid or Information and Communication Technology (ICT) will affect the other very strongly. That was the reason they carried out dependability analysis for ensuring dependable power supply in future. They presented an approach which was extending the application of analytical approach to problem generally solved by simulation. Their approach combined structural and dynamic models and used their complementary advantages. They also showed the use of Markov Model during the pivotal decomposition to include dependencies between entities, limited repair facilities and other system dynamics .The problem with this approach is that it is highly complex [17].

S. Sridhar et al (2012) presented a layered approach for evaluation of risk based on the security of both the physical power applications and its supporting cyber infrastructure. They presented a classification which highlighted dependencies between cyber physical controls required to support the smart grid and the communication and computation that must be protected from cyber attacks. In their work, they provided an overview of smart grid operation, its associated cyber infrastructure, and power system controls which directly influence the quality and quantity of power delivered to the end user [12].but the work is still in early stage.

Ye Yan et al (2011) studied possible security vulnerabilities while deploying advanced metering infrastructure. They also explored various aspects relating to customer behavior, customer privacy and message authentication. They proposed an in-network collaborative scheme for providing secure and reliable communications in smart grid. There approach successfully provides data privacy, trust services and integrity. They also proposed a transmission scheme for facilitating data collection and management message delivery between smart meters and a local collector. They also proved their claim with the help of simulation [18].

R. Berthier et al (2010) emphasized on the security of Advanced Metering Infrastructure (AMI). For the purpose they categorized the available approaches to build secure architecture into three classes: prevention, detection and mitigation. They surveyed the literature to understand the better detection technology. Based on the different threats targeting the advanced metering infrastructure they presented the requirements and architecture for a comprehensive monitoring solution [19].

S. Mclaughlin et al (2010) discussed about the principle component of smart grid i.e. Advanced Metering

Infrastructure (AMI). AMI is replacing the analog meters with computerized systems that report usage over digital communication interfaces e.g. Phone lines. They pointed out the risks involved in this infrastructure. They documented the method a malicious user use to manipulate the data. They also performed penetration testing to validate these attacks. Their purpose was to demonstrate that despite of many benefits the AMI has severe security related drawbacks [20].they pointed out the problem but they did not give the proper solution.

G. N. Erricssion (2010) discussed that the development of communication capabilities, moving power control system from islands of automation to totally integrated computer environment have opened up new possibilities as well as new vulnerabilities. He emphasized the role of cyber security and Physical System Communication (PSC) system in conjunction with each other. He took cyber security issues and highlighted access points in a substation. They also modeled information security domain [21]. The approach is superficial in nature.

D. Major organizations working on smart grid security

Not only U.S. Government, initiatives has been taken from the Government of various countries for establishing successful smart grid infrastructure. Following are the Government organizations actively working in the area:

- ✓ NIST (National Institute of Standards and Technology)
- ✓ NEB (National Energy Board)
- ✓ IEC (International Electro-technical Commission)
- ✓ EPRI (Electric Power Research Institute)
- ✓ ISA (International Society of Automation)
- ✓ IEEE 1402-2000
- ✓ NAERC (North American Electrical Reliability Corporation)
- ✓ IGSTF(India Smart Grid Task Force)

i. Technologies being Deployed

Following is the wire and wireless communication technologies being deployed for making the grid smart:

- ❖ **Multiprotocol Label Switching (MPLS)**
  High - performance telecommunications networks used for data transmission between network nodes.
- ❖ **Broadband over Power Lines (BPL)**
  It is power line communication with Internet access.
- ❖ **Wireless LAN (IEEE 802.11 based)**
  It provides robust and high speed communications that allows multiple users to occupy the same frequency band with minimal degradation to other users.
- ❖ **WiMAX (Worldwide Interoperability for Microwave Access)**
  802.16 series standards for Wireless Metropolitan Area Network (WMAN), 3.5 GHz Licensed spectra allow higher power and longer distance transmission.

ii. The Grid Infrastructure and their Security Issues

The Smart grid security is crucial to maintain stable and reliable power system operation during the contingency situation due to the failure of any critical power system component. Ensuring a 'secured smart grid' involves with a less possibility of power grid collapse or equipment malfunction. Due to lack of the proper 'security measures', a major blackout may occur which can even lead to a cascading failure. Therefore, to protect this critical power system infrastructure and to ensure a reliable and an uninterrupted power supply to the end users, smart grid security issues must be addressed with high priority.The Smart Grid concept is evolved to make the power grid more energy efficient and intelligent. According to the US Department of Energy, smart grid can be defined as: "Smart grid generally refers to a class of technology people are using to bring utility electricity delivery systems into the 21st century, using computer-based remote control and automation. These systems are made possible by two-way communication technology and computer processing that has been used for decades in other industries. They are beginning to be used on electricity networks, from the power plants and wind farms all the way to the consumers of electricity in homes and businesses. They offer many benefits to utilities and consumers -mostly seen in big improvements in energy efficiency on the electricity grid and in the energy users' homes and offices.

iii. Advanced Metering Infrastructure (AMI)

Advanced metering infrastructure (AMI) is an integrated system of smart meters, communications networks, and data management systems that enables two-way communication between utilities and customers. Customer systems include in-home displays, home area networks, energy management systems, and other customer-side-of-the-meter equipment that enable smart grid functions in residential, commercial, and industrial facilities. The goal of an AMI is to provide utility companies with real-time data about power consumption and allow customers to make informed choices about energy usage based on the price at the time of used.

In smart grid, AMI plays a vital role in two way communication. If it is used in the power distribution system, it has the potential to save utility energy. Due to more efficient meter reading it is beneficial to both customer and supplier. In AMI networks, wireless devices are used in the smart meters located on the end point of the grid or distribution side customer's houses. Through AMI real time energy pricing is possible with the two-way communication networks between the utilities and their customers.

Despite of various benefits offered by AMI, following are the major issues involved while deploying AMI:

- ✓ Physical security of these wireless devices is a major concern along with cyber security.
- ✓ By using malicious software, device memory can be modified.
- ✓ Because of two way communication, control system may be compromised [22, 23].

iv. Phasor Measurement Units (PMU)

A phasor measurement unit (PMU) is a device which measures the electrical waves on an electricity grid using a common time source for synchronization. Time synchronization allows synchronized real-time measurements of multiple remote measurement points on the grid. The resulting measurement is known as a synchrophasor. Phasor measurement unit is also termed as Synchrophasors. This is used to measure real power; reactive power, frequency, and phase angle 12 times per cycle whereas previous measurement technology takes measurements every 2 or 4 seconds. PMU's sampling rate is 1.4 MHz.PMU contains information like bus voltage phasor, current phasor, network parameters and its location. With the help of PMU, operator can visualize the exact angular difference between different locations. GPS receivers, microprocessor based relay, disturbance fault recorder, IEEE standard make PMU for fast control to mitigate voltage collapse in low cost and time. Its advantage list is long as compared to previous technology but its security has become major concern as it involves the following issues:

- ✓ Break down infrastructure instrument may collapse the whole system.
- ✓ Its high measurement & controlling ability may attract attackers.
- ✓ Microprocessor devices data collector nodes could be programmed maliciously for sending messages regarding measured data which can cause damage to the power system.

III. RESULTS AND DISCUSSION

SCADA – The Brain of the Smart Grid

The term smart grid elicits a mental image of a fully automated power distribution system, capable of monitoring usage and voltage levels, constantly making adjustments to keep everything running at optimal levels. This vision does encapsulate what a true smart grid is able to deliver, but load tap changers, capacitor banks and recloses are not smart enough on their own to make adjustments; they have to be told when and how to respond. At the core of smart grid decision making is SCADA, supervisory control and data acquisition. Line sensors and other connected equipment on a smart grid provide a stream of data back to a central control room where the information is analysed and decisions are automatically made and executed, regulating voltage levels, optimizing efficiency, routing and generation. The SCADA system in the control room is able to make these automated decisions in real-time by running algorithms based on the data it receives and orchestrate adjustments to optimize voltages and self-heal any disruption issues.

SCADA (supervisory control and data acquisition) is a category of software application program for process control, the gathering of data in real time from remote locations in order to control equipment and conditions. SCADA is used in power plants as well as in oil and

gas refining, telecommunications, transportation, and water and waste control.

SCADA is efficiently monitoring an entire power system in real time efficiently [27]. This monitoring is performed by data acquisitions including meter reading, communication network. In SCADA, data is fetched with the help of sensors, Current Transformers (CTs), Potential Transformers (PTs) and Intelligent Electronic Devices (IEDs). This data is fed to a remote terminal unit (RTU). The control centre scans RTU's data and then displays the same. This provides a complete log of the system containing information like circuit breaker status, voltage measurement, current measurement, time of event, power flow etc.

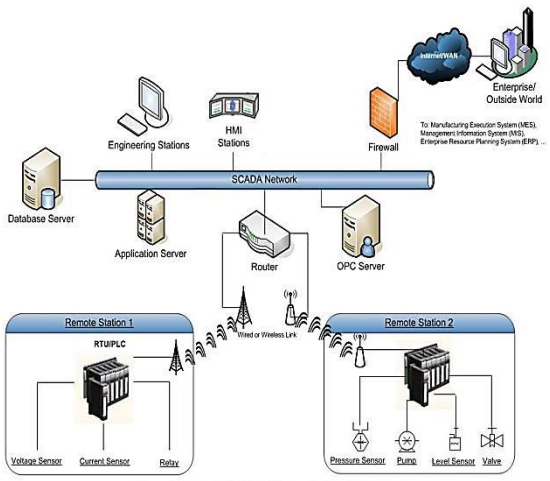

Figure. SCADA Network

SCADA control systems consist of set of application specific software called as energy management systems (EMS). Modern EMS provides information very helpful to power system monitoring and control. EMS ultimate tool is state estimate (SE) which is an on line application used for Contingency Analysis (CA). Though SCADA offers several advantages but suffers from limitations too. The reason behind August 2003 Northeast U.S. blackout is the misuse of the SCADA systems [24]. Following are the issues to be still worked upon:

- Existence of several vulnerabilities in the SCADA system architecture may invite the attackers very easily [25].
- Direct tampering of RTUs, communication links from RTUs to the control center is simple [25].

grid may become a major issue which can affect nation's economy.

a) Recommendations for Security Enhancement of Smart Grid

The transition from analog to digital electricity infrastructure has introduced the challenge of communication security and data management. As digital networks are more prone to malicious attacks from software hackers, security becomes the key issue to be addressed. In addition, concerns on invasion of privacy and security of personal consumption data arise. The data collected from the consumption information could provide a significant insight of consumer's behaviour and preferences. This valuable information could be abused if correct protocols and security measures are not adhered to.

If above two issues are not addressed in a transparent manner, it may create a negative impact on customer's perception and will prove to be a barrier for adoption. Despite of the efforts, most of the available literature related to security of the smart grid does not consider all the dimensions of smart grid security. Following are the few recommendations made after studying the literature available:

- There should be an approach which provides a holistic solution to the enhancement of security in smart grid.
- Since smart grid is a cyber-physical system hence the approaches available for security improvement must be different from those available for improvement of purely cyber systems.
- The wireless devices are used in the smart meters located on the customers' premises. Since these devices are outside the utility's physical security perimeter, they are at high risk of compromise. Hence, energy meter should be placed and protected more smartly.
- Each device should be password protected.
- Awareness programmers for consumers should be organized regarding grid security issues.
- Regular training of system engineers on cyber physical security issues.
- Regular filtering of bulk data for their usefulness.

IV.CONCLUSION

Though smart grid has introduced the possibility for affordable, reliable and sustainable supply of electricity .They have also taken along with them the risk of being manipulated, failed or compromised. The reason behind is the grid's dependency on its cyber infrastructure. Without a concrete attention given to security, smart grid's benefit cannot be achieved. Since smart grid is a cyber-physical system so the approaches available to be used for only cyber world shall not be fit for this cyber physical system. The researchers has discussed about the areas which still need attention to realize smart grid concept. Some guidelines have been suggested for improving smart grid security.

V. REFERENCES

[1]. Singari Pavan Kumar,Sande Krishna Veni, Y.B.Venugopal, and Y.S.Kishore Babu, "A Neuro-Fuzzy based Speed Control of Separately Excited DC Motor", IEEE Transactions on Computational Intelligence and Communication Networks, pp. 93-98, 2010.

[2]. V.S.K.Balijepalli, S.A.Khaparde,R.P.Gupta,and Y.Pradeep, "Smart Grid Initiatives and Power Market in India", In Proceeding IEEE ,pp. 1-7, 2010.

[3]. J. R. Roncero, "Integration is Key to Smart Grid Management", CIRED Seminar 2008: Smart Grid for Distribution, pp.1-4, june 2008.

[4]. X. Fang, S. Misra, G. Xue and D. Yang, "Smart Grid-The New and Improved Power Grid: A Survey"communication Surveys & Tutorials, 2012, IEEE 14(4), pp. 944-980.

[5]. E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi and C. Assi, "Communication Security for Smart Grid Distribution Networks", IEEE Communications Magzine, , pp. 42-49, January 2013.

[6]. B. Vaidya, D. Makrakis and H.T. Mouftah, "Authentication and Authorization Mechanisms for Substation Automation in Smart Grid Network", IEEE Network, pp. 5-11, 2013.

[7]. Eduardo F. Camacho, Tariq Samad, Mario Garcia-Sanz, and Ian Hiskens, "Control for Renewable Energy and Smart Grids,", January 2011.

[8]. X. Liang, K. Gao, X. Zheng and T. Zhao, "A study on Cyber Security of Smart Grid on Public Networks", In Proceeding of 2013 IEEE Green Technologies Conference, IEEE Computer Society, pp. 301-308.

[9]. J. Vijayan, BStuxnet renews power gridsecurity concerns, [Computerworld, Jul. 26, 2010. [Online]. Available:http://www.computerworld.com/s/article/9179689/Stuxnet_renews_power_grid_security_concer

[10]. A. Greenberg, "Hackers Cut Site's Power", In Forbes, January 2008.

[11]. S. Spoonamore and R.L. Krutz, "Smart grid and cyber challenges – national security risks and concerns," March 2009, available online: http://www.whitehouse.gov/files/ documents/cyber/Spoonamore-Krutz- Smart Grid Cyber Security Risks and Concerns.pdf

[12]. R. Raghunath, I. Lee, L. Sha, J. Stankovic, "Cyber Physical System- The Next Computing Revolution", In Proceeding of Design Automation Conference 2010, ACM, pp. 731-736.

[13]. Jeena et al, "Challenges of Smart Grid", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,Vol. 2, Issue 3,pp.976-981, March 2013

[14]. S. Sridhar and A. Hahn and M. Govindarasu, "Cyber Physical System Security for the Electric Power Grid", In Proceedings of the IEEE, 100(1), 2012, pp. 210-224.

[15]. A. Hahn, A. Ashok, S. Sridhar and M. Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid", IEEE Transactions on Smart Grid, vol. 2, no. 2, June 2013, pp. 847-855.

[16]. A. Anwar, A. Mahmood, "Cyber security of smart grid infrastructure", The State of the Art in Intrusion Prevention and Detection, CRC Press, Taylor & Francis Group, USA, January 2014, pp. 449-472.

[17]. K. C. Sou, H. Sandberg and K. H. Johansson, "On the Exact Solution to a Smart Grid Cyber-Security Analysis Problem", IEEE Transactions on Smart Grid, vol.4, no. 2, June 2013, pp. 856-865.

[18]. E. Bou-Herb, C. Fachkha, M. Pourzandi, M. Debbabi and C. Assi, "Communication Security for Smart Grid Distribution Network", IEEE Communication Magazine, January 2013, pp. 42-49.

[19]. J. Wafler and P.E. Heegard, “A Combined Structural and Dynamic Modeling Approach for Dependability Analysis in Smart Grid”, In Proceeding of SAC’13, ACM, 2013, pp. 660-665.
[20]. Y. Yan, Y. Qian and H. Sharif, “A Secure and Reliable In- Network Collaborative Communication Scheme for Advanced Metering Infrastructure in Smart Grid”, In Proceeding 2011 IEEE Wireless Comminications and Networking Conference (WCNC), 2011, pp. 909-914.
[21]. R. Berthier, W. H. Sanders and H. Khurana, “Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions”, In Proceeding of First IEEE International Conference on Smart Grid Communications, IEEE, 2010, pp. 350-355.
[22]. S. Mclaughlin, D. Podkuiko and P. McDaniel, “Energy Theft in Advanced Metering Infrastructure”, Critical Information Infrastructure Security, Lecture Notes in Computer Science, Springer, vol. 6027, 2010, pp. 176-187.
[23]. G. N. Erricssion, “Cyber Security and Power System Communication- Essential Parts of a Smart Grid Infrastructure”, IEEE Transactions on Power Delivery, vol. 5. No.3, July 2010, pp. 1501-1507.
[24]. F. Li, W. Qiao, H. Sun, H. Wan, Y. Xia, Z. Xu and P. Zhang, “Smart Transmission Grid: Vision and Framework”, IEEE Transactions on Smart Grid, vol. 1, no. 2, 2010, pp. 168-177.
[25]. Eng. Adnan Sahen, “ Smart Grid ”, 4NEWHAMAK,Suria, September 2012.
[26]. Goodspeed, Travis, Darren R. Highfill, Bradley A. Singletary, “Low-level Design Vulnerabilities in Wireless Control Systems Hardware,” Proceedings of the SCADA Security Scientific Symposium 2009 (S4), pp. 3-1–3-26, January 21–22, 2009.
[27]. Sameer Saadoon Mustafa,Iraq,Mahmud Khidr Salman, “Study the Iraqi National Super Grid Power Flow Based,”, 201O 7th International Multi-Conference on Systems, Signals and Devices,pp. 978-983.
[28]. Richard DeBlasio, “Standards for the Smart Grid” ,IEEE Energy,USA, November, 2008.