Chapter - 2

LITERATURE REVIEW

CHAPTER-2

LITERATURE REVIEW

This chapter depicts the survey of an existing literature carried out to understand the concept of Smart grid technology and its various components. The gap areas are identified from the reviewed papers for design and implementation of prototype. The findings from various research papers are briefly described in the chapter.

2.1. LITERATURE REVIEW

Smart grid is a multi-faceted technology with integration of electrical and communication infrastructure. Numerous areas of smart grid design and development such as communication standards, security issues, reliability aspects, optimization techniques, safety issues, standardization, electric vehicles, Plug-in hybrid electric vehicles, micro grid design, power converters, renewable integration, test bed development etc. are explored by researchers.

Various facts and statistics of Indian energy scenario are illustrated in [1] to [6]. These facts exemplify the need of transformation in energy sector. India's energy scenario is depicted in [1]. The deficit energy is in Indian power sector is 0.6 percent. Still 6088 villages are deprived of electricity [2]. Decentralization energy can be achieved by using renewable energy resources. India has a great potential for renewable energy sources [2]. Aging of coal based thermal power plants [4] is an important motivational factor behind development of new technology and decentralization of energy. Primary energy resources are scarce in nature which necessitates the use of alternative and renewable energy resources [5]. Furthermore, distribution and theft losses degrade the efficiency of transmission and distribution. An IoT enabled Smart grid infrastructure can resolve these issues through monitoring and control of real time data and AMI [6].

Y. Yan et al. have discussed motivations, requirements and challenges of Smart grid communication infrastructure in [7]. Authors have discussed that as Smart grid technology may reach up to millions of customers and comprises of enormous devices, reliability and security aspects become extremely crucial and complex. Vulnerabilities of Smart grid technology especially for SCADA system and threats are also discussed. Authors have depicted state of the art review of various aspects of Smart grid technology.

H. Farooq et al. [8] have reviewed various options available for an implementation and deployment of Smart grid communication architecture. Authors have analyzed the characteristics of IEEE 802.11 as well as IEEE 802.15.4 standards using simulator. Gungor et al. [9] have discussed various standards and technologies for Smart grid communications.

At present, the power grid is ill-suited for the necessities of 21st century. Real-time communication of information is vital for delivery of power from utilities to consumer premises in Smart grid technology. Scalability, security, interoperability, robustness, reliability, availability and Quality of Service (QoS) are the most significant requirements of Smart grid technology [9]. Amin et al. [10] have discussed wireless standards for heterogeneous Smart grid technology. Scheduling algorithm is also proposed by authors in [10]. Microgrid plays a pivotal role to provide clean energy and distributed generation. Shah et al. have discussed a solar microgrid in [11]. Various renewable energy resources such as solar, wind, hydro etc. can be explored in microgrid architecture.

Elkhorchani et al. have explored microgrid with solar, wind and battery as energy sources. They have also considered the microgrid architecture with island and grid connected modes in [12]. Upgradation of existing power grid requires a robust and reliable communication infrastructure. Self-healing, dynamic power control in grid connected as well as island mode, dynamic and smooth switching between modes etc. necessitates an integration of intelligence with microgrid architecture. Moallem et al. have discussed hierarchical power management and dynamic functionalities using Matlab simulations in [13]. AC grid technology is cost effective and simple compared to DC counterparts. Remarkable improvements and implementations have been made in the area of solar PV technology in last decade. Shenai et al. [14] have discussed a scalable DC microgrid for community, residential and commercial usage using solar and wind sources.

Communication infrastructure is inevitable for microgrid in order to achieve reliability, efficiency, economy, flexibility and fault tolerance. Bahramara et al. have discussed various components of Smart microgrid technology and described a planning of different renewable energy sources using HOMER simulation tool in [15]. A smart micro grid can be defined as a low voltage small grid connected to medium grid. Biagi et al. have developed the method of active power dispatching in smart microgrid in [16]. Mulla

et al. have reviewed various wireless communication standards for Smart grid architecture in [17]. IEEE 802.15.4 based WirelessHART technology is described in [18].

Power electronics converters are required for an integration of renewable energy resources. Authors have discussed various challenges such as harmonics and transients produced as a result of inverter usage. Bera et al. and Athreya et al. have discussed significance of smart meters in Smart grid technology in [19, 20]. Parvez et al. have discussed and proposed suitable frequency band for HAN and NAN. Authors have proposed 2.4 GHz band for NAN and 868/915 MHz band for HAN applications in [21]. Alamifar et al. [22] have discussed an optimization of WiMAX standard for Smart grid communication using network simulator tool. Authors have investigated and optimized different parameters such as duration of frame, traffic characteristics and choice of scheduling strategies and category of service in [22]. PHEV is one of the innovative component of Smart grid technology. For PHEV, communication interface is required between vehicle, power supply and grid. Kaebisch et al. have implemented the set-up of electric vehicle using IEC 61850 standard in [23]. Smart grid technology has drawn an attention of various stakeholders and researchers due to its inventive and advanced features. An implementation of Smart grid technology enforces enormous challenges in different environments in terms of mobility, climatic conditions and geographic locations. Authors in [24] have proposed cognitive radio based solution for reliable communications. Hartmann et al. in [25] have discussed Smart grid communication topologies for real time data. Alamifar et al. have examined and proposed the viability of powerline communications in Smart grid technology in [26].

Traffic in Smart grid communication can be categorized as traffic for home area network and traffic for distribution automation. Authors have proposed narrowband and broadband powerline communications for various applications of Smart grid using simulation results in [26]. Smart grid communication network comprises of HAN, NAN, and WAN layers. Various communication standards for Smart grid technology are reviewed by Mahmood et al. in [27].

Lee et al. have discussed a comparative study of various local as well as personal area network standards on the basis of frequency band, data throughput, coverage area etc. in [28]. Ma et al. [29] have discussed opportunities, communication standards, challenges, and importance of WSNs in Smart grid architecture. Microgrid is an

inevitable component of Smart grid technology to expedite the usage of renewable energy resources and to reach the remote areas with limited or no electricity facility. Real time, secured and comprehensive data communication is vital for Smart grid network.

Xu et al. have discussed various communication standards for interconnected Smart grid systems and networks in [30]. A consumer premises or household network is a crucial element of Smart grid network for information exchange with smart meters, energy management system, smart appliances and plug-in hybrid electric vehicles. Selection of proper communication protocols having low power consumption, simple design and operation, security, high data rate, adaptability, reliability, broad coverage and low deployment and operational cost is vital for home area network [31].

Personal area network is applicable for data logging in Smart grid network. A detailed review of IEEE 802.15.1 standard is described in [32]. Communication standards such as WiMAX, Wi-Fi, cellular, Zigbee etc. are discussed and compared in [33]. WirelessHART is an IEEE 802.15.4 based protocol mainly used for industrial automation. It provides short distance communication in terms of few hundred meters between different devices. Chen et al. have discussed the applications of WirelessHART for real time industrial automation in [34, 35].

Fernandez et al. have presented a concept of Smart city with IEEE 802.11 as well as IEEE 802.15.4 standards. They have depicted simulation results using Jemula simulator in [36]. Data communication is the core characteristic of Smart grid network. Internet of Things (IoT) will require huge amount of information exchange for real time monitoring and control. High data throughput and reliable communication is inevitable for efficient operation of Smart grid network. Perahia et al. [37] have discussed multi Gbps wireless local area network for higher data rates in Gbps using 60 GHz frequency band. If the implementation this standard is successful, then it can be a quantum leap towards IoT in Smart grid. Camps et al. [38] have reviewed and analyzed direct Wi-Fi technology for device to device communication.

Wireless mesh network is an essential part of wireless sensor networks which forms a base of Smart grid communication infrastructure. IEEE 802.11 series of standards are globally established for reliable wireless communications. Hiertz et al. [39] have reviewed IEEE 802.11s standard which is an improved version of IEEE 802.11 family of standards in terms of high data throughput and mesh networking. Wireless mesh

technology facilitates connection between various devices. Peer to peer connection improves data throughput, load balancing, fault diagnosis, monitoring and control of communication network. Thus, wireless technologies are better compared to their wired counterparts in terms of enhanced and easily expandable connectivity.

In [40], Lee et al. have reviewed various standards for mesh networking. IEEE 802.16 group of standards are aimed for metropolitan area networks. Xergias et al. have proposed a scheduler for providing different treatment to various data connections based on QoS in [41]. Ghosh et al. have explored the features and future opportunities of WiMAX standard in [42].

Cellular communication standards and technologies can be a backbone of Smart grid communication infrastructure. 5G can provide enhanced data throughput, extensive device support, and Multiple Input Multiple Output connectivity. Gupta et al. have presented a survey on 5G technology in [43]. 5G network can be implemented for Smart grid network as it has an ability to facilitate ubiquitous communication network. Gohil et al. have discussed the merits and applications of 5G technology in [44]. Real time management of entire Smart grid network necessitates huge bandwidth for data communication. Bandwidth is a limited resource. Cognitive radio technology facilitates efficient spectrum utilization by facilitating the use of unoccupied spectrum space. IEEE 802.22 standard is established for cognitive radio applications. Cognitive radio based Smart grid applications have many advantages such as efficient spectrum usage, economical operation and distance coverage etc. [45].

Machine to Machine communication (M2M) is an inevitable feature of Smart grid communication infrastructure as it facilitates communication, processing and control among devices with minimal human intervention. Cognitive radio can efficiently reduce spectrum scarcity issues and facilitate efficient M2M communication in Smart grid network [46]. Yu et al. have depicted a hierarchical architecture of Smart grid network based on cognitive radio in [47].

Smart grid communication infrastructure must be able to handle interconnected data communication with heterogeneous communication networks. Ghassemi et al. have proposed a model of Cognitive radio based WAN for Smart grid communication network in [48]. Cognitive radio technology can enhance network performance by its adaptive performance. Gungor et al. [49] have described an application of cognitive radio

technology in various Smart grid domains such as Monitoring, control, distribution generation, smart metering, power failure detection and home automation.

Wireless sensor networks are critical constituents of Smart grid in terms of spectrum usage, energy restraints, reliability and security. An adaptive and opportunistic operation of cognitive radio network can proficiently address these challenges and requirements [50].

Bu et al. [51] have proposed a heterogeneous model of Smart grid network with real time billing and demand side management. Smart grid is a multi-layered and heterogeneous network. Sreesha et al. have proposed an energy saving routing algorithm for Smart grid home area network in [52].

Hierarchical Smart grid architecture, spectrum sensing mechanisms, applications, architectures, challenges and future research are rigorously analyzed by Khan et al. in [53]. Cognitive radio technology facilitates adaptive spectrum access, interference prevention, adaptive data rates and critical data communication in emergency scenarios [54].

Various wireline as well as wireless communication standards are inevitable for information exchange in Smart grid technology. Design constraints and trade-offs for these technologies are discussed by Sebaali et al. in [55]. Hoch has reviewed and compared G3 PLC and PRIME wireline technologies in [56]. Berganza et al. have discussed results and analysis of PRIME deployment in [57]. Braun has analyzed Broadband over Powerline technology (BPL) for Smart grid applications in [58]. Brissette et al. [59] have discussed IEEE 802.3 standard for home automation in Smart grid context. Hung et al. [60] have proposed cross layer design for WiMAX mesh network for interference aware scheduling and routing.

Cross layer optimization approach considers collaborative design approach between various network layers. Shah et al. have proposed a cross layer approach based on Lyapunove drift optimization for WSN performance enhancement in [61]. Wireless local area network can be handled by backbone network. Cross layer approach is advantageous in terms of QoS and throughput enhancement. Concept of cross layer design is depicted in [61]. Shakkotai el al. have discussed cross layer approach in [62].

Home area network is one of the hierarchical network of Smart grid architecture. It consists of intelligent devices, smart meters and wireless sensor nodes. Wireless sensor nodes accumulate and transfer the data to smart meters. Smart meters are linked with utilities through neighborhood and wide area networks to communicate the statistics of energy usage.

Various communication standards such as IEEE 802.11, IEEE 802.15.1, IEEE 802.15.4, IEEE 802.16 etc. are suitable for home area networks. Piyare et al. have discussed an implementation of Bluetooth based home automation system in [63]. Young et al. have described transmission of ECG data using patch sensor on Bluetooth radio link in [64].

Kumar et al. have discussed mobile based home automation system with IoT in [65]. Zigbee is a personal area network working on 2.4 GHz band. It facilitates mesh connectivity and simple firmware interface. Most of the research work on home automation explores Zigbee technology.

Fang et al. have developed Zigbee based intelligent home automation system in [66]. Most of the technologies applicable for wireless personal and local area networks operate in 2.4 GHz band. So, an issue of coexistence of various wireless technologies at same frequency must be considered. Domínguez et al. [67] have presented findings and recommendations for interference avoidance during Zigbee and Wi-Fi coexistence. Rathod et al. have developed home automation using Zigbee technology with light sensing, temperature sensing and intrusion detection system in [68]. Ghazal et al. have depicted smart home concept using multi control chandelier using Zigbee technology in [69]. Hua et al. have designed smart home system using Zigbee network and Ethernet interface in [70].

Kantarci et al. have discussed various issues and challenges for Smart grid deployment in [71]. Real time monitoring, control, and self-healing features of Smart grid technology rely on machine to machine communication. Subhani et al. have analysed various challenges and issues for device to device communication such as security, interference, spectrum scarcity, standardization, energy efficiency etc. in [72].

Radasky et al. have presented high power EMI threats and their impacts in [73] and [74] respectively. Yu et al. have discussed EMI impacts and considerations for Smart

grid network in [75]. Thomas has reviewed conducted emission in distribution system of electric grid in [76]. Smart meter is an integral part of Smart grid technology. It will produce intentional as well as unintentional emissions. Intentional EMI is directly involved with transmission of information. Unintentional emissions are caused due to out of the band spurious EMI. Tyndall et al. have discussed potential EMC problems for various Smart grid components such as smart meters, display and various communication equipment in [77]. Smart grid comprises of various power electronic converters for reliable operation in the presence of diverse energy sources. Switching of various power devices cause EMI. Smolenski et al. have discussed EMI threats due to power electronics converters in Smart grid in [78] with the help of experimental investigations. Proliferation of Smart grid technology has imposed critical challenges. Yu et al. [79] have discussed testing considerations for safety, EMI and environmental compliance.

Duffy et al. have discussed various standards for electromagnetic compatibility in [80]. Electromagnetic interference can be classified in two major categories such as narrowband and wideband. The peak electric fields contained in narrowband EMI threat is greater than 100 V/m. It is a very high power threat. It may result into malfunction of an equipment such as failure due to thermal heating. Wideband EMI is spreaded over a broad range of frequency.

The energy density of wideband EMI is very less at a specific frequency. There are less chances of thermal heating but the repetitive frequencies can produce malfunction. Publicly accessible computer systems can be damaged as a result of either radiated or conducted EMI [81]. Test methods and installation requirements for Smart grid communication equipment is depicted in [82]. Smart grid network can be realized though reliable and secured data communication. As it is a hierarchical and heterogeneous network with multiple layers, cyber security is the biggest challenge for secured operation of Smart grid. Line et al. have discussed various cyber security challenges for Smart grid network in [83]. Liu et al. have discussed various security issues for AMI, SCADA etc. components of Smart grid system in [84].

IoT is an inevitable component of Smart grid communication for real time monitoring and control of entire network. Real time statistics of various networks as well as commands are communicated using Internet. Granjal et al. have reviewed various security issues for IoT in [85]. Anu et al. have discussed various risks in the operation of

Smart grid in [86]. Smart metering is a breakthrough concept of Smart grid technology for various types of metering and billing based on time of the day use. Anzalchi et al. have discussed various issues and countermeasures for secured metering infrastructure in [87]. Meraj et al. have depicted impacts of cyber-attacks on Smart grid network in [88]. Khaitan et al. have discussed cyber physical methodology for electrical grid in [89].

Accessibility of real time statistics and secrecy of data are the most imperative characteristics of secured Smart Grid infrastructure. Cyber security is vital for authenticity and integrity of information communicated at various network layers using heterogeneous communication protocols. Hu et al. have described cyber architecture of Smart grid and standardization activities in [90].

Standardization of cyber security is the most crucial requirement for reliable operation of Smart grid network. Wang et al. have discussed some of the research endeavors in Smart grid information security in [91]. Yang et al. have discussed effects of cyber security issues on Smart grid network in [92]. Smart grid comprises of distributed energy resources as well as distribution automation. Tinton et al. Have depicted various stretagies for Smart grid cyber security in [93]. SCADA, programmable logic controllers and distribution systems are integral part of Industrial control systems. Colella et al. have presented an analysis of sequential cyber threats by considering Zigbee protocol in [94].

Schukat et al. have depicted cyber threats for machine to machine communication in [95]. Authors of this paper have suggested the use of transport layer protocol for IP based Smart grid infrasrructure. The communication protocols used in Smart grid infrastructure are highly vulnerable to cyber threats. Cyber-attacks may result into sequential disaters, malfunction of system and expenditure. Yan et al. Have presented a survey on Smart grid cyber security in [96]. Smart grid is the most gigantic and complex infrastructure of present era. Security of information is a crucial requirement of Smart grid operation. Moreover, Smart grid being a consumer centric technology, trust of consumers on safe operation of the network is essential. Ling et al. Have presented the descriptive data analysis of twelve countries and derived sixteen security requirements in [97].

Smart meters are integral components of HAN as they communicate the collected statistics pertaining to energy consumption to utilities. Security as well as system recovery are inevitable features of Smart meter. Mahmud et al. [98] have discussed

threats and solutions for cyber-attacks on Smart meters. Authors have suggested various solutions such as bidirectional encryption, authentication, intrusion detection etc. The stochastic nature of various renewable energy resources makes the system vulnerable to cyber-attacks. Moness et al. have discussed cyber threats for wind energy systems in [99].

Bad data can be injected from either cyber side or physical side for intrusion and exploitation of actual information. Password stealing, device catastrophe, worm attack, intrusion etc. are some of the possible cyber-attacks. Wang et al. have discussed an experimental investigation of bad data injection attacks in Smart grid network in [100]. Smart grid is a cloud based network. Moreover, it uses some of the ISM standards which are also termed as open standards. This makes the system more vulnerable to cyber threats as analyzed by Puttonen et al. in [101]. Smart grid is a data centric technology. Cyber security and interoperability are major challenges of Smart grid network. Shutang et al. have analyzed data architecture for Smart grid in [102]. Smart grid is an amalgamation of physical and cyber components which makes it vulnerable to cyber as well as physical attacks pertaining to hardware and software. Macana et al. have discussed various cyber as well as physical vulnerabilities of future grid in [103].

Distribution automation is one of the key feature of Smart grid technology. Kiani et al. have discussed various reliability and operational issues for Smart microgrid cyber physical architecture in [104]. Wireless sensor network is the most vulnerable component of Smart grid technology. Due to their limited storage and processing capabilities, security issues for WSN must be handled differently. Can et al. have depicted various cyber-attacks and intrusion detection system for WSN in [105]. WSN is vulnerable to passive as well as active attacks. Neogy has depicted various challenges, attacks and security measures against cyber-attacks using cryptography, key management and routing protocols in [106].

The pivotal part of cyber-physical safety and security is recognized by various organizations. The institutions like NIST, IEEE and NERC-CIP have designed and developed the guidelines for Smart Grid cyber security. Harvey et al. have presented a survey and analysis of NISTIR 7628 guidelines for cyber security in [107]. FitzPatrick et al. have discussed action plans for NIST framework for cyber security issues in [108].

2.2. RESEARCH GAPS

Smart grid technology is going to bring a massive transformation in an existing power grid. There are enormous research areas which are being explored in electrical as well as ICT domain. Present research work investigates some of the areas such as demand side management, Smart meters, PHEVs, distribution automation, Microgrid operation and management, centralized and decentralized grid operation and control, renewable integration, multi agent based Smart grid operation, choices available for Smart grid communication, review of various communication protocols etc. Most of the prototypes are developed using IEEE 802.15 standard which is a PAN and does not facilitate an integration with backbone network.

This research work explores some of the gap areas derived from the review of existing literature. Comparative analysis and various factors affecting an appropriateness of a specific communication protocol are not extensively explored in an existing literature. Moreover, interoperability between various communication standards and devices is a major and crucial issue to be addressed for realization of Smart grid communication infrastructure. Suggestive framework for interoperable communication protocols for deployment of entire Smart grid network is not broadly explored in existing literature. This thesis illustrates design and implementation of communication infrastructure for all hierarchical layers of Smart grid network through prototype development. Cross layer or joint optimization is inevitable for performance enhancement of ubiquitous Smart grid network.

This thesis includes some of the major research gaps derived from the literature review such as comparative analysis of communication standards for smart grid, implementation of IoT based network and cross layer optimization of IEEE 802.11 based networks. The experimental research work explored in this thesis includes design and development of prototype using IEEE 802.3, IEEE 802.15.1 and IEEE 802.11 communication standards.

CHAPTER SUMMARY

This chapter depicts a brief illustration of referred literature for understanding of Smart grid technology and identification of gap areas. There are many diverse research endeavors to be explored in the area of Smart power grid. As the Smart grid is a

developing technology, still some of the areas are less explored in the literature. Design and development of complete IoT based infrastructure of Smart grid network, comparative analysis and network optimization are identified as research gaps to carry out this research work.