INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)
ISSN 2278 – 7631 (Print)

Cyber Security For Smart Grids Using Cognitive Radios

Rajeev Srivastava
Humanities and Social Science Department
Jaypee University of Engineering and Technology, Raghogarh, Guna (M.P.), India
Divyanshu Kapoor
Research and Technology Department
Landis+Gyr Limited (part of Toshiba Corporation), Noida, India

Abstract:
This paper is motivated and inspired from the National cyber security policy of India 2013 and the upcoming Smart Grids. In this, the approach to bring up the smart grids for human welfare in a secure way is discussed. Further, recent initiatives and the for the communication in smart grids the concept of cognitive radios is discussed which can handle the network architecture of smart grids in intelligent fashion.

Key words*: Smart Grids, security, Process Control Systems Cognitive Radios*

1. Introduction

Smart Grid is a complex architecture connecting all human made technological developments along with upcoming advancements interconnected within cyberspace [1]. This provocative concept involves uncertain risks from cyber attacks which can be intentional or unintentional, thoughtful or mishaps thereby leading to disastrous impacts. Cyber space involves people, technology and services. To create a secure communication establishment for smart grid network which works with trust and confidence involving electronic talkbacks between network devices is the need of present time to setup smart grid portfolio. This paper looks into those issues which make it necessary to consider the cyber security aspect of grids which include smart and resilient next generation networks.

International forum and bodies on smart grids (like IEEE, ITF etc.) are working on standards[5] and setting up a common platform to communicate between cheap and small devices among each other through wireless and other media access. The dimension of applications for these networks are wide spreading from wireless telecommunications, environmental, medical, monitoring, heating and ventilation sensors, automotives etc. This is planned to be implemented using embedded devices and controllers which will intervene the human survival and living.

The main concern which is of prior importance is the attacks focused to home are networks, advanced metering infrastructures and electric generation utilities. For dealing this, standard based solutions which are well proven in advanced, developed for open architecture have to imbibed in the nourishment and upbringing of smart grids. Addressing all network points with a secure measure and making them recumbent to these probable disturbances for a smooth functioning of smart grids can be made achievable. The rate of common attacks which includes hacking, terrorism, viruses has shown an ever rising trend in past few years, hence intimating the present outrage to develop highly sophisticated tools which can intrude into secure networks through weak-leaky links is a challenge to tackle for smart grid cyber security.

Cyber security of smart grids has been a key concern of the present times and many initiatives have been taken depending upon mainly the geographical origin and type. Cyber security for smart grids is important to prevent and protect smart grids from the attacks aimed at disturbing the communication system protocols on an overall basis. These attacks can damage the system hence protecting them from such attacks, otherwise detecting the incurred attack and responding to it in the best possible resiliency form is the overall perspective which has been aimed to understand by the means of this paper. This needs to be understood as the upcoming technologies for the advent of smart grid systems and solutions, as the two way communication involved in this upbringing of the demand and provisions must be secure in all diversified approaches.

Some of these approaches which can be dealt from the beginning of the upcoming secure smart grids are listed as the following four step model:

i. **Well framed architectural algorithms for monitoring and analysis:** Within these smart grid communication protocols lots of data streaming will happen from the utilities, control centers, substation hubs, monitorial agencies etc. hence strongly instrumented and carved approaches and algorithms for monitoring and analysis of this is prior need for setting up such grids which are safe from cyber attacks.
ii. **Detection of probable mischievous activities:** If certain potential abnormalities are observed in the architectural plan of smart grids then certain mechanism should be framed in order to categorize them into threats and dangers which are potentially hazardous.
iii. **Defense against Cyber Attacks:** Once a categorical cyber attack is detected which can hamper the system stability, methods and procedures have to be undertaken in order to bypass, reroute and protect the remaining network from this disruption. Few of the know algorithms for cyber defense include rerouting, network partitioning and in pursuance of power defense: generation shift, load shedding, reactive power dispatch, controlled islanding are few concepts.
iv. **Modeling and virtual simulation:** For the per se of the above applicability's we need a simulation environment where we can test and measure the implications of cyber attacks on smart grids and accordingly fortune our thinking and methodologies to tackle such threats.

As the security analysis of smart grids is the prime concern which also associates risk analysis for such system, we require a full proof virtualization of the concept so as to understand the implications of cyber attacks. This can also help in creating shield which in conclusion makes the smart grid automatically forfeit from any of the cyber threats and attacks.
Major concern regarding the security of smart grids is its easy vulnerability to the attackers. There are many factors constraining the roadway to reduce this vulnerability of smart grids. Few of them enlisted below:

- **Dependencies on the legacy systems**
  This concern is one of the most stealthy issue as the smart grid backbone lies within the legacy power distribution system which have existed since ages. They will continue to work which at present have insufficient security mechanisms and considerations.
- **Long term perspectives**
  Deployment of smart grids would be done keeping a long term perspective in mind which will be more than the life span of usual networking systems hence these system deployments have to be adaptable with the future upgrade and modification capabilities.
- **Inapplicable physical safety**
  Smart grid network elements will be more easily accessible from any location instead of substations and can be infected with ease thereby increasing the threat in the cyberspace.
- **Geographically disperse**
  The extent of smart grid system on the geographical map would be vast which makes it difficult to manage and maintain creating a error and threat prone web with limited accessibility.
- **Interoperability of proprietary communication systems**
  Smart grid systems involves various groups, forums, organization on private and public levels hence an architecture from physical medium to application perspectives should be interoperable in terms of technology and protocols keeping in view all the security aspects.
- **Policy and standards framework**
  The present circumstances for security in smart grids lack in international policy and standard documentation, regulations, good and bad practices, economic or financial guidelines, technical detailed analysis, information sharing, research and development on a robust platform. This needs to brought up in a rigorous manner.

Process Control Systems (PCS)[2] are used to control and monitor power grids. Most common PCS for electrical power grid is Supervisory Control and Data Acquisition (SCADA) system. Since the PCSs will be controlling physical aspects of the electric power grid, the security of these systems is very important. When a computer is compromised only the data on the computer is compromised, and in extreme cases some of the hardware in the computer may be damaged. When a PCS is compromised, multi-million dollar equipment can be physically damaged in addition to data being lost. In extreme cases it can cause human injury or loss of life. The most important security objective of the PCS is availability. The electrical power system must be available at all times, so the PCS controlling the power system must also be always available. The integrity of the PCS is the next important security objective. It will not be able to make correct decisions if it is given false data as input. Confidentiality is the least important security objective. The PCS needs to run in real time, and that means the system must have minimal overhead. Implementing confidentiality may be too time-consuming to meet latency requirements.
Keeping in view the above criticalities for understanding the need of security for smart grids , certain measures and initiatives are mentioned considering the present environment in this domain of technological and managerial future research initiatives to make smart grids secure:

- **International agency**
  An association of public bodies from different countries, which support its members, seeks to achieve common goals and collaborates with other similar agencies and even non-member countries.
- **Industry association**
  An association that supports and protects the rights of a particular industry and the people who work in that industry, and which seeks to achieve the common goals of its members. There may be a public entity within these associations, but it does not have a leading role.
- **Public Private Partnership**
  A government service or private business venture which is funded and operated through a partnership of government and one or more private sector companies.
- **Public body:** An organization whose work is part of the process of government, but is not a government department.
- **Regular private organization**
  An organization which is privately run and does not rely on money from the government and funds from charities. They get make their own money by providing a service at a cost.
- **Professional association**
  Also called a professional body, professional organization, or professional society. A professional association is usually a non-profit organization seeking to represent a particular profession, the interests of individuals engaged in that profession, and the public interest.
- **Specialized event**
  Workshops, forums, conferences or summits focusing on cyber security.
- **Online resource**
  A specialized website, blog, e-forum, online group, and similar resources.
- **Project**
  Simulation and virtual projects portraying the security of smart grids.
- **Other**
- When an initiative or an organization does not match with any of the previously defined types, it will be classified with this value.

2. Recent Initiatives

The research and development of robust and secure communication protocols, dynamic spectrum sensing, and distributed and collaborative security should be considered as an inherent part of smart grid architecture. An advanced decentralized and secure infrastructure needs to be developed with two-way capabilities for communicating information and controlling equipment, among other tasks, as indicated in the recently published "Guidelines for Smart Grid Cyber Security Vol.1" by the National Institute of Standards and Technologies. The complexity of such an endeavor, coupled with the amalgam of technologies and standards that will coexist in the development of the smart grid, makes it extremely necessary to have a common platform of development, with flexibility and reliable performance.

Field programmable gate arrays (FPGAs) development platforms share these advantages, not to mention the fact that a single silicon FPGA chip can be used to study several smart grid technologies and their implementations. FPGA chips offer significant potential for application in the smart grid for performing encryption and decryption, intrusion detection, low-latency routing, data acquisition and signal processing, parallelism, configurability of hardware devices,

and high-performance and high-bandwidth tamper-resistant applications. A distributed FPGA-based network with adaptive and cooperative capabilities can be used to study several security and communication aspects of this infrastructure both from the attackers and defensive point of view.

Revolutionary communication architecture is required for effective operation and control of smart grid, and cognitive radio[3] based communication architecture can provide a solution. Cognitive radio refers to the wireless systems that are context-aware and capable of reconfiguration based on the surrounding environments and their own properties. In the same frequency range, there are two coexisting systems: the primary system and the secondary system. The primary system refers to the licensed system with legacy spectrum. This system has exclusive privilege to access the assigned spectrum. The secondary system refers to the unlicensed cognitive system, which can only access the spectrum that is not used by the primary system. The primary system refers to the licensed system with legacy spectrum. This system has exclusive privilege to access the assigned spectrum. The secondary system refers to the unlicensed cognitive system, which can only access the spectrum that is not used by the primary system.

3. Conclusion

By leveraging cognitive radio technology and imbibing the security aspect into the proposed communications infrastructure promises to utilize potentially all available spectrum resources efficiently in the smart grid environment making them secure and relying.

4. References

1. National Cyber Security Policy 2013, India Ministry of Communication and Information Technology, Department of Electronics and Information Technology.
2. Manimaran Govindarasu , Adam Hann and Peter Sauer "Cyber-Physical Systems Security for Smart Grid Future Grid Initiative White Paper" Iowa State University,2012.
3. Ruiliang Chen, Jung-Min Park, Y. Thomas Hou, and Jeffrey H. Reed, "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks" Virginia Polytechnic Institute and State University.
4. W. Sanders, "Tcip: trustworthy cyber infrastructure for the power grid," Tech. Rep., Information Trust Institute, University of Illinois at Urbana-Champaign, 2011.
5. Naveen Sastry and David Wagner, "Security Considerations for IEEE 802.15.4 Networks"