Chapter - 6

ISSUES AND CHALLENGES IN REALIZATION OF SMART GRID COMMUNICATION INFRASTRUCTURE

CHAPTER-6
ISSUES AND CHALLENGES IN REALIZATION OF SMART GRID COMMUNICATION INFRASTRUCTURE

This chapter addresses the major concerns for safety and security of Smart grid network. EMI issues and challenges as well as Cyber security issues are discussed which can be useful for future research endeavors. Different cyber-attacks are also depicted.

6.1. INTRODUCTION

An existing power grid is being transformed into heterogeneous, complex, advanced and layered architecture at a very rapid pace. Amalgamation of ICT, power electronics devices and numerous communication standards results into advancement with several challenges [71, 72]. Hierarchical network layers with diverse set of protocols inflicts various cyber security challenges. Unification of communication infrastructure and electrical network enacts electromagnetic interference [73]. Various grid components such as WAN, network devices, switches, transmission lines, transformers, generation equipment, SCADA etc. are vulnerable to EMI threats and its adverse effects. Causes of conducted and radiated Electromagnetic Interference (EMI) must be known so that their effects and consequences can be mitigated to avoid hazards and catastrophic events. Moreover, WSN being an inevitable part of Smart grid communication architecture, imposes security challenges of diverse nature due to its vulnerabilities.

A secured, robust and reliable infrastructure is inevitable for gigantic amount of data communication. Safety and security of Smart grid infrastructure are the huge challenges to overcome. Interoperability and scalability are also of a major concern for reliable operation of Smart grid network. Various standards for security and safety are being developed by various leading organizations such as ANSI, IEEE and IEC. This chapter describes various concerns and challenges in realization of Smart grid infrastructure.

6.2. EMI ISSUES AND CHALLENGES IN SMART GRID INFRASTRUCTURE

EMI can be defined as an interference generated from external or internal sources due to conducted or radiated emissions. EMI affects adversely to the electronics devices and components which results into performance degradation [73-80].

Smart grid is a gigantic network comprising of various electronics and electrical components such as transmission lines, conductors, transceivers working at various frequency bands, transformers, generating equipment, SCADA, renewable energy sources, switches, power electronics converters and network devices such as routers, switches etc. Integration of all these diverse set of devices and equipment is highly vulnerable to radiated and conducted emissions. The span of adverse effects of EMI is from malfunction of devices to disastrous events. In existing grid, the low and medium frequencies below 1 GHz are taken into consideration for EMI issues. While in Smart Grid, communication standards operate in the range of above 1 GHz and mostly 2.4 GHz. Moreover, many standards operate in the same 2.4 GHz band which is of the biggest concern for EMI issues. Smart grid integrates wired and wireless communication standards along with electronics and electrical apparatus which makes it vulnerable to radiated as well as conducted EMI. The classification of various causes of EMI is depicted in Fig.6.1.

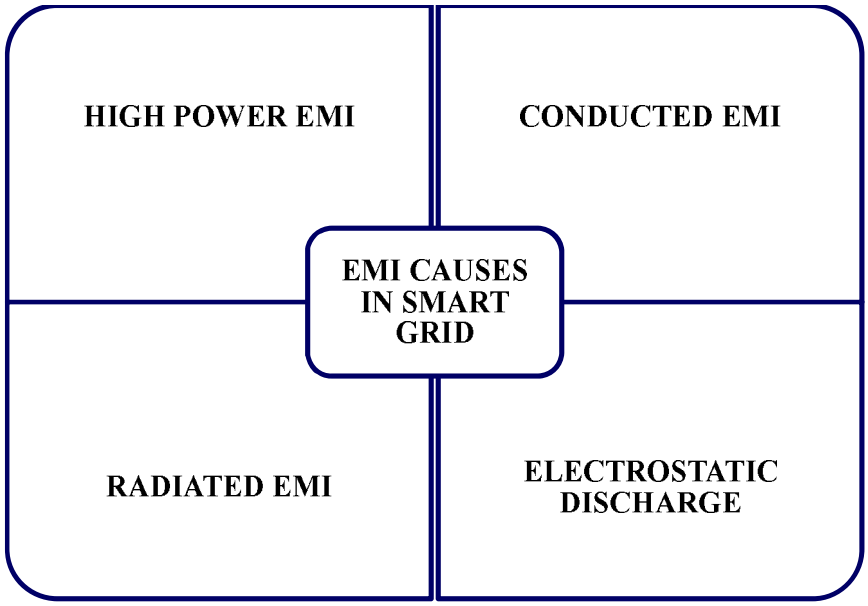

Fig.6.1. EMI Causes in Smart Grid

6.2.1. High Power EMI

High power EMI is due to geomagnetic storms produced as a result of solar activity and pulses. Corona flares and sunspots are caused by constant solar activities. Solar activities repeat every eleven years. The solar cycle reaches at its peak every hundred years. An interaction between magnetic field of earth and charged particles

produced from solar activities results into geomagnetic disturbances which is a high power EMI.

Geomagnetic storms causes varying currents through neutral of transformer in the high voltage grid [73]. This may cause damaging effects on grid. An Intentional EMI is the term used to point out a deliberate effort of impairment of the device or grid network through conducted and/or radiated EMI. This attacks are performed by means of high power microwave pulses, electromagnetic artilleries or nuclear activities. This attack can result into destruction of equipment, jamming and denial of service. High altitude EMI pulses are caused through bursts at above 30 Km of earth's surface. This is caused by powerful EM pulses [74]. These pulses can penetrate through the boundaries of substation and destroy equipment. It can also couple with transmission lines and cause damaging effects.

6.2.2. Conducted EMI

Major sources of conducted EMI are power electronics converters, devices and renewable energy sources. Conducted EMI spreads through cables, transmission lines and conductors. There are many sources of conducted EMI such as switching, lightning and inductive circuits [75]. Various power electronics converters can produce harmonics due to high speed switching. Interface between various electronics devices can cause conducted EMI. Conducted EMI can be produced at both AC and DC side in the grid when solar panel is connected in the microgrid. An aggregation of various EMI sources produce further damaging effects. Conducted EMI can reach over longer distances through transmission lines and cause destructive effects [76]. Inverters and rectifiers located at the substations cause broadband EMI pulses.

6.2.3. Radiated EMI

Radiated EMI can be due to either wireless communication transceivers or high voltage discharges [77]. The most crucial province of Smart grid infrastructure is its communication network comprising of layered and heterogeneous architecture. Communication infrastructure of Smart grid comprises of diverse set of communication standards for HAN, NAN and WAN operating in various frequency bands. The radiation from various communication transceivers is a major source of radiated EMI. Harmonics, frequency conversion products and inter modulation products of transceiver modules can

cause radiated EMI [78-80]. Smart meters are crucial for data communication in Smart grid for billing and usage statistics. Smart meters operate using various communication standards such as Wi-Fi, Zigbee, Bluetooth, WiMAX, LTE etc. Co-existence of various frequencies from different sources is the biggest concern for radiated EMI.

Radiated EMI can also be produced as a result of spurious signals which do not fall into the spectrum being used in the operation of various smart grid transceivers. The causes, effects and remedies of radiated EMI must be meticulously studied and analyzed to avoid its damaging effects on grid.

Surface arcing and corona discharging as a result of various electronics circuits operating in Kilovolts can cause radiated EMI. Switching and gap sparks are the major sources of radiated EMI. Microgrid is categorized as DC or AC microgrid. It expedites the usage of renewable energy resources. Various power electronics converters are used as per the requirements. These converters are operated through fast switching of various power electronics devices mostly using Pulse Width Modulation (PWM) method. This fast switching produces radiated EMI in lines. Integrated switches and oscillators operating at high frequencies also produce EMI effects.

6.2.4. Electro Static Discharge (ESD)

Two or more electronics or electrical devices having different electrostatic potential in the vicinity of each other or having direct contact exchange or transfer electric charge and cause ESD. ESD can take place when a moving electronics device come in the vicinity of a static device or when an equipment with cables is relocated from one place to another. ESD can also be caused due to high humidity level in data centers [78]. It can be mitigated by controlling the difference in static voltages between various devices [81, 82].

Various standards such as IEC 61000 series, IEC 60255, ANSI C12.1, ANSI C63.12, IEEE 1613, IEEE 60870-2-1, IEEE 1909.1, OIML R 46-1 and 2 etc. can be used for testing of Electromagnetic compatibility [81, 82].

6.3. CYBER SECURITY ISSUES IN SMART GRID COMMUNICATION INFRASTRUCTURE

Smart Grid is being transformed from idea to actual execution and deployment. There are several issues and challenges to be deciphered during design, development and

deployment process. Cyber security is one of the key challenges for secured and reliable operation of Smart grid technology [83-87]. Cyber security can be defined as safeguard from exactions transported by computer network and/or terminals and the safekeeping of assets from alterations or damage from inadvertent or malicious use of software based control amenities.

Smart grid communication infrastructure integrates WSN, communication transceivers, AMI, SCADA, electronics devices with firmware, and various network devices entailed for hierarchical communication network layers [88-90]. All these components are crucial and inevitable for Smart grid communication infrastructure. These components are vulnerable to cyber-attacks. NIST has provided guidelines for standardization of cyber security. [90, 91]. Cyber security is a ubiquitous concept as Smart grid is an always on network comprising of IoT. Conceptual model of various Smart grid cyber security outlying areas defined by NIST and IBM are depicted in Fig.6.2.

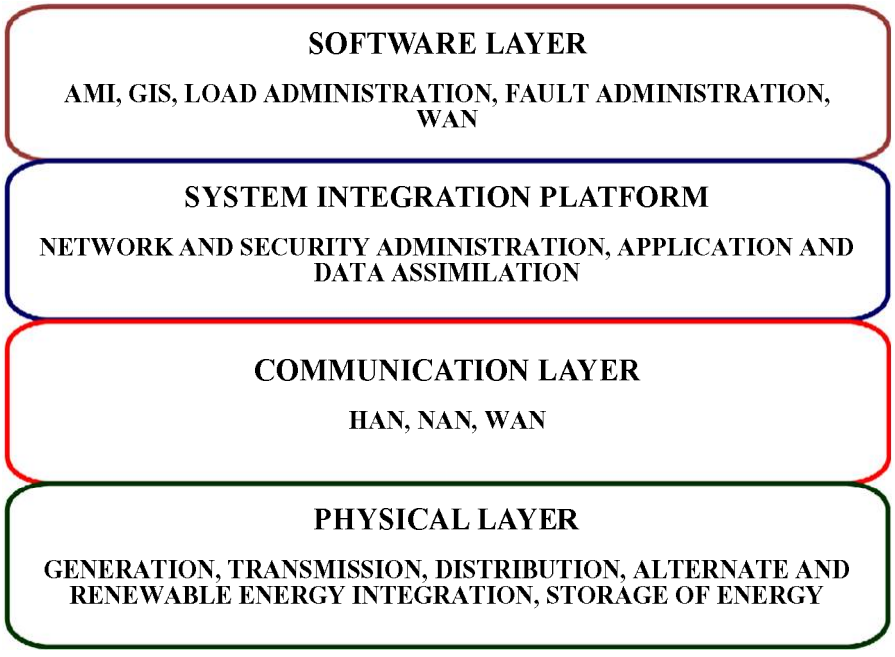

Fig.6.2. Conceptual model of Smart grid

Siemens's SIMATIC-WinCC SCADA system was attacked in July 2010 by Stuxnet. As per Symantec's statistics, around 45000 networks have been affected as a result of cyber-attacks till time around the globe. Confidentiality, obtainability of real time data and authenticity of information are the three most basic and crucial

requirements of reliable and secured operation of Smart grid. Various cyber-attacks are depicted below [86-88, 92].

6.3.1. Denial of service (DoS) attack

Smart grid comprises of IoT which is an IP based network. Each and every device and equipment connected in the network contains a unique IP address. In the DoS attack, an authenticated user is denied service as a result of exploitation of network services by intruders. An attack is performed by altering the network configuration of legitimate user. The confidentiality of the information is hindered by attackers [93-97].

6.3.1.1. Identity Spoofing

In this attack, trespasser imitate authenticated and authentic user without any password. Most of the usual attacks are network spoofing, message replays, man in the middle, software manipulation etc. [98-100].

6.3.1.2. Side channel attacks

These attacks are performed by exploitation of encrypted information. The purpose of these attacks is to gain the control of Smart grid management system. Some of the common side channel attacks can be listed as power analysis, electromagnetic analysis, timing attack etc. This attack hampers the confidentiality and authenticity of network [86-88, 98].

6.3.2. Password stealing

Password snuffling or dictionary attack is performed to hamper the confidentiality of network user. It is either social engineering or technical attack to steal the password of legitimate user.

6.3.3. Eavesdropping

Eavesdropping is performed on various network layers. IP packets are sniffed by intruders by hindering the wireless transmission at various network layers. Confidentiality and security of Smart grid communication network is violated as a result of this attack.

6.3.4. Malware attack

Malware is a vindictive program containing worms. Viruses, backdoors, trapdoors, Trojan horse, logic bomb etc. are some of the examples of malware. Malware attack can also be formed by pre insertion of malicious program which may attack the system in future.

6.3.5. Intrusion

The purpose of this attack is to attain the control of entire system. It results into malfunction of network devices and violation of confidentiality, authenticity, and integrity of the system. IP scans and port scans are performed to perform this attack.

6.3.6. WSN security

Wireless sensor network can be defined as a congregation of sensor nodes to acquire and communicate the information pertaining to various measured parameters such as current, temperature, humidity etc. Real time monitoring and control of various heterogeneous and hierarchical networks is the most crucial feature of Smart grid technology [101-104]. WSN forms the base of Smart grid communication infrastructure. WSN comprises of power supply unit (mostly battery), transceivers, memory, processor, and location finding system.

The security aspects and challenges for WSN must be differently addressed due to its design and functionality limitations [105]. In a typical communication network, the address of transmitter and receiver are important for data communication but WSN comprises of redundant nodes for data communication and so the transfer of data is more important than the address of a specific node. For example, the readings pertaining to humidity, temperature, or current may be sent from any of the node place in the particular region and thus data collection becomes more important. WSN differs in terms of its information oriented approach compared to address oriented approach of traditional communication network. Moreover, the computational ability of WSN node is very limited which prevents an application of advanced and memory consuming algorithms for security measures [106]. This limitation enhances the security consideration for the sake of safekeeping of redundant nodes. WSN security is the most critical, vulnerable, complex and puzzling aspect of Smart Grid security. Various challenges of WSN are depicted in Fig.6.3. Fig.6.4. depicts the classification of various WSN attacks.

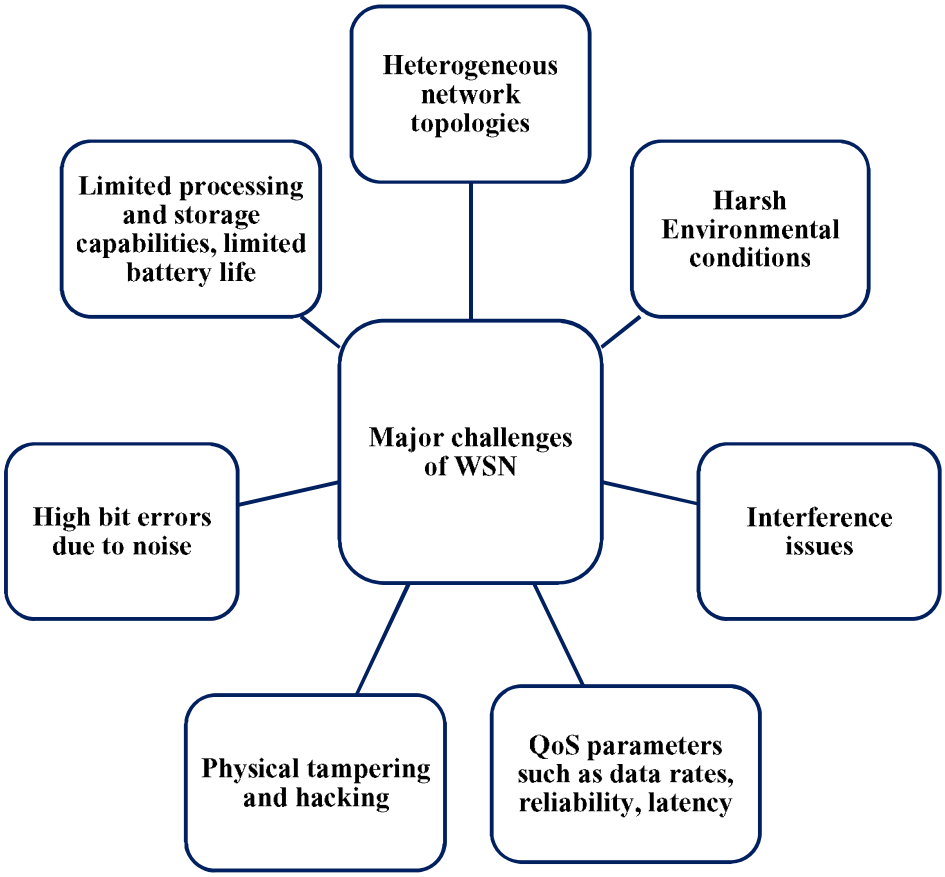

Fig.6.3. Major challenges of WSN

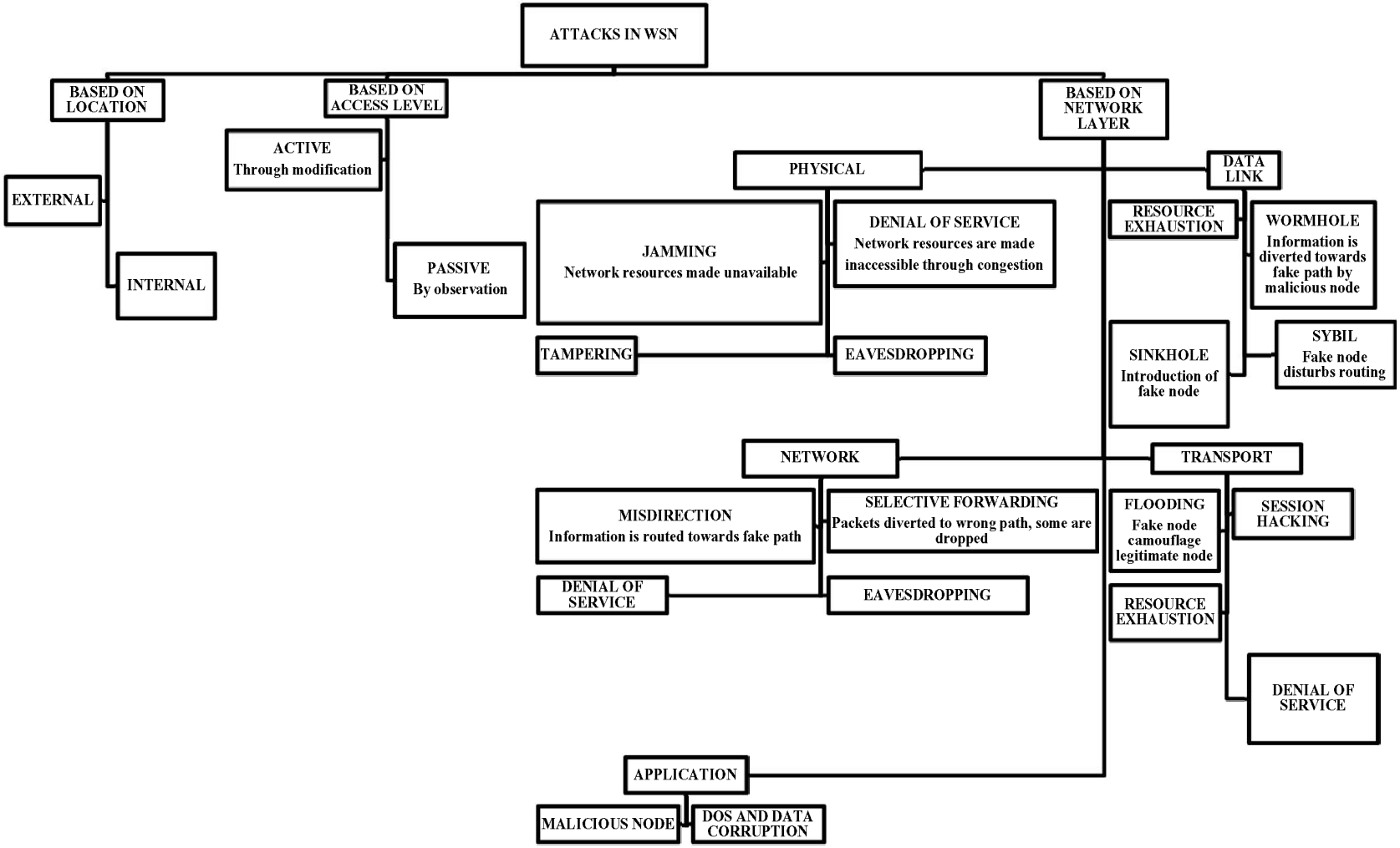

Fig.6.4. Types of attacks in WSN

Smart grid standardization activities are being carried out by some of the institutions and organizations such as NERC-CIP, IEEE and NIST [107]. NISTR-7628 illustrates the guidelines for complete Smart grid infrastructure [108]. IEEE 1686 describes the cyber security guidelines for IEDs at substations. Still more research endeavors are required for establishment of completely secured Smart grid cyber-physical architecture. Smart grid is a gigantic network comprising of sub-networks. Several protocols and standards are integrated for realization of Smart grid architecture. The Smart grid network architecture must be reconfigurable to withstand various dynamics. The network must be robust enough to manage uncertainties and complexities of operation. Reliability of Smart grid is a huge challenge to overcome. Integration of renewable energy resources for energy generation has introduced new challenges such as consistency of power supply, load profile, scattered resources, forecasting etc. pertaining to reliability of power grid. Efficiency of Smart grid technology is also one of the major challenges to overcome due to complex architecture of Smart grid comprises of diverse energy sources, EV, PHEV, microgrid, WSN, distinctive loads, AMI and SCADA.

CHAPTER SUMMARY

An integration of various electrical equipment, transceivers, power electronics converters and communication standards makes the system vulnerable to EMI effects which may result into disastrous events. Different EMI effects such as conducted, radiated, high power and ESD are specifically classified for Smart grid network. Furthermore various cyber security issues and attacks are also classified. Harmonization between various standards is inevitable to overcome the above mentioned challenges. This chapter is expected to serve as a directive for future research endeavors.