

Microgrid Energy Management System

by

Ashray Gururaja Manur

*A project report submitted in fulfillment of the
requirements for the degree of*

*Master of Science
(Electrical Engineering)*

at the

UNIVERSITY OF WISCONSIN-MADISON

December 2015

APPROVED BY :

V. Venkatesh

Advisor: *Prof. Giri Venkataramanan*

Professor

Advisor Title

26 Jan 2016

Date

Abstract

The concept of microgrid is emerging to be a viable approach to integrate various types of electricity sources and storage devices within or close to load locations. While the fundamental technical features of microgrids have been demonstrated in laboratory and field settings, a large number of operational issues remain to be solved before they can become widespread. Chief among them is an approach for asset or energy management within the microgrid. In contrast to the well-established centralized electricity grid enterprise, microgrids are expected to be small in scale and maintain a peer-to-peer interaction among devices with rough parity between supply and demand in terms of size. In this scenario, it is critical to have a robust operational protocol within the microgrid to prioritize and manage loads, sources and storage to prevent the collapse of the microgrid. This study presents the design framework for a Microgrid Energy Manager (MEM) which uses the internet of things (IoT) paradigm and wireless sensor networks (WSN) to overlay a communication and control layer for real-time energy management in microgrids.

Acknowledgements

My deepest gratitude is to my advisor, Prof. Giri Venkataramanan. His passion towards the subject and thrust to take engineering research beyond the walls of the laboratory is phenomenal. I'm thankful for his time, support and mentorship which has shaped my abilities as an engineer and a researcher.

My sincere thanks to Prof. Suman Banerjee (Computer Sciences), Prof. Sarada (School of Business), Prof. Alfonso Morales (Urban and Regional Planning) and Prof. Nancy Wong (School of Human Ecology). I am grateful to them for lending me their expertise, guidance and collaborating with me on some exciting projects.

I would like to thank Raul Martins, Zeng Fan and Jared Pierce for helping me in the development and de-bugging of the hardware platform. I would like to extend my gratitude to the Wisconsin Electric Machines and Power Electronics Consortium (WEMPEC) faculty, students and the administrative staff for making it a world class research group.

All of this would not have been possible without the constant support and encouragement of my family and friends. I'm grateful to my father, Gururaja Manur for his spot-on pragmatic advice on academics, life and beyond, my mother, Rekha Manur for encouraging the dreamer in me and my sister, Anusha Manur for the sheer brilliance that she is.

Contents

Abstract	i
Acknowledgements	ii
1 Introduction	1
1.1 Introduction	1
1.2 Microgrids: Definition	2
1.3 Overview of Microgrid Energy Manager	2
1.4 Goal	5
1.5 Document Organization	5
2 Microgrid Energy Management: State of the Art	6
2.1 Microgrid Control	6
2.2 Wireless Communication Framework for Microgrids	9
2.3 Cloud Computing for Microgrids	11
2.4 Summary	12
3 Microgrid Network (MN)	13
3.1 Introduction	13
3.2 IEEE 802.15.4	13
3.3 Microgrid Sensor Network	17
3.4 Summary	23
4 Microgrid Cloud	24
4.1 Introduction	24
4.2 Cloud Computing	24
4.3 Microgrid Cloud (MC) Physical Infrastructure	25
4.4 MC Framework	26
4.5 Summary	30
5 Experiments and Results	31
5.1 Microgrid Network Architecture	31
5.2 MEM Hardware Platform	32
5.3 Wireless Sensor Network (WSN) for Microgrids	35
5.4 MSN Conclusion	46
5.5 Cyberphysical System (CPS) for Microgrids	47
5.6 CPS Tests Conclusion	51
Conclusion and Future Work	52
A MEM Gateway and Node Schematics	53

List of Figures

1.1	Typical microgrid architecture	2
1.2	Microgrid Energy Manager Architecture	4
2.1	Centralized Energy Management System	8
3.1	Network Topologies in IEEE 802.15.4	14
3.2	Mesh Topology	14
3.3	Tree Topology	14
3.4	IEEE 802.15.4 communication stack	15
3.5	IEEE PHY Frame Structure	16
3.6	IEEE MAC frame structure	16
3.7	LWM Network	18
3.13	MSN algorithm overview	21
3.14	MSN ACK handler	22
3.15	MSN response handler	22
4.1	MC system architecture	26
4.2	MicroE command set	27
4.3	Sample request and response commands	27
4.4	Setting up MEM users	28
4.5	Setting up MEM grid	29
4.6	MEM heartbeat	29
4.7	MicroE command set	30
5.1	MicroE request-response mechanism	32
5.2	MEM hardware architecture	32
5.3	MEM Communication Board	34
5.4	MEM Power Interface Board	34
5.5	Physical Environments	36
5.6	Linear Topology Test	37
5.7	RSSI and LQI variation for linear topology in the laboratory	38
5.8	PRR and RRR for linear topology in the laboratory	38
5.9	Microgrid Reliability Test for linear topology in the laboratory	39
5.10	Distributed Topology in the laboratory	39
5.11	RSSI and LQI for distributed topology in lab	40
5.12	PRR and RRR for distributed topology in the laboratory	40
5.13	Distributed topology in home	41
5.14	RSSI and LQI for distributed topology in home	41
5.15	PRR and RRR for distributed topology in home	42
5.16	Microgrid reliability test for home environment	42
5.17	RSSI and LQI for linear topology in field	43
5.18	PRR and RRR for linear topology in field	43
5.19	MRF for linear topology in an open field	44
5.20	PRR and RRR for distributed topology in an open field	44

5.21	RSSI and LQI for distributed topology in field	45
5.22	PRR and RRR for distributed topology in field	45
5.23	RTT variation over the course of the experiment	48
5.24	RTT variation per day basis	49
5.25	RTT variation due to interference	50

List of Tables

5.1	MicroE Sample Request and Response Commands	32
-----	---	----

List of Abbreviations

SCADA	Supervisory Control and Data Acquisition
PCC	Point of Common Coupling
WSN	Wireless Sensor Network
IoT	Internet of Things
MN	Microgrid Network
MC	Microgrid Cloud
MG	Microgrid Gateway
MEM	Microgrid Energy Manager
DER	Distributed Energy Resource
DSM	Demand Side Management
EMS	Energy Management System
UC	Unit Commitment
PLC	Power Line Communication
DNO	Distribution Network Operator
MGCC	Microgrid Central Controller
LC	Local Controller
CAN	Controller Area Network
WLAN	Wireless Local Area Network
LAN	Local Area Network
AP	Access Point
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
QoS	Quality of Service
DoS	Denial of Service
PRR	Packet Reception Ratio
LQI	Link Quality Indicator
RSSI	Received Signal Strength Indicator
MAC	Medium Access Control
TCP	Transmission Control Protocol
IP	Internet Protocol
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
SOAP	Simple Object Access Protocol
LWM	Light Weight Mesh
FFD	Fully Functional Device
RFD	Reduced Function Device
PAN	Personal Area Network
PLME	Physical Layer Management Entity
PPDU	PHY Protocol Data Units
MPDU	MAC Protocol Data Units
AODV	Ad-hoc On Demand Distance Vector
HTTP	Hyper Text Transfer Protocol

SOA	S ervice O riented A rchitecture
RRR	R esponse R eception R atio
MRF	M icrogrid R eliability F actor
CPS	C yber P hysical S ystems
ISP	I nternet S ervice P rovider
ACK	A cknowledgment
RF	R adio F requency
RTT	R ound T rip T ime

Chapter 1

Introduction

1.1 Introduction

Today's electricity grid can be broadly sub-divided into four categories: electricity generation, transmission, distribution and utilization systems. Generating stations are connected to the distribution system through transmission lines and the distribution system connects all the loads in a particular region. For a number of reasons, both technical and economical, individual power systems are connected together to form power pools. These regional or area electric grids operate independently, but are also interconnected to form a national grid. This paradigm is based on a centralized infrastructure. However, there is an emerging trend to move towards a more de-centralized energy supply and control with the emergence of microgrids [1]. Microgrids are aimed at solving some problems of centralized grid system such as

- **Environmental challenges** - traditional power generation systems are a major cause of man-created carbon dioxide emissions [2]. This needs a shift towards greener sources of energy. Also, natural catastrophes such as earthquakes, hurricanes, tornado make the electricity grid highly susceptible to failure.
- **Infrastructure challenges** - with decreasing investments and ageing infrastructure, it has become difficult for making improvements to meet the increasing load demand leading to congestion and unreliable power supply.
- **Integration of innovative technologies** - with the existing infrastructure, it will be difficult to integrate advancements in materials, power electronics and communication technologies.

While the basic principles of a power system remain the same for a centralized grid and a microgrid, they differ in many aspects.

- **Energy sources** - microgrids tend to have a higher mix of renewable energy sources when compared to a traditional grid.
- **Coordination and Protection System** - Due to high penetration of power electronic interfaces, microgrids show a lower inertial characteristics. This means that the conventional control and design concepts are insufficient for microgrids.
- **Critical demand-supply balance** - In islanded microgrids, coordination among different entities in the microgrid is a complex problem. This is challenging due to the critical demand-supply balance.

This illustrates that traditional communication and control infrastructure used in centralized grids cannot be applied directly in microgrids. There is a need for an advanced control and communication scheme which is intelligent, low-cost, low-power and time-sensitive.

1.2 Microgrids: Definition

Microgrid is defined as a small cluster of distributed generation units, loads, energy storage systems that can work when connected to the main grid or as an island in a disconnected state from the main grid [3].

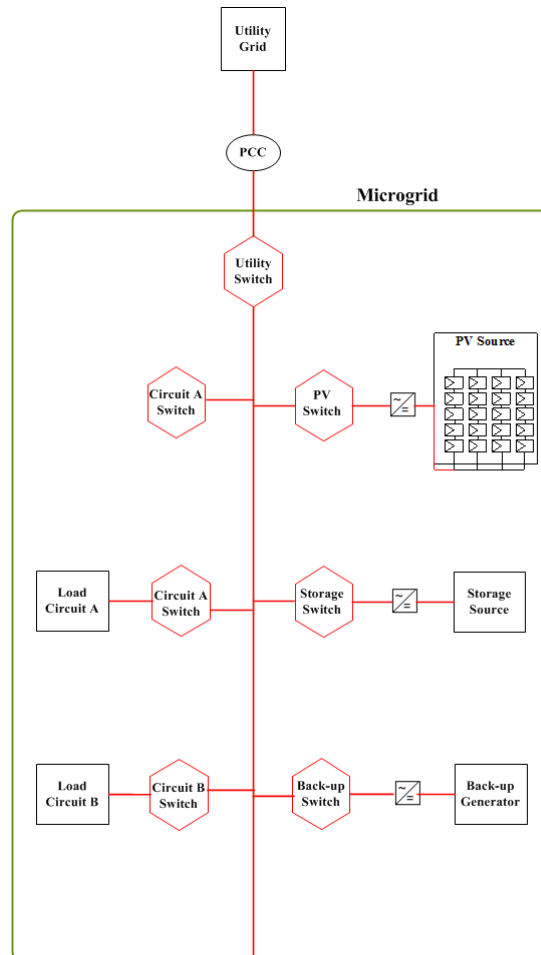


FIGURE 1.1: Typical microgrid architecture

A microgrid can operate in grid connected mode and island mode with the capability of handling the transitions between these two modes of operation [4]. In grid connected mode, the power deficit can be supplied by the main grid. When the microgrid is operated in an island mode, the microgrid controller or manager is responsible for the balance between the real/reactive power, loads and the storage units.

1.3 Overview of Microgrid Energy Manager

The concept of microgrid is emerging to be a technically viable approach for meeting reliable supply of electricity with increased availability in the presence of large scale grid disturbances induced by severe weather events, as well to integrate various types of electricity sources and storage devices. A microgrid is expected to have several features such as, scalability, stable operation in grid-tied and islanded modes of operation, among others. Several researchers have developed techniques to ensure stable operation of the microgrid with various types of configurations, controllers, generators,

loads, etc [5]. However, all these approaches that ensure stability are predicated upon the condition that the total demand in the system is less than the total supply in the system, and that the system operates without reaching its capacity margins. When the total demand exceeds the supply capacity, the question of stability is moot, and the system collapses. Nevertheless, when the total generation capacity is roughly in par with the nominal demand, and that loads typically operate asynchronously at-will, and that generation sources may potentially be non-dispatchable, such scenarios would be common enough, calling for a suitable energy management system. It is designed to have the following functional capabilities

- Immediate wireless remote switching control of loads
- Scheduled switching control of loads and sources
- Prioritized switching of loads to maintain margin between supply and demand
- Real-time load or source status tracking
- Time of use for each load or source
- Daily, weekly and monthly load or source based reports for each user

In order to perform these functions with a high degree of flexibility in communications, various technologies are integrated to develop a platform with a general architecture illustrated in *figure 1.2*. All the user interactions with the microgrid, sources and loads take place through personal input/output devices such as smart phones, personal computer or mobile phones. These interactions are mediated through the Microgrid Cloud (MC). The microgrid cloud interacts with the microgrid through the internet with the Microgrid Gateway (MG) using a local Access Point (AP). The MG communicates to all the load and sources through various microgrid nodes (MN).

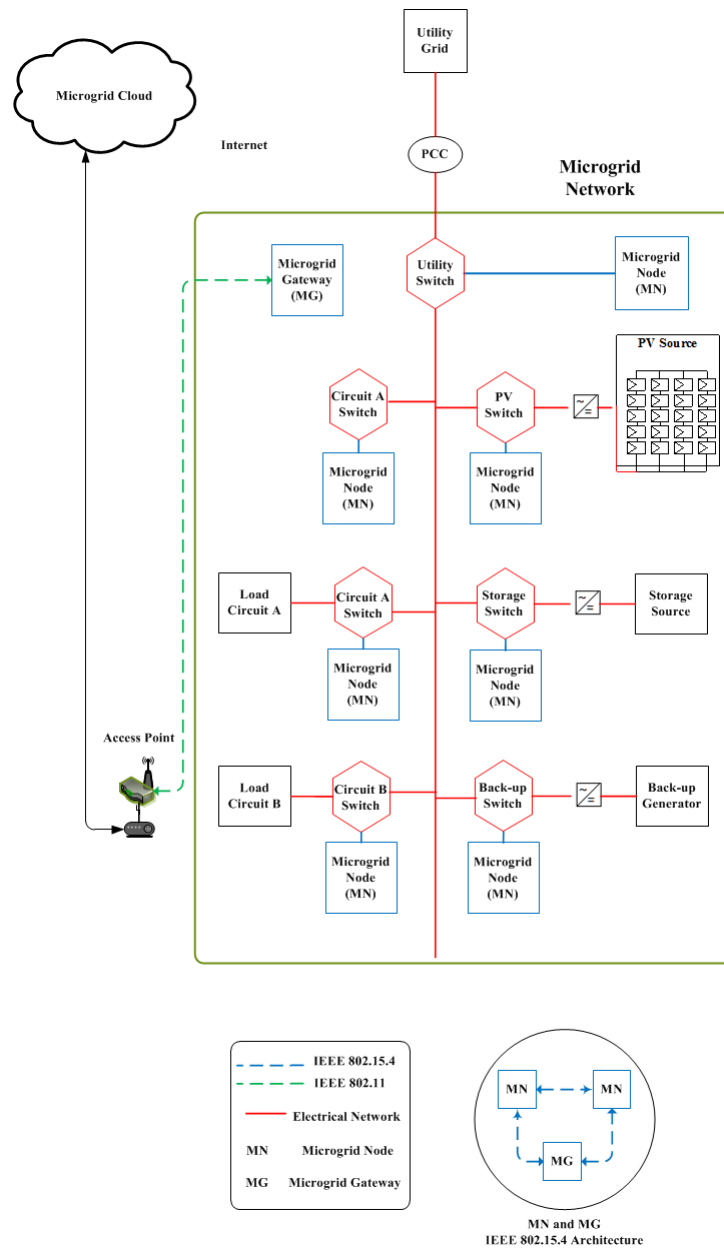


FIGURE 1.2: Microgrid Energy Manager Architecture

1.4 Goal

As the electricity grid makes a transition from a centralized scheme to a distributed and a greener paradigm, several challenges arise. Energy management is one of the most important challenges in a microgrid in both grid connected state (when it is connected to the utility grid) and islanded mode of operation (disconnected from the main grid and works as a standalone system). In instances where the energy supply is roughly in par with the nominal load, a robust control and management system is necessary. The inherent or the primary layer of control based on droop control mechanisms are insufficient when there is a critical energy supply-demand balance. There is a need for a secondary and tertiary control and management systems to maintain grid stability. This study presents a new framework for energy management system which has the capabilities to provide secondary and tertiary control. Integrating advanced communication capabilities, an end-to-end solution is presented which includes both hardware and software solutions. The asset management system is built on Internet of Things (IoT) paradigm and Wireless Sensor Networks (WSN). The study focuses on developing hardware and software platforms for management system and studying the interaction between different cyber components and the physical system.

1.5 Document Organization

In Chapter 2, a detailed literature review is presented. It includes topics directly and indirectly related to control and management of microgrids. Since the core component of a management system is the communication framework, different wireless technologies have been reviewed. Chapter 3 and Chapter 4 present the Microgrid Sensor Network (MSN) and the Microgrid Cloud (MC) respectively. Chapter 5 describes the experiments and results of two studies conducted on cloud and embedded system framework and the performance evaluation of Microgrid Sensor Network (MSN). In Chapter 6, a summary of the document is presented along with conclusions and future work.

Chapter 2

Microgrid Energy Management: State of the Art

2.1 Microgrid Control

Since a microgrid significantly differs from a traditional grid in regard to Distributed Energy Resource (DER) integration, size and few other parameters, there is a need to re-design some of the control and protection systems. The typical reliability and safety assumptions from a traditional power system cannot be applied here. The key challenges and desired features [6] of a control system for a microgrid are as follows

- **Time sensitive power control** - microgrids usually show a low-inertia characteristic due to the lack of high number synchronous generators typically found in traditional power systems. This can lead to severe frequency deviations very quickly. The microgrid controller should be capable of making sudden changes to keep frequency and voltage deviations within desired limits.
- **Entity monitoring and control** - Due to the critical balance of demand and supply, the control should be capable of monitoring the output voltage and current of various sources and loads and take immediate actions to prevent deviations from the set operating points. This requires advanced measurement sensors and controls with a robust communication setup.
- **Demand Side Management (DSM)** - It is essential to deploy DSM techniques for effective load management and to boost utilization of renewable energy sources. Well planned and executed DSM schemes can increase user interaction and help make the microgrid more energy efficient and reliable.
- **Economic Dispatch** - Appropriate dispatch of the energy sources can increase the profitability of microgrid operation. For example, priority utilization of PV during sunny days and utilization from central grid during off-peak periods.
- **Transition** - the control system should be able to function in both grid connected mode and island mode with the capability to transition seamlessly between the two modes of operation. The sophistication and complexity of a microgrid controller or control system will depend on its primary mode of operation. In grid connected mode, importance is given to the interconnection to the main grid whereas in an island mode reliability becomes an issue of prime importance.

It is clear that a robust control system is needed for reliable functioning of the microgrid and this differs from the control system, techniques and tools applied to conventional power systems. Microgrid control scheme usually consists of three control levels: *primary*, *secondary* and *tertiary* which is presented in the following sections.

2.1.1 Primary Control

This is the internal or inherent control in the power system which usually provides the fastest of all responses. In systems with synchronous machines, the control and sharing is performed by the voltage regulator, governor and the inertia of the machine. In microgrids with power electronic interfaces for DC sources, control systems have to be designed to simulate the inertia characteristics of synchronous generators which is usually done by emulating droop characteristics. The main advantage of droop control is that it eliminates a need for an extra layer of control and communication. This works well when there is no critical supply-demand balance and the supply is much higher than the demand requirements of the power system. However, there are some disadvantages [7], [8], [9] which can be seen below.

- **Fast/large changing load dynamics** - droop controllers cannot adapt to large or fast change in load dynamics.
- **Poor performance due to low X/R ratio** - leads to poor performance due to low X/R ratio which increases the coupling of active and reactive power.
- **Inability to handle large deviations** - there might be large voltage and frequency deviations due to failures, sudden changes and this cannot be handled by the droop controllers if the deviation is too large.
- **Inaccurate power sharing** - since there are no extra sensing mechanisms accurate power sharing will be tough to achieve due to uncertainties in output impedances.

All the above disadvantages lead to the adaption of another layer of control in microgrids which is referred to as secondary control or microgrid Energy Management System(EMS).

2.1.2 Secondary Control

This type of microgrid control is usually referred to as microgrid Energy Management System (EMS) in literature. This layer of control sits on the primary control mechanism and is responsible for reliable operation of the microgrid in grid-connected or in island mode of operation. EMS is responsible for taking actions to minimize frequency and voltage deviations and restore the microgrid to desired set-points of operation. It usually involves a framework consisting of a communication system and an intelligent controller which can find an optimal Unit Commitment(UC) and dispatch the available energy resources. EMS architecture can be of two types:

Centralized architecture

In this framework, the centralized controller acts as the brain of the microgrid and will be single point of information from all sources, loads, network parameters and the communication framework. Based on information it gathers, it has the capability to make intelligent decisions based on the pre-determined objectives and with an ultimate goal of maintaining a reliable grid operation. A practical implementation of a similar architecture can be seen in [10]. Here a centralized controller is implemented with a number of local controls at entity level. This system uses ethernet and PLC for communication. In centralized approach, the controller can make decisions online or locally. A typical structure and functionality of a centralized EMS is shown in *figure 2.1*.

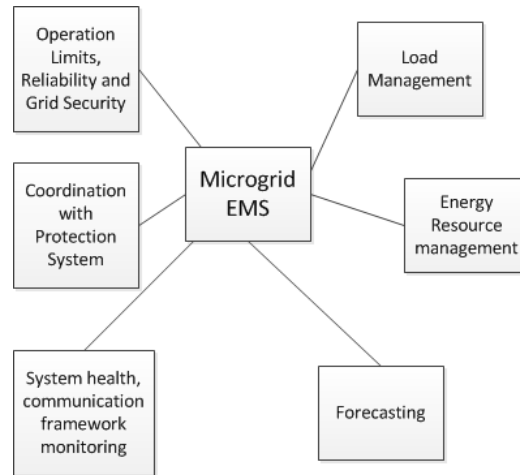


FIGURE 2.1: Centralized Energy Management System

In general, a centralized EMS scheme is more suitable for isolated microgrids where there is a critical balance between energy demand and supply.

De-centralized architecture

In this framework, highest autonomy is given to the different entities in the microgrid like loads and energy resources. A three level structure which includes Distribution Network Operator(DNO), Microgrid Central Controller (MGCC) and Local Controllers (LC) is presented in [11] .

- **Distribution Network Operators** - These are responsible for coordination and management of multiple microgrids in a specific area. They interact with the Microgrid Central Controller (MGCC).
- **Microgrid Central Controller** - MGCC is the brain of a specific microgrid. It ensures grid stability, optimizes power generation and consumption in terms of price, user based set-points and also handle transition between grid connected mode and island mode of operation.
- **Local Controller** - LCs receive instructions from MGCC but may also have certain level of intelligence. The LC controls the DER units and the controllable loads within a microgrid. One of the differences between centralized and de-centralized scheme lies in the operation of LCs. In centralized control, LCs get set points from the MGCC and it then takes the necessary actions. In de-centralized approach, LC makes decisions locally.

2.1.3 Tertiary Control

This is the highest layer of control. The function of this layer of control is to set long term goals and optimize on the economics of energy supply and demand. It also plays an important role when coordinating the operation of multiple microgrids and handling power import/export between them. Since this study focuses mainly on the secondary control of microgrids, this control level is not discussed further.

2.2 Wireless Communication Framework for Microgrids

Since this study is more aligned towards control and management of microgrids, secondary and tertiary control of the microgrid becomes extremely important for reliable and cost-effective operation of the microgrid. Last section presented some of the challenges in using droop control techniques in microgrids and particularly in islanded mode of operation. A centralized microgrid secondary control can achieve higher performances in island and grid-connected mode of operation. However, this is highly dependent on an efficient, reliable, low cost and low power communication framework. Connecting all loads and sources by wired communications like CAN, serial or ethernet becomes really complex, expensive and tough to manage when the number of loads and resources increases and the microgrid occupies a large geographical area. This section reviews different communication frameworks and topologies in literature.

A number of different communication technologies, protocols and sensor networks have been adopted in power system. While some are aimed at microgrid management, many wireless frameworks are designed for a building or a particular setting. This section reviews wireless communication schemes and energy management systems for generic power systems, microgrids, smartgrids, buildings and homes as there is a possibility that architectures in other settings can be adopted in a microgrid with some design modifications. A Wireless Local Area Network (WLAN) and IEEE 802.11g Wi-Fi based system for monitoring and control purposes is presented in [12]. Although certain performance parameters like speed and throughput can be higher for Local Area Network (LAN), the advantages of Wi-Fi include easy installation, wireless, low cost and flexibility of installation. This architecture involves using a wireless node for every entity in the microgrid. However, it does not take into account the high power consumption of Wi-Fi enabled devices and the possibility of the Access Point (AP) being a bottle neck. A three layer microgrid control architecture with an operation center, microgrid control center and switches at entity level is presented in [13]. CSMA/CA based communication scheme is adopted in this study. However, no specifics on the communication protocol or a practical implementation of mentioned architecture has been implemented. The advantages of using Wi-Fi based wireless sensor network has been highlighted in [14]. Comparing it to other wireless sensor protocols, Wi-Fi offers capabilities such as extended range, higher data transmission and better non-line-of-sight transmission. However, the disadvantages include higher power consumption, cost and AP bottleneck issues.

2.2.1 Wireless Sensor Networks for Microgrids

This section deals with Wireless Sensor Networks (WSNs) for control and management in smart grids, microgrids or residential and industrial establishments. WSNs have a number of advantages over wired or traditional wireless technologies like low cost, low power, flexibility and ease of deployment. However, there are some challenges of implementing WSNs in microgrids [15]:

- **Environmental factors** - In power system environments, sensors may be subjected to RF interference, caustic or corrosive environment, dirt, dust and other conditions that affect the performance of WSN [16].
- **Reliability and latency requirements** - control and management of an islanded microgrid is a time-sensitive operation. It becomes a difficult task to achieve

different Quality-of-Service(QoS) requirements and other network specifications such as latency, jitter, packet loss, congestion control etc.

- **Large scale deployment and autonomy** - WSNs in power systems will have large number of nodes spread over the deployment field. In many cases, the placement of these nodes can be random and this requires the WSN nodes to establish connections and maintain network connectivity autonomously.
- **Security** - This plays a crucial role in the design of WSN to prevent attacks and intrusions. These include external Denial-of-Service (DoS) attacks, eavesdropping using packet analyzers and other active attack techniques like node capturing, routing attacks or flooding.
- **Integration with Internet and other wireless/wired networks** - For remote access of data or control of WSN, it becomes necessary to integrate WSN with internet through a gateway. This adds complexity to the architecture as there is a protocol translation needed for all data packets from an IEEE 802.15.4 to IEEE 802.11(b/g/n) and vice-versa.

Several experimental studies have been conducted to understand WSNs [17], [18], [19]. Performance parameters have been assessed in different physical environments. Energy management tool based on IEEE 802.15.4 protocol has been proposed in [20]. This study is aimed at residential energy management in smart grids through load management using an optimization scheme. The simulation study uses a ZigBee sensor network to control loads. However, it does not provide a hardware and practical implementation to support simulation results. Apart from providing an optimizing scheme, the simulation study does preliminary analysis of sensor network parameter such as delay and jitter. It was found that sensor network performance decreased with increasing packet size and the jitter was negligible. Wireless sensor network in power systems for monitoring and control of segments in power transmission and delivery has been presented in [21],[15], [22], [23]. A wireless sensor network has been implemented in [15] for a substation, industrial power control room and an underground network transformer fault. This study uses the radio chip CC2420 from Texas Instruments that supports IEEE 802.15.4. It operates in the 2.4 GHz spectrum with an effective data rate of 250 kb/s. Apart from modeling the wireless channel model, the study also makes noise and interference measurements. The average noise level was found to be -90 dBm. It was also found that the background noise changes with temperature and interference levels. Introduction of a microwave oven varied the Packet Reception Ratio (PRR) between 35 - 100% and introduced a 15-dBm interference in the 2.4 GHz channel. LQI and RSSI were used to measure the radio link quality. On measuring PRR and LQI for an indoor room, it was found that there is a strong correlation between LQI and PRR and it was concluded that LQI is a good measurable indicator of the packet reception probability. Also, experimental results show that RSSI does not provide any correlated behavior with PRR.

Packet delivery measurement for different environments has been performed in [18]. This study uses about 60 sensor nodes in the 433 MHz range. The study assessed packet delivery performance at two layers of the communication stack: PHY and MAC layer. It was found that, when physical layer is taken into consideration (in the absence of interfering transmissions), packet delivery performance is a function of the environment, physical layer coding scheme and individual sensor characteristics. The study uses a linear topology with a single sender in three environments: office building, local habitat and a parking lot. Experiments in these environments showed that the

packet loss in the physical layer was about 10-30% and 50-80% communication energy is wasted in overcoming packet collisions.

The quality of wireless communication depends on the environment, the frequency spectrum its using, the modulation schemes in use and the communicating devices. Some important parameters and takeaways for WSN design and testing include

- **RSSI and LQI**- RSSI and LQI are important hardware measurement metrics in assessing radio link quality. Experimental studies have shown strong correlation between LQI and Packet Reception Ratio (PRR).
- **Noise and interference due to external appliances** - instruments and appliances affect WSN performance and this can be assessed by measuring PRR. Appliances operating in the 2.4GHz spectrum like microwave oven and cordless phones have a direct but a variable impact on PRR.
- **Background noise** - choosing a frequency channel with the least background noise may aid sensor network performance. Experimental studies have shown that the noise continuously changes over time which can be caused by changes in temperature and interference levels.
- **Packet Reception Ratio (PRR)** - one of the most basic evaluation criteria is the Packet Reception Ratio (PRR). Sensor networks are usually configured for multi-hop fashion. This scheme is much more reliable and energy-efficient than a single hop. Assessing cumulative PRR will help assess application level performance.
- **Transmit power** - radio transmit power has a direct influence on the network performance. There is a direct correlation between increase in transmit power and performance in the absence of noise and other interference levels. However, the trade-off will be increased use in battery power. However, some experiments in literature have reported that lower transmit power improved delivery performance.
- **Data Rate** - most of the experimental studies have pointed towards an increased performance with reduced data rate.

2.3 Cloud Computing for Microgrids

Although cloud computing has not been studied deeply in the context of power systems and microgrids, few studies have tried to explore the possibility of integrating cloud computing in power system technologies. A survey of integrating energy efficiency technologies with networking and cloud computing technologies is explored in [24]. Popularity of mobile smart phone and internet technologies such as Internet of Things (IoT) and cloud computing along with increased awareness of smart grid and microgrid technologies has led to increased attempts to integrate these technologies. With the advent of smart or intelligent buildings with sensors for lighting, HVAC, security, water, temperature, metering and automation, there is a need to store and analyze the data on a centralized platform which can be achieved by using widely adopted communication protocols such as TCP/IP and cloud computing technologies. Energy monitoring system using smart phones was proposed in [25]. It uses cloud computing for data storage, modeling and analysis. A cloud platform for a smart grid platform is described in [26]. The cloud platform in this study is used for storage, intelligence, web and a mobile application. The intelligence is mainly used for deploying

dynamic demand response techniques which entails real time detection, notification and response to adapt to instantaneous changes in the power system. The study uses both private and public clouds and IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) clouds. Cloud applications for energy management has been listed in [27]. The advantages a cloud infrastructure include elasticity, easy implementation of control and management techniques and resilience against failure of central communication center (utility operator) and real time management of different entities in the grid. A cloud based demand response architecture for smart grids has been proposed in [28]. This is in contrast to the master/slave demand response where the participants directly interact with the utility. A cloud service based intelligent power monitoring and early warning system has been proposed in [29]. A smart power management and service system on cloud computing platform has been implemented in [30]. This study uses ZigBee communication protocol for in-home communication and uses IP to communicate with the cloud through Simple Object Access Protocol (SOAP). It uses this framework for transferring energy, temperature and other statistics to the cloud. While several studies try to integrate cloud computing and IoT with power systems, a comprehensive experimental or practical deployment of this integrated system has not been implemented. Algorithms to handle multiple connections, data acquisitions, intelligence and reliability have not been assessed or implemented. This study presents the design framework of a cloud platform suitable for a microgrid scenario and also analyses the RTT performance of this system.

2.4 Summary

This chapter presents a detailed literature review of microgrid control and management, wireless sensor networks and cloud computing for microgrids. Several studies propose different techniques for microgrid control. The need for secondary and tertiary control for microgrids to maintain grid stability has been highlighted. Several studies propose different communication technology frameworks for several energy management systems in homes, buildings and power systems. However, they do not make a comprehensive effort to implement and evaluate these technologies in the domain of microgrids where latency and reliability is very critical. Lastly, cloud computing technologies for power systems has been reviewed. Exhaustive evaluation and performance analysis of the server framework for power systems and IoT systems has not been explored in literature. The next chapter deals with the Microgrid Network which consists of the power systems and the wireless sensor network for monitoring, control and management.

Chapter 3

Microgrid Network (MN)

This is an IEEE 802.15.4 based network with Atmel's Light Weight Mesh (LWM) as the communication stack. This sensor network forms part of the communication framework which is responsible for controlling and monitoring loads and energy sources at the microgrid level. A simple application layer was written for exchange of messages between the Microgrid Node (MN) and the Microgrid Gateway (MG).

3.1 Introduction

The key challenges and desired features [6] of a microgrid control system include time sensitive control, entity monitoring and management, demand side management, economic dispatch and capability to handle transitions. This requires a reliable, low cost and low power communication framework. Wired technologies become really expensive and complex as the number of loads and resources increase. Enabling every load and resource in the microgrid with a wired communication channel might not be an optimum solution. Wireless technologies aim to solve issues of cost, scalability and power constraints [31].

3.2 IEEE 802.15.4

This section gives an overview of the IEEE 802.15.4 standard [32]. IEEE 802.15.4 belongs to the category of Wireless Personal Area Network(WPAN). IEEE 802.15.4 based sensor networks are low data rate and low cost communication. Some of the characteristics of a WPAN are

1. Over-the-air data rates ranging from 20 kb/s to 250 kb/s
2. Implementation of Carrier Sense Multiple Access with Collision Avoidance(CSMA)
3. Low power consumption
4. Star or peer-to-peer operation
5. Allocated 16 bit short or 64 bit extended addresses
6. Link Quality Indication
7. Energy Detection
8. Allocation of guaranteed time slots

Two devices can participate in WPAN; Fully Functional Device (FFD) and a Reduced Function Device (RFD). The FFD can talk to FFDs and RFDs whereas RFD can only talk to an FFD.

3.2.1 Network Topologies

The standard defines two network topologies: star topology and peer-to-peer topology as shown in *figure 3.1*.

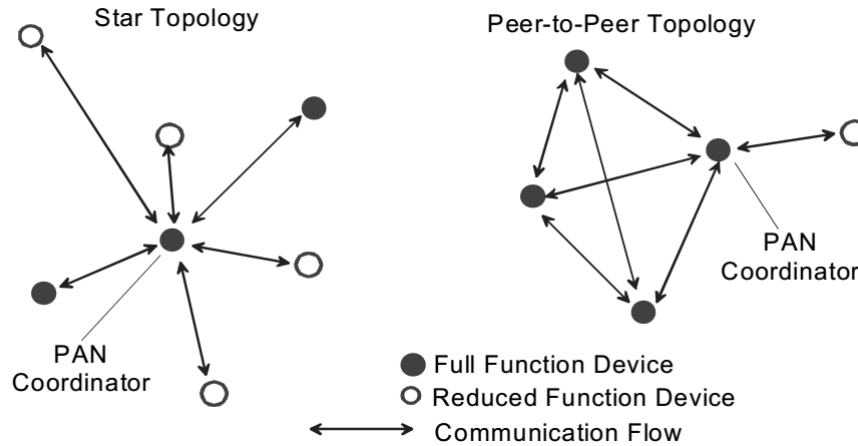


FIGURE 3.1: Network Topologies in IEEE 802.15.4

In the star topology, the communication is between the devices and a single central controller called PAN coordinator. Each of the nodes can communicate with each other only through the PAN coordinator. If the end device has to send a message from one node to another, it has to be sent to the PAN coordinator which then relays it to the destination device. The disadvantage of this topology is that there is no alternative route if the RF link fails between the PAN coordinator and the source/destination node. Also, the PAN coordinator can be a bottle-neck. The PAN coordinator may also be responsible for initiating the network or terminating the network. In peer-to-peer topology, any device can communicate with the other as long as they are in the communication range.

Two other topologies can be implemented by application layer protocols using IEEE 802.15.4: tree topology and mesh topology illustrated in *figure 3.3 and 3.2* respectively.

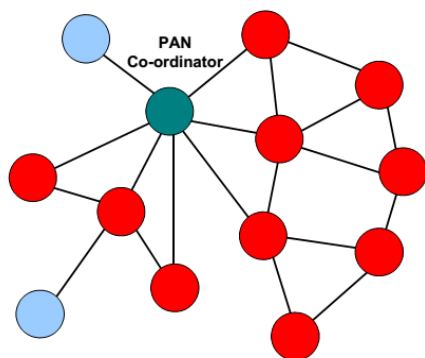


FIGURE 3.2: Mesh Topology

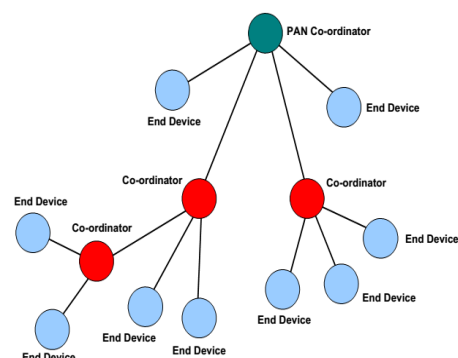


FIGURE 3.3: Tree Topology

The tree topology has a parent-child relationship based architecture. Each node except the main PAN coordinator has a parent. The nodes may have one or more children. Each node can only communicate with its parent and children. Cluster tree

topology is a slight modification of the tree topology where each parent-children group is regarded as a cluster and is given a cluster ID.

In mesh topology, the devices can be identical and are deployed in an ad-hoc arrangement. Even if the nodes are not in range with each other, the message is relayed through the network till it reaches the final destination.

3.2.2 IEEE 802.15.4 Protocol Stack

The IEEE 802.15.4 protocol stack is slightly different from the traditional WSN stack. It is illustrated in the figure below.

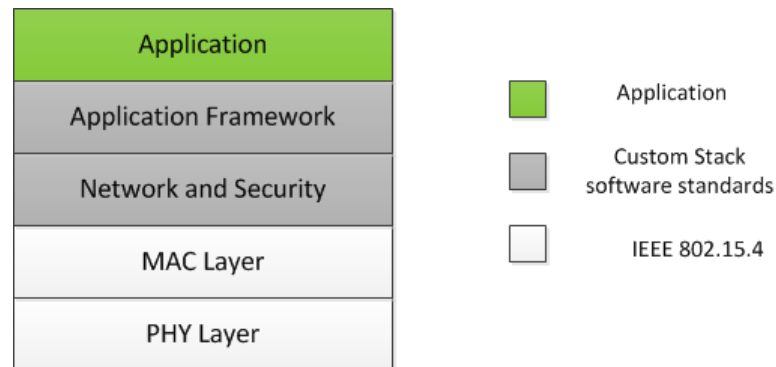


FIGURE 3.4: IEEE 802.15.4 communication stack

IEEE 802.15.4 PHY layer

The physical layer (PHY) standard is defined by IEEE 802.15.4 and is utilized by different custom software stacks and applications. The PHY provides two services: PHY data service and PHY management service interfacing to the Physical Layer Management Entity (PLME). The PHY data service enables the transmission and reception of PHY protocol data units (PPDU) across the physical radio channel. Its functionalities can be broadly defined as

1. Activation and de-activation of the radio transceiver.
2. Link quality indication for received packets - The LQI measurement is a characterization of the strength and/or quality of a received packet.
3. Clear channel assessment of CSMA/CA packets - The clear channel assessment is performed according to one of following methods
 - (a) **Energy above threshold** - CCA will report a busy medium upon detecting any energy above the ED (Energy Detection) threshold.
 - (b) **Carrier Sense** - CCA will report a busy medium only upon detection of a signal with modulation and spreading characteristics of IEEE 802.15.4 above or below the ED level.
 - (c) **Carrier sense with energy above threshold** - CCA will report a busy medium upon detection of a signal with modulation and spreading characteristics of IEEE 802.15.4 above the ED level.

4. Energy detection with the current channel - This measurement is done by the PHY layer and this used for the channel selection algorithm. It is an estimate of the received signal power within the bandwidth of the IEEE 802.15.4 channel.
5. Channel frequency selection - This is done based on the value received from the energy detection.
6. Data transmission and reception

PHY Frame Structure

The frame structure has the following components

- Preamble (32 bits) - for synchronization
- Start of Packet delimiter (8 bits) - to identify new data packet
- PHY header (8 bits) - PHY Service Data Unit (PSDU) length
- PHY Service Data Unit (127 bytes)

Sync Header		PHY Header		PHY Payload
Preamble	Start of Packer Delimiter	Frame Length (7 bit)	Reserve (1 bit)	PHY Service Data Unit (PSDU)
4 Octets	1 Octet	1 Octet		0 – 127 Octets

FIGURE 3.5: IEEE PHY Frame Structure

IEEE 802.15.4 MAC Layer

The MAC layer provides two services: MAC data service and MAC Management Service Interfacing to the MAC sub layer management entity. The MAC data service enables the transmission and reception of MAC protocol data units (MPDU) across the PHY data service. MAC Data service (MCPS) provides a mechanism for passing data to and from the next higher layer. The MAC Management Services (MLME) provides the mechanism to control the settings for communication, radio and networking functionality from the next layer.

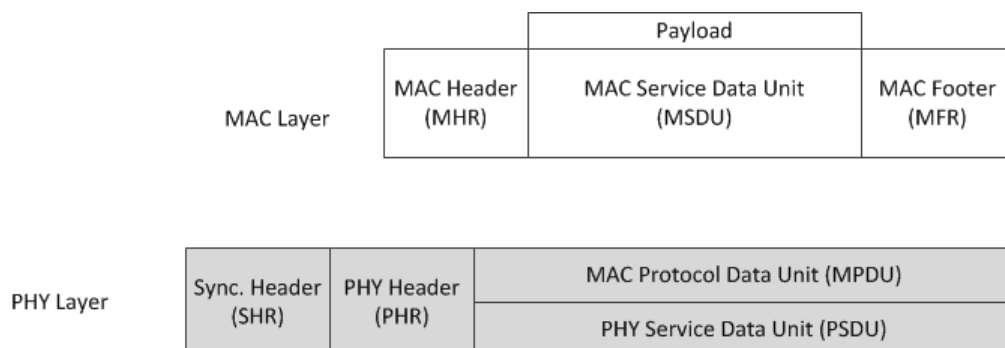


FIGURE 3.6: IEEE MAC frame structure

3.3 Microgrid Sensor Network

MSN implements LWM which is a low power wireless mesh network protocol from Atmel [33]. LWM does not require a dedicated node to start a network and it defines two types of devices: routing and non-routing. The routing nodes form the core of the network and are involved in routing. Non-routing nodes are not involved in routing purposes but can send and receive messages. These serve as end nodes in the network. LWM supports two types of routing protocols: native LWM routing where the route discovery happens based on the data from the received and transmitted frames and Ad hoc On-Demand Distance Vector (AODV) routing. The stack has a small footprint which is typically about 8KB Flash and 4KB RAM. The LWM network header and application payload are encapsulated inside the standard IEEE 802.15.4 data frame payload and it uses the standard MAC header but does not process IEEE 802.15.4 command frames. This means that it uses the standard physical frames but does not follow the MAC specifications. Instead, it implements the mesh routing protocol. Zigbee Pro is a common network stack used in IEEE 802.15.4 networks. However, it has higher resource requirements and bigger footprint compared to LWM. Performance comparison between LWM and ZigBee was conducted in [34]. The study found that LWM performed better than Zigbee Pro in throughput and latency.

3.3.1 Features of LWM

LWM protocol has the following features

1. No dedicated node is required to start a network
2. Has a theoretical limit of 65k nodes
3. No periodic service traffic occupying bandwidth
4. It has 2 distinct nodes: routing and non-routing
5. Route discovery can happen automatically
6. No child-parent relationship between the nodes
7. Routing table is updated automatically based on data from the received and transmitted frames.

Network Topology

The IEEE 802.15.4 standard [32] defines two network topologies: star and peer-to-peer. MSN deploys a mesh topology through LWM. In this topology, the devices can be identical and in an ad-hoc arrangement. If the nodes are not in range with each other, the data packet is relayed through the network till it reaches the final destination. Another advantage of the mesh network is the self-healing capabilities of the sensor network where it can autonomously react to network disruptions. If the packet between a source node and a destination node is relayed through an intermediate node, a disruption to the intermediate node will initiate a route discovery to relay the packet through another available intermediate node to ultimately reach the destination.

The network topology is illustrated in the figure below. Sensor nodes in blue are routing nodes and the non-routing nodes are indicated in green. Non-routing nodes can send and receive data but will not be used for routing purposes and hence cannot be used as range extenders.

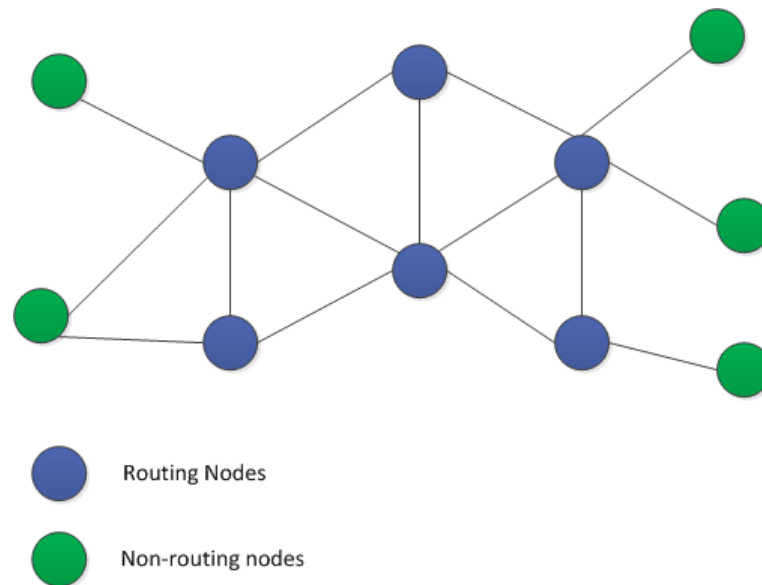


FIGURE 3.7: LWM Network

3.3.2 LWM Routing

The LWM protocol implements native routing in this energy management system.

LWM native routing

Native Routing This is the native LWM routing algorithm. When compared to AODV, this is simple, compact and does not use additional commands to perform route discovery. One of the disadvantages of this algorithm is that it cannot guarantee that the discovered routes are optimal since it performs only local optimization. There is no special route discovery procedure; routes are discovered as part of normal data delivery. The following set of figures will illustrate the routing protocol. The following assumptions are made:

- Nodes 1, 2 and 3 are capable of routing packets
- Routing tables on all nodes are empty
- Node 1 has to send a data packet to node 3
- Node 3 is out of range for node 1 and hence it has to take a multi-hop path through node 2

FIGURE 3.8: Initial Network Configuration

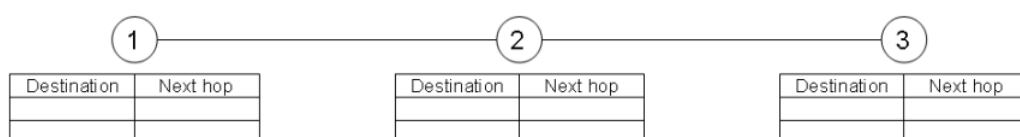


Figure 3.8 shows the initial network configuration.

Since node 1 has to send a data packet to node 3 and the route is unknown, the route discovery takes place. Node 1 sends a packet with network destination address set to 3 and the MAC address set to 0xffff (which stands for broadcast). This is illustrated in figure 3.9. The destination MAC address is set to broadcast because the routing table is empty and the packet has to be sent to all nodes to learn the route. Node 2 receives this packet and adds this entry for node 1 to its routing table.



FIGURE 3.9: First Step in Routing

In the next step, node 2 broadcasts the frame. Node 3 receives the frame and adds the entry for node 2 to its routing table. It also adds an entry for node 1 from the network source address since it is the destination node. This is illustrated in figure 3.10.

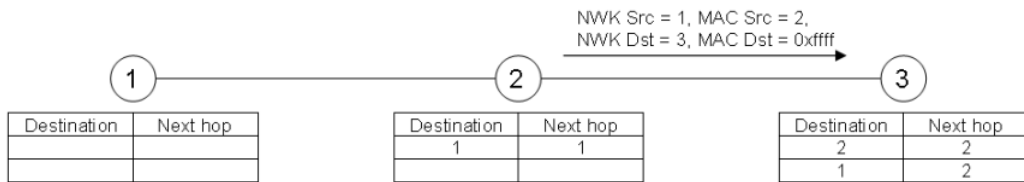


FIGURE 3.10: Second Step in Routing

In the third step, node 3 sends an ACK. This is done to establish a reverse route. Since node 3 now knows the reverse route, it sends an unicast frame back to node 1. This is shown in figure 3.11

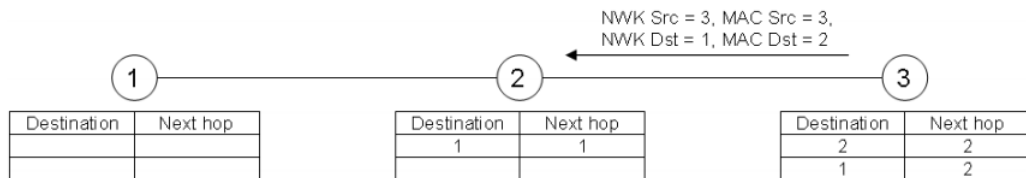


FIGURE 3.11: Third Step in Routing

In the final step, node 2 receives the frame from node 3. Since it has an entry for node 1, it forwards the packet to node 1. Node 1 then adds the entry for node 3. This is illustrated in figure 3.12

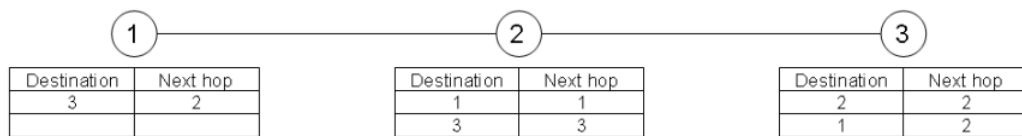


FIGURE 3.12: Final Step in Routing

3.3.3 MSN Algorithm

This section deals with the algorithm deployed for the MSN network. In-depth explanation of network configuration, packet transmission and reception, ACKs, packet re-tries and microE has been provided.

MSN deploys an IEEE 802.15.4 based WSN which uses Atmel's LWM as the communication stack. The algorithm first sets few critical network parameters: *network address*, *network identifier*, *frequency channel*, *transmit power* and *receiver state*. These parameters define the configuration of the sensor network and affect individual node performance. Each node in MSN has a unique network address which helps identify it in the network. This is set by *network address*. *Network identifier* sets the PAN ID for the sensor network. There is a possibility of multiple PANs to exist in the same frequency channel. It is important that all radios designed to be in the same network have the same PAN ID. *Frequency channel* and *transmit power* help set the frequency channel and the transmit power of the radios. The lower level part of the stack is initialized by calling a *system initialization* function. This function performs the low level hardware initialization. Once this is completed, the *system task handler* function runs the internal stack tasks. This includes handling the transceiver, encryption, modulation, data transmission and reception at the physical level. The *application task handler* is responsible for handling tasks at an application level. An overview of the algorithm is shown in figure 3.13. The *application task handler* implements a state machine model.

The application task handler defines four states: *initialization*, *idle*, *queue* and *send*. The flow between the states is shown in figure 3.13. During the network setup, the task handler goes to *initialization* state which sets various parameters such as *network identifier*, *network address*, *frequency channel*, *transmit power* etc. When data packets have to be sent, the data is encapsulated in the right format in the *queue* state. In the *send* state, the *message send handler* sends the data packet. The transmission and reception of the data packet is a synchronous operation. In the event of an incoming ACK, the *ACK handler* emits a status indicator to notify if the acknowledgment was received or if message transmission failed. On success, the *application task handler* goes to an idle state. If the ACK fails, the task handler executes a packet retry. This depends on the type of retry mechanism implemented. This is illustrated in figure 3.14.

In the event of an incoming message, *response handler* handles the incoming message and implements the necessary action. At this level, the request and response packets are implemented in *microE*. The *response handler* is responsible for decoding the command header from the microE data packet and executing the necessary task. MicroE commands are shown in table 5.1. If the data packet received has a request command, the *response handler* will send the specific response to the source node or MG. This response may include node health, relay status indicators or grid parameters like voltage, current, frequency, power factor etc. If the data packet received is a response packet, which is usually sent from MN to MG, MG decodes the response command header and relays the response to MC. The event handlers *ACK* and *response* handlers are executed

by the stack in the event of ACK and message reception respectively. The data packet is received and processed by the stack and the *application handler* is notified which then handles the task at the application level. In the case of *message send handler*, the application handler calls it in the event a data packet has to be sent. The data packet is then processed and sent by the lower levels of the stack.

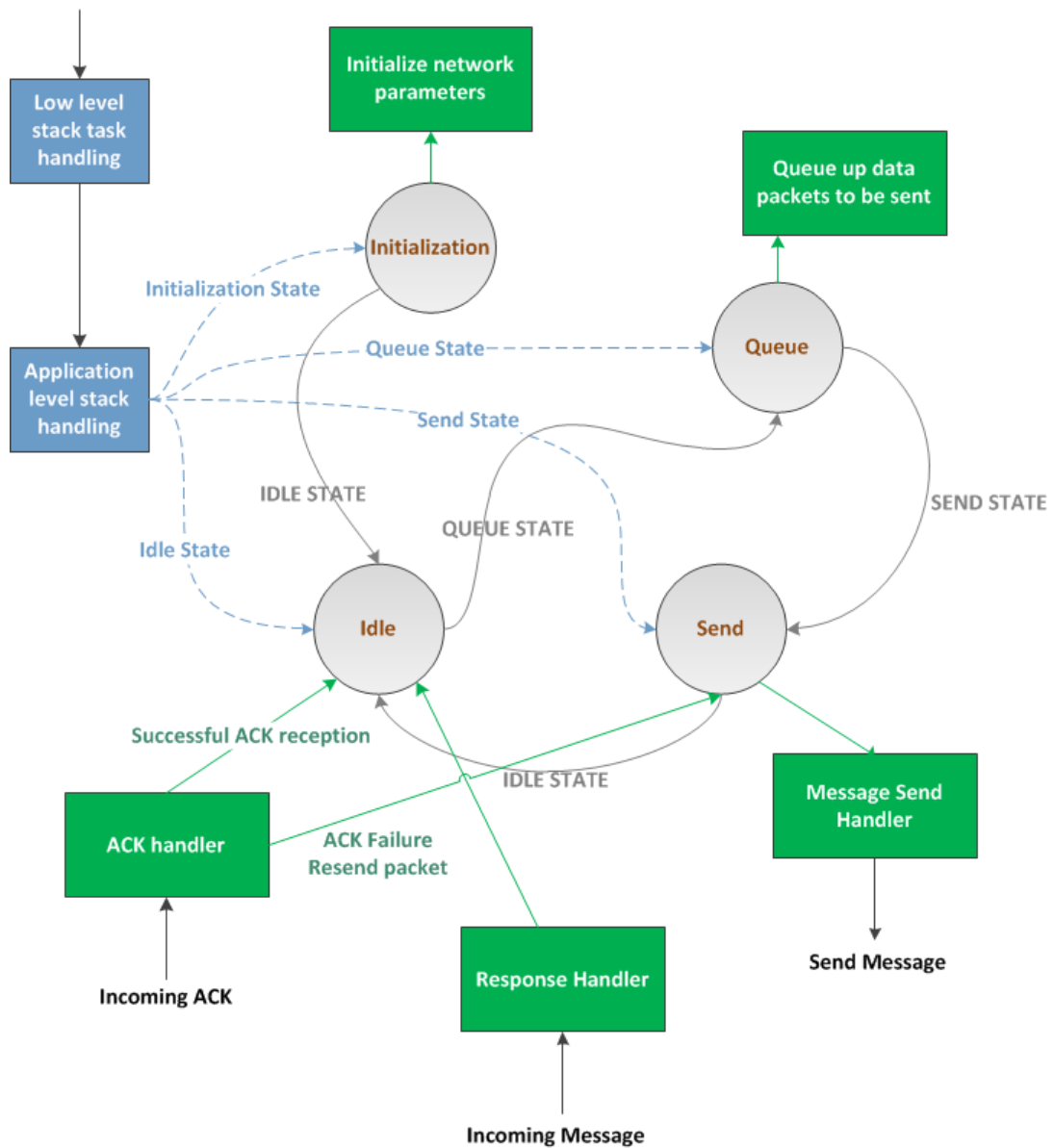


FIGURE 3.13: MSN algorithm overview

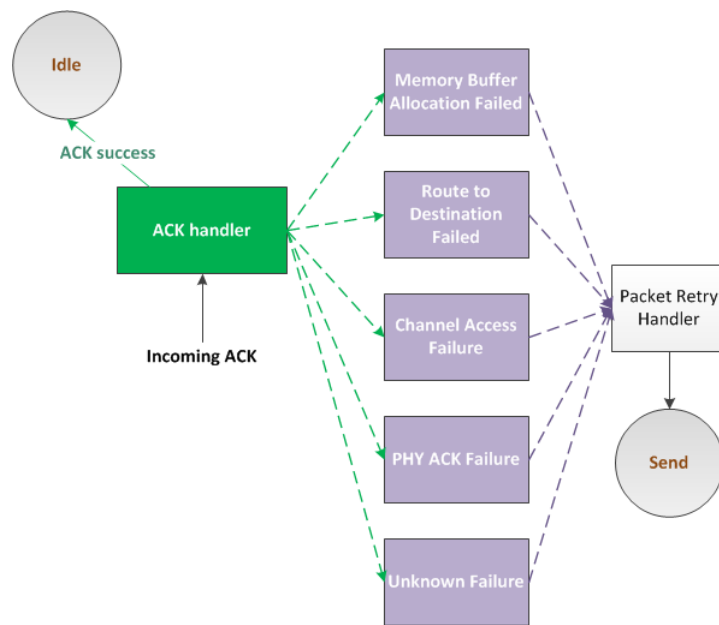


FIGURE 3.14: MSN ACK handler

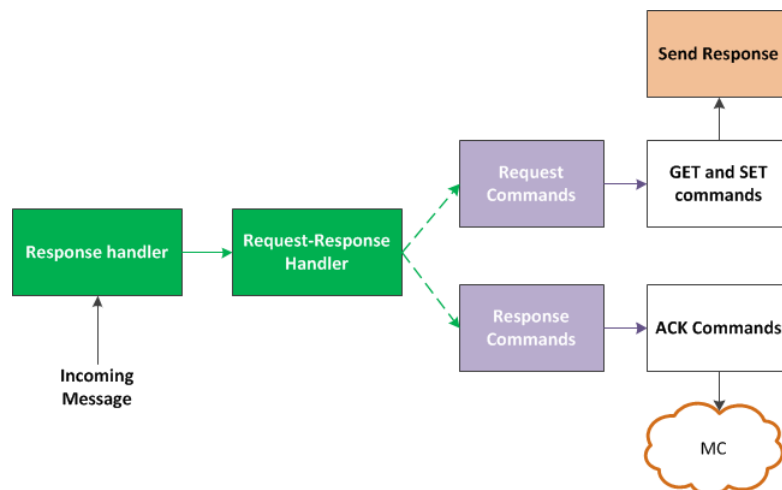


FIGURE 3.15: MSN response handler

3.4 Summary

An introduction to IEEE 802.15.4 protocol and Atmel's Light Weight Mesh (LWM) has been presented in this chapter. IEEE 802.15.4 based WSN has several advantages over other wireless technologies such as low cost, low power, higher reliability and self-healing capabilities. Over the IEEE 802.15.4 protocol, Atmel's LWM was implemented which can be compared with ZigBee. It offers advantages such as lower footprint, latency, easy network configuration and start. However, it does not implement the IEEE 802.15.4 MAC layer. The stack also has the capability to implement the native routing protocol or AODV routing. For this study, native routing was chosen. The MSN algorithm is also presented for transmission and reception of ACKs and messages through the RF network is also presented. The next chapter presents the Microgrid Cloud (MC).

Chapter 4

Microgrid Cloud

4.1 Introduction

This chapter introduces the concept of cloud computing and the cloud architecture used for the Microgrid Cloud (MC). Cloud computing is becoming ubiquitous in today's era. With increasing data generation from social media, services and businesses there is a need for storage, analysis and access from different mobile platforms in real time. Cloud computing solves these issues by providing a number of hardware and software services. Although word "cloud" seems ubiquitous, a clear definition is necessary to understand its importance and relevance in microgrid energy management. The next few sections define cloud computing and various technologies associated with it. The Microgrid Cloud (MC) is then discussed in detail.

4.2 Cloud Computing

4.2.1 What is a Cloud?

Cloud computing refers to both the applications delivered as services over the internet and systems software in the datacenters [35]. The datacenter hardware and the software together is referred to the *cloud*. Cloud computing infrastructure offers a number of features and capabilities that an ordinary remote or a private server cannot offer.

- **Elasticity and Scalability** - cloud computing platform gives the users an illusion of infinite computing resources on demand. This eliminates the need for users to plan ahead for provisioning. As the load on the application decreases or increases, the users can request for a scale down or up of resources very easily.
- **Pay for use** - the flexibility to only pay for the resources used. The resources can be acquired and released whenever required by the user.
- **Resiliency** - data centers and cloud computing service provides implement a number of fault tolerance techniques to guarantee server up-time to users.
- **Shared Resources** - multiple tenants can share the same set of physical resources which is virtualized to accommodate multiple users.

4.2.2 Cloud Service Models

Cloud computing services follow a Service Oriented Architecture (SOA) model which can be classified as below:

- **Infrastructure as a Service (IaaS)** - this is the basic cloud service model where the users lease physical/virtual machines, storage and networks. In this model, the users are responsible for managing the operating file system. Example of this model include Amazon EC2, Microsoft Azure, Google Compute Engine, Rackspace etc.
- **Platform as a Service (PaaS)** - in this model, the cloud service providers deliver a platform which will typically include an operating system, execution environment, database solution and web servers. The users can lease this platform to run applications in a specific language or environment. Examples include MapReduce, java runtimes, databases (MySQL, Oracle) and webservers (Apache, Tomcat) etc.
- **Software as a Service (SaaS)** - the cloud service providers manage the infrastructure and the platform and let users access to specific software which can be used on a subscription or pay-per-use basis. Examples include Concur, Salesforce, NetSuite etc.

4.2.3 Cloud Deployment Models

The cloud can be deployed in different ways: private, public, virtual private and hybrid

- **Private Cloud** - this model is usually adopted by organizations which have security and privacy restrictions or the need to support specific and higher performance in the cloud. It is usually implemented behind a firewall and the infrastructure is usually located in the organization premise. The advantages of this model include higher speed, flexibility, security and higher performance. However, the cost of establishing such infrastructure is exorbitant.
- **Public Cloud** - this is the most common model which is adopted by millions of users for development and deployment. This is provided as a service by cloud providers which let users remotely access hardware and software services. It has a shared pool of computing and network resources like servers, networks, storage and applications. The advantages include low cost and ease of use while the disadvantages can be lower performance, privacy and security concerns.
- **Virtual Private Cloud** - for users who need a higher level of security and regulatory compliance without the investment of a private infrastructure, this model is beneficial. It provides a private solution using the public cloud infrastructure of a service provider. This is achieved by dedicated VLANs, providing network isolation, virtual private networks and dedicated firewalls. The advantages include higher security, performance while the disadvantage can be cost.

4.3 Microgrid Cloud (MC) Physical Infrastructure

The MC has been deployed separately in two locations: Amazon EC2 and Wisconsin Wireless and Networking Systems (WiNGS) Laboratory at the University of Wisconsin-Madison. One t2.micro instance on Amazon EC2 has been deployed which offers a 64 bit VM with 1 CPU, 613 MB RAM with high frequency Intel Xeon Processor with turbo up to 3.3GHz. The operating system deployed is an Ubuntu Server 14.04 LTS 64 bit version. The WiNGS machine runs a 64 bit Ubuntu Server 14.04 LTS with 4 GB RAM and 20 GB storage. Both machines have public IP and run similar software stacks.

4.4 MC Framework

The overall system architecture of MC has been illustrated in *figure 4.1*. It can be seen

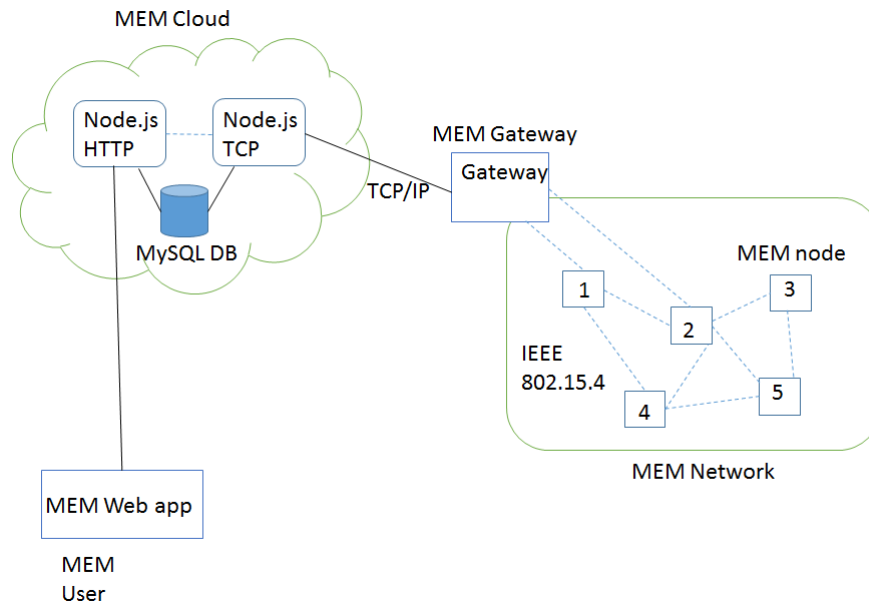


FIGURE 4.1: MC system architecture

that the internally, two Node.js servers have been deployed. Node.js HTTP is a HTTP server to cater to the MEM Web app and the Node.js TCP is a TCP server which is the core back-end engine for the MEM network.

4.4.1 Node.js

Node.js is a framework that provides event-driven I/O and asynchronous platform for server-side JavaScript [36]. It is a single-threaded server-side JavaScript environment implemented in C and C++ and utilizes the JavaScript V8 engine. Traditional server frameworks have an explicit client and server side implementation with a different set of languages for both. This meant using languages and frameworks like HTML, CSS, JavaScript, AJAX on the client end and server languages such as PHP, Perl, ASP, Java, Python etc. which are used to implement server frameworks such as Apache HTTP, LIGHTTPD, NGINX, LITESPEED, ZEUS etc. Node.js simplifies some of the implementation by having full stack JavaScript using which programmers could use the same programming language on client and server side. While this is one of the major advantages, other advantages include non-blocking asynchronous model and easier implementation of sockets.

4.4.2 Implementation Details

The MEM nodes are connected to each other directly or indirectly through a wireless mesh network which is not TCP/IP based. This is a sensor network which is used for intra-grid communication. Every node or gateway in the Microgrid Network (MN) has an associated address. This is used by the sensor network communication and also for MC to individually identify the nodes. The MEM system implements a hybrid push-pull mechanism for communication. This means the MEM nodes have the ability to

respond to requests sent by the MEM gateway (pull mechanism) or MC and send information independently to the MG/MC through a push mechanism. This is usually an energy log which is sent every minute automatically. The MEM gateway receives this and automatically pushes it to MC. An application layer called *microE* was written to handle application level communication in the microgrid network. The MC is responsible for encapsulating the data packets in this format. A sample command set is shown in figure 4.2.

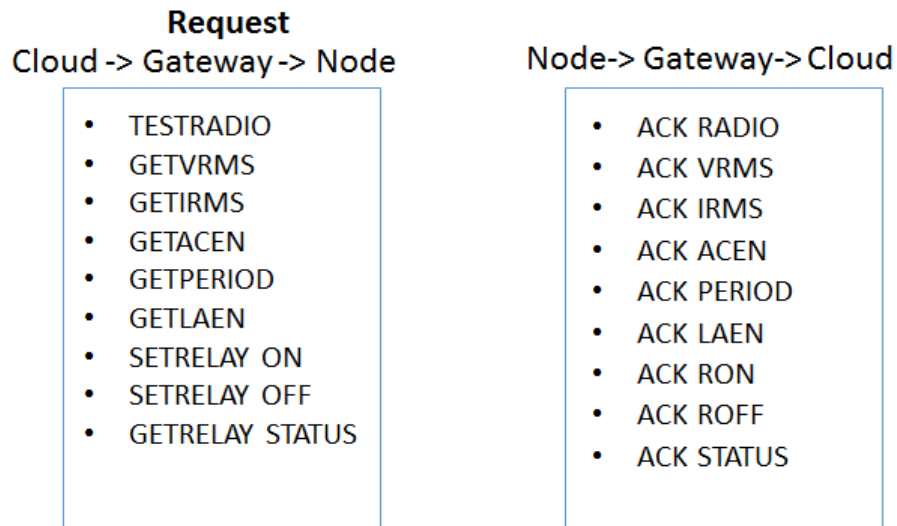


FIGURE 4.2: MicroE command set

A sample request and response is shown below.

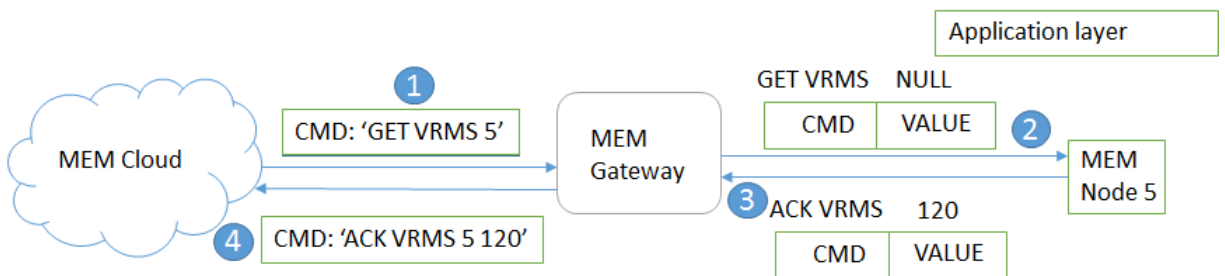


FIGURE 4.3: Sample request and response commands

The web application helps users control and manage the microgrid. While the development of the web application is in progress, it is aimed to have the following features

- **Grid Network** - this feature of the web application gives the user a complete overview of the microgrid. This features the list of active nodes, total energy consumption, grid voltage and current. The user also has the capability to remotely turn on or off a source or a load.
- **Microgrid Scheduler** - the user can set schedules for each load or source in the microgrid to turn on or off at a particular time.
- **Health** - the stability of the microgrid depends on MG and MN being active. This enables the commands from MC to be executed immediately on these nodes. The

back-end engine sends a 'heartbeat' to MN to assess if all the nodes are active and notify the user if two successful heartbeats to a particular node fail. This section of the web application constantly updates to tell the user the health of the grid.

- **Spending** - tracking energy costs is one of the most important features. This will help users how their spending varies over hour, day, week or month of the year.

MEM User and Grid setup

This section illustrates few basic steps in setting up the web application and the back-end engine. Each user has an unique keyword called *MEM ID* which is used to authenticate the TCP connection and also identify the user across the web application and the TCP back-end engine.

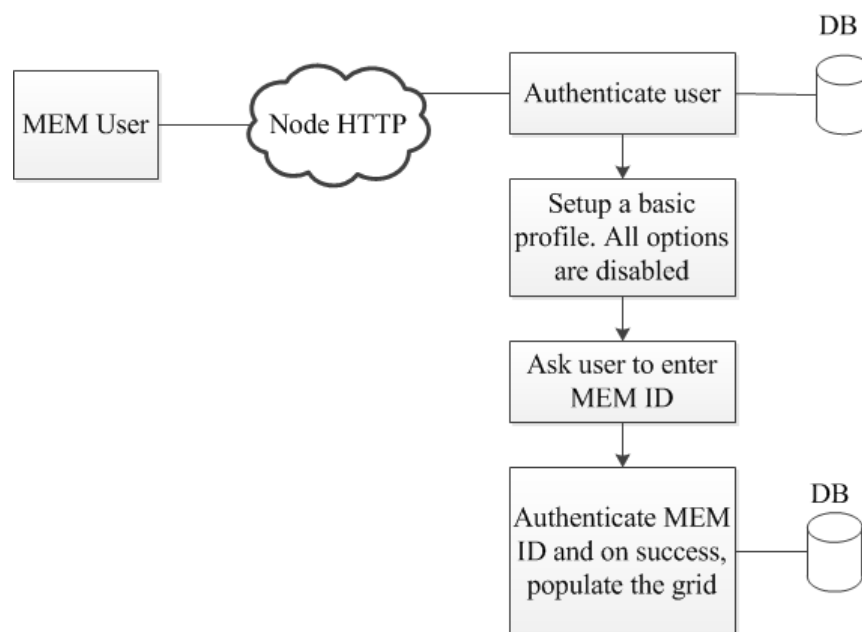


FIGURE 4.4: Setting up MEM users

Figure 4.4 shows the first step to setup MEM users. Each user is given an unique code called MEM ID. To get access to the microgrid network on the web app and to unlock full functionality, the user has to enter this the first time the application is used. Once the user enters the MEM ID, the back-end engine authenticates this and on a success, enables full functionality of the application.

The TCP sever constantly handles multiple connections from different gateways. It acts on the connections only after authentication. Un-authenticated TCP connections are discarded by the back-end engine. Figure 4.5 shows the flow for setting up the grid. On every attempt of a TCP connection establishment between MC and MG, MG emits the *MEM ID* as the first set of bytes. This helps MC to authenticate each connection before processing it. Once the connection is authenticated, Node TCP sends a heartbeat to assess the configuration of the grid. MG receives this and sends it as a broadcast to all the nodes. An example is shown in figure 4.6.

The broadcast takes place in the MSN and all active nodes respond back with a specific response command. The gateway then relays these messages back to the cloud. This gives the back-end engine the complete grid configuration.

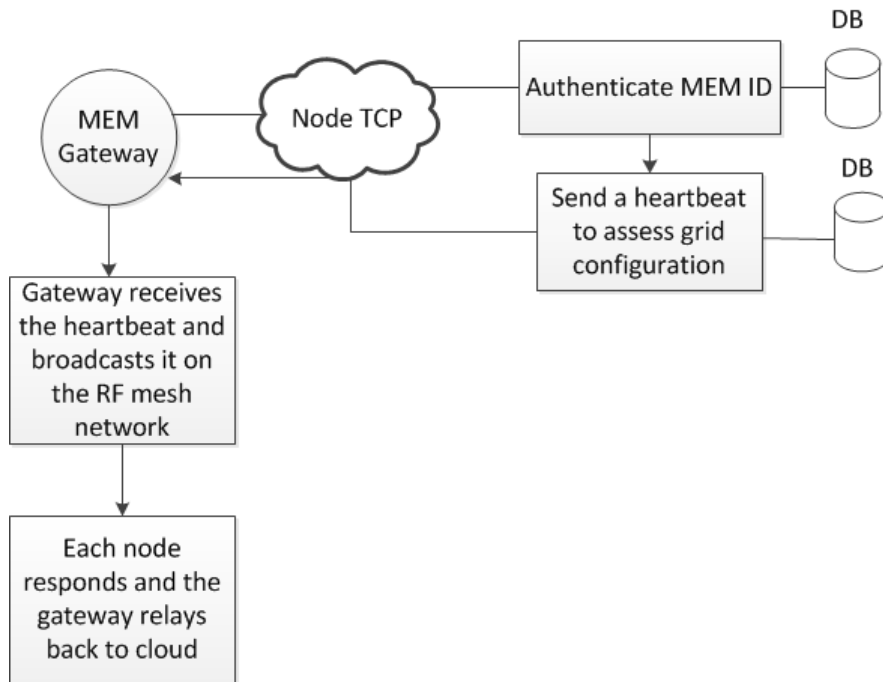


FIGURE 4.5: Setting up MEM grid

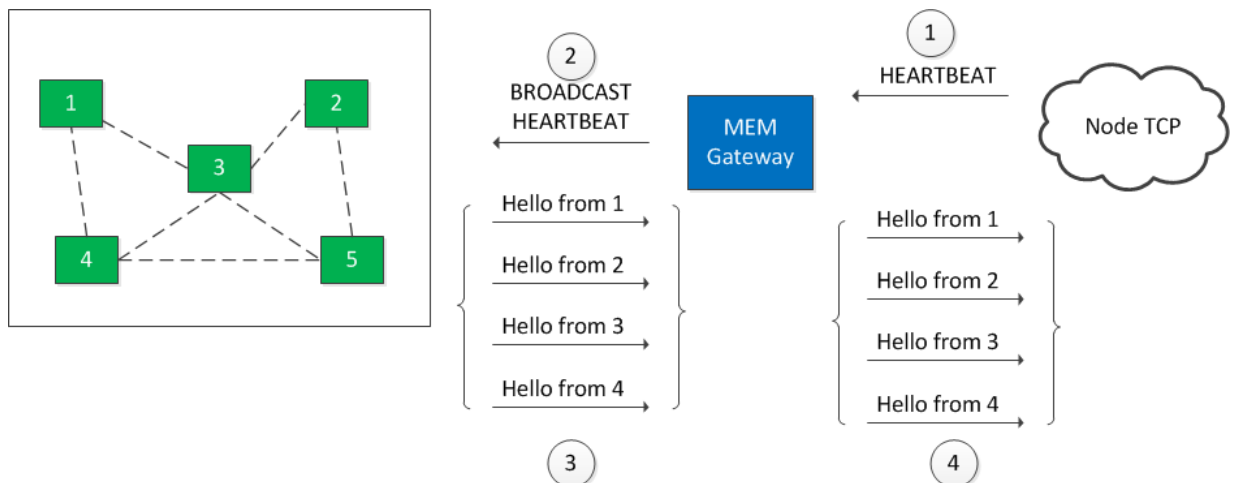


FIGURE 4.6: MEM heartbeat

Once the MC gets a list of all active nodes, it is now ready to send or receive commands to the MN.

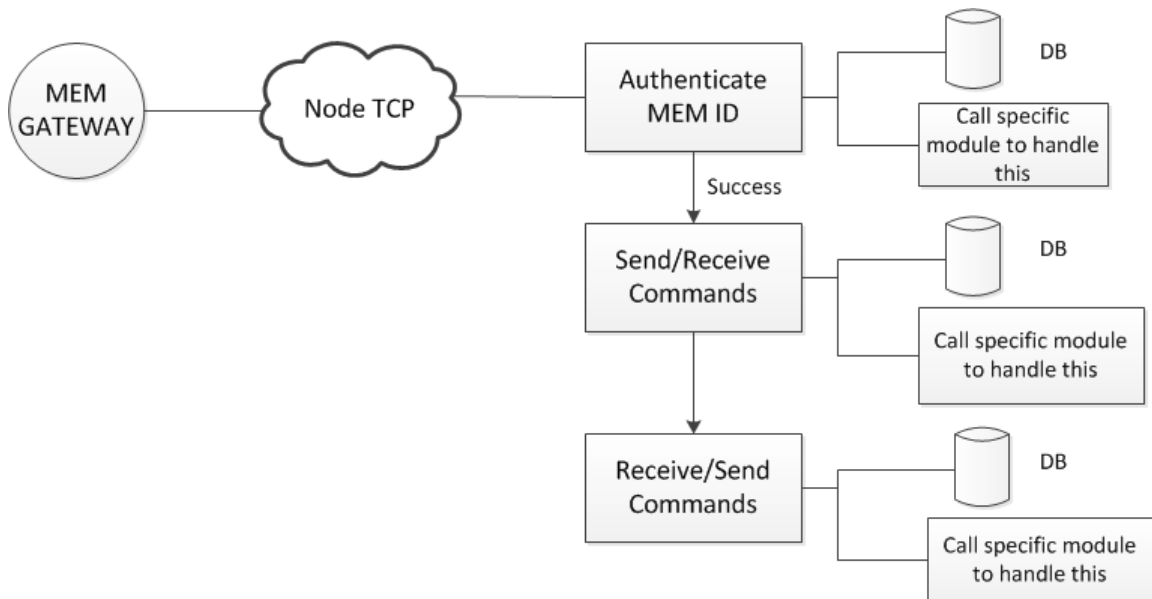


FIGURE 4.7: MicroE command set

4.5 Summary

Cloud computing technologies provide a number of advantages such as scalability, resource sharing, elasticity etc. Its been increasingly used for social media and utility applications. An introduction to cloud computing and its features has been presented in this chapter. Integrating cloud computing technologies to a power system is particularly interesting as it enables easy implementation of applications like IoT and help deploy intelligence and big data stacks. The implementation of a Node.js based cloud platform for MEM has been presented in detail. The core back-end engine has been de-coupled from the web application making all subsystems modular and fault tolerant. The Node.js TCP server is responsible for handling communication with the MN and the Node.js HTTP handles the web application. The two servers share a MySQL database. Node.js is an event-driven framework which has the ability to handle thousands of connections and execute asynchronous actions smoothly. The next chapter presents the Microgrid Network (MN) architecture and MEM hardware platform. Performance analysis of MSN and the CPS for microgrids has also been presented in-depth.

Chapter 5

Experiments and Results

5.1 Microgrid Network Architecture

The Microgrid Network (MN) forms the core of the entire framework. The architecture is illustrated in *figure 1.2*. It consists of the following components.

- *Microgrid Power Network* - In *figure 1.2*, network in red indicates the power topology. The microgrid connects to the utility at the Point of Common Coupling (PCC). The loads are connected to the microgrid through their respective switches and DC entities like PV, battery banks are interfaced through inverters. The microgrid is capable of operating in island mode (when it is disconnected from the utility grid) or in grid connected mode (when it is connected to the utility).
- *Microgrid Sensor Network (MSN)* - This is an IEEE 802.15.4 based network with Atmel's Light Weight Mesh (LWM) as the communication stack. This sensor network forms part of the communication framework which is responsible for controlling and monitoring loads and energy sources at the microgrid level. A simple application layer was written for exchange of messages between the Microgrid Node (MN) and the Microgrid Gateway (MG).
- *Microgrid Gateway (MG)* - This integrates the Microgrid Sensor Network with the Microgrid Cloud. It acts as a translator between IEEE 802.11 communication protocol and IEEE 802.15.4 network. MG is responsible for analyzing and converting the IEEE 802.15.4 data from MN and packaging it into IEEE 802.11 protocol for transmission to MC. MG should also be capable of converting data from IEEE 802.11 protocol to IEEE 802.15.4 protocol for communicating with MSN.
- *Microgrid Node (MN)* - Every load and energy source is connected to MN. MN offers a number of features in addition to WSN capabilities like energy measurement, control relays, time-stamping of all events through Real Time Clock (RTC) and local storage through Secure Digital (SD) card.
- *MicroE* - This is an application for controlling and monitoring entities in the microgrid. It sits on the mesh communication stack. Every microE packet sent or received has a command header and a value header as shown in *figure 5.1*. The MG acts as a central controller for the MSN and dispatches request commands to the desired MN. The MN responds with a microE packet which consists of a request command and a value. Sample request and response commands are shown in table 5.1.

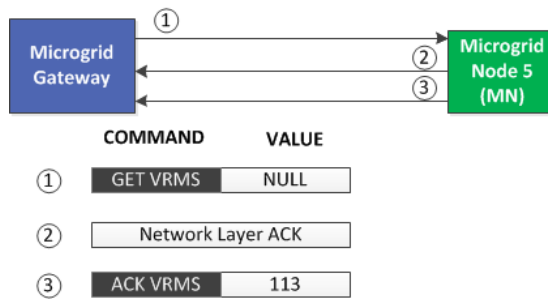


FIGURE 5.1: MicroE request-response mechanism

TABLE 5.1: MicroE Sample Request and Response Commands

Request Command	Response Command
TEST RADIO	ACK RADIO
GET VRMS	ACK VRMS
GET IRMS	ACK IRMS
GET ACEN	ACK ACEN
GET PERIOD	ACK PERIOD
SET RELAY ON	ACK RELAY ON
SET RELAY OFF	ACK RELAY OFF
GET RELAY STATUS	ACK STATUS

5.2 MEM Hardware Platform

In order to implement various communication and utility functionality such as Wi-Fi, RF, storage, RTC (Real Time Clock), a robust embedded platform is required. This section deals with the hardware used for this study.

5.2.1 MEM Hardware Architecture

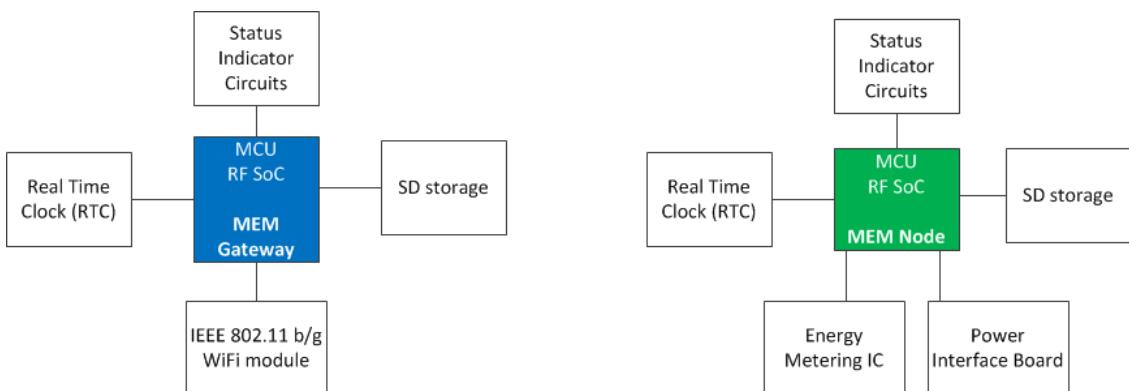


FIGURE 5.2: MEM hardware architecture

The core functionality of MG is to act as a translator between different communication protocols. It consists of a central CPU with an integrated IEEE 802.15.4 compliant RF transceiver. It also consists of a Wi-Fi module, SD storage and a RTC. The MEM node shares a similar platform without wireless internet capabilities. However, it has

energy metering capabilities to measure current, voltage, energy, frequency and power factor of each entity in the microgrid. This is shown in *figure 5.2*.

MCU

The MEM MN and MG use Atmel's ATmega256RFR2 as the core CPU. It has the following features

- 256K bytes of In-System Programmable (ISP) flash
- 8K bytes EEPROM
- 32K bytes SRAM
- Max. operating frequency up to 16 MHz
- Integrated 2.4 GHz RF transceiver.
- Supports 250 kb/s, 500 kb/s, 1 Mb/s and 2 Mb/s data rates
- USART, SPI, I2C interfaces
- Supports ZigBee, IEEE 802.15.4 stacks, RF4CE, SP100, WirelessHART, IPv6, 6LoWPAN

Energy Measurement

One of the important functions of MN is to measure grid parameters at the entity level such as voltage, current, energy, frequency and power factor. MN uses ADE7763 energy metering IC to accomplish this task. The energy IC is interfaced with the Micro Controller Unit (MCU) through Serial Peripheral Interface (SPI).

Data Logging

MN logs all measured data and events locally onto a Secure Digital (SD) module. In case of loss of connection to the MC, data can be retrieved. Also, once the connection to MC is re-established, MC can sync with the MGN by requesting history data from MN.

Time Stamping

All measurements, data logging and activity at MN are times-stamped using DS1337 Real Time Clock (RTC). This helps understand the behavior of the individual entity and the grid for future data analysis.

The hardware platform consists of a communication board and a power interface board as shown in *figure 5.3* and *5.4*.

The communication board hosts the microcontroller unit, the communication and storage systems. The power interface board hosts the latching relays, relay interface circuitry, load current and input voltage filtering and divider circuitry. The two boards interface through a ribbon cable or jumper wires. The advantage with this kind of architecture is that the communication board is not exposed directly to high voltage and current. This reduces noise on the communication lines. The communication board provides digital signal lines which interface with the LED indicators, relays, voltage and

current measurement circuitry on the power interface board. The other advantage is that the interface board can be easily modified to accommodate higher or lower rating relays depending on the application or user requirements.

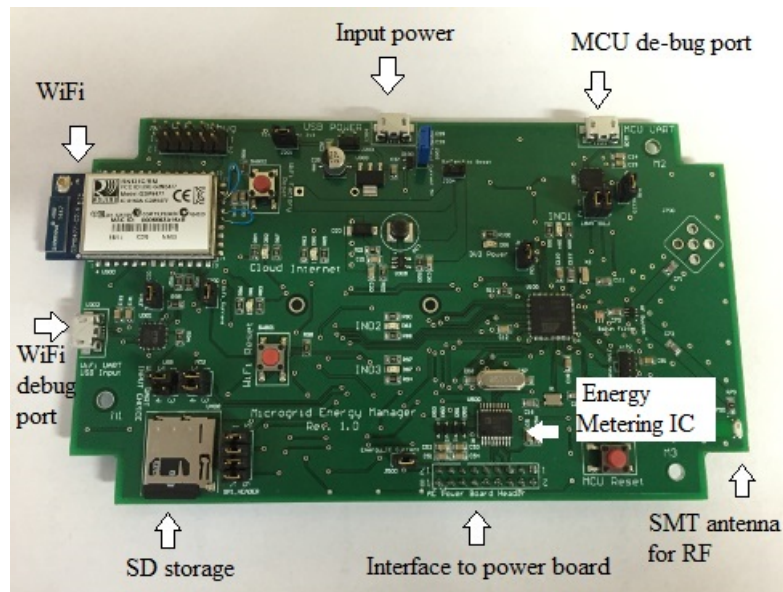


FIGURE 5.3: MEM Communication Board

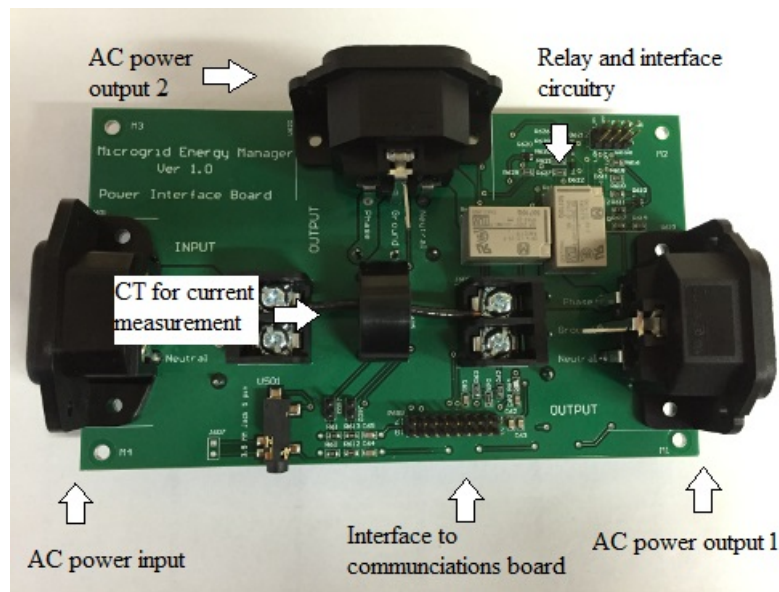


FIGURE 5.4: MEM Power Interface Board

5.3 Wireless Sensor Network (WSN) for Microgrids

While a number of studies have evaluated WSNs in different environments such as buildings, residential establishments or power substation, they fall short of a comprehensive evaluation which takes into account all the key factors that affect the performance of WSN like spatial arrangement, physical environment and interference. Another key concept which several studies fail to take into account is variation of application reliability in wireless sensor networks. For microgrids, the application reliability can be defined as the ability of the system to perform microgrid specific tasks such as sending request messages through MSN to energy sources and loads to obtain grid parameters such as voltage, current, frequency or to send instructions from the MG to turn ON/OFF a specific load or energy source. It is important to evaluate the effect of wireless sensor network on the ability to complete these tasks. The paper evaluates the WSN with the traditional performance metrics such as PRR, LQI and RSSI and builds on that by introducing two new metrics RRR (Response Reception Ratio) and Microgrid Reliability Factor (MRF) which assess WSN in a microgrid context. The study aims to focus on interesting topics such as

- Performance of MSN in different physical environments both indoor and outdoor
- Effect of spatial arrangement (physical topology) of sensor nodes (linear and distributed topology) on the performance of MSN
- Assessment of application level reliability in MSN for microgrid applications.
- Study of correlation between RSSI, LQI and network performance

5.3.1 Physical Environments

Three physical environments were chosen to evaluate the performance of MSN. These include a home, an open field and an electrical engineering lab. The home was chosen to emulate the physical environment of a home microgrid where WSN would be used to monitor and control different loads like TV, washer, dryer and energy sources and storage systems such as PV and a battery system. The electrical engineering lab which houses electric machines, power electronics and mechanical tools and machines was chosen to emulate an industrial setup. An open field was chosen to understand the performance in outdoor environments.

5.3.2 Performance Metrics

This study defines a new performance metric: Microgrid Reliability Factor (MRF) to assess the WSN performance in a microgrid context. It also takes into account traditional evaluation of the network performance through Packet Reception Ratio (PRR) and Response Reception Ratio (RRR). Link Quality Indicator (LQI) and Received Signal Strength Indicator (RSSI) are defined as correlation performance metrics and experiments have been conducted to understand if there is a strong correlation between LQI, RSSI and network performance.

- *Microgrid Reliability Factor (MRF)* - application layer reliability is extremely important in microgrid control and management. MRF can be defined as the ability of the communication framework to perform microgrid related tasks such as

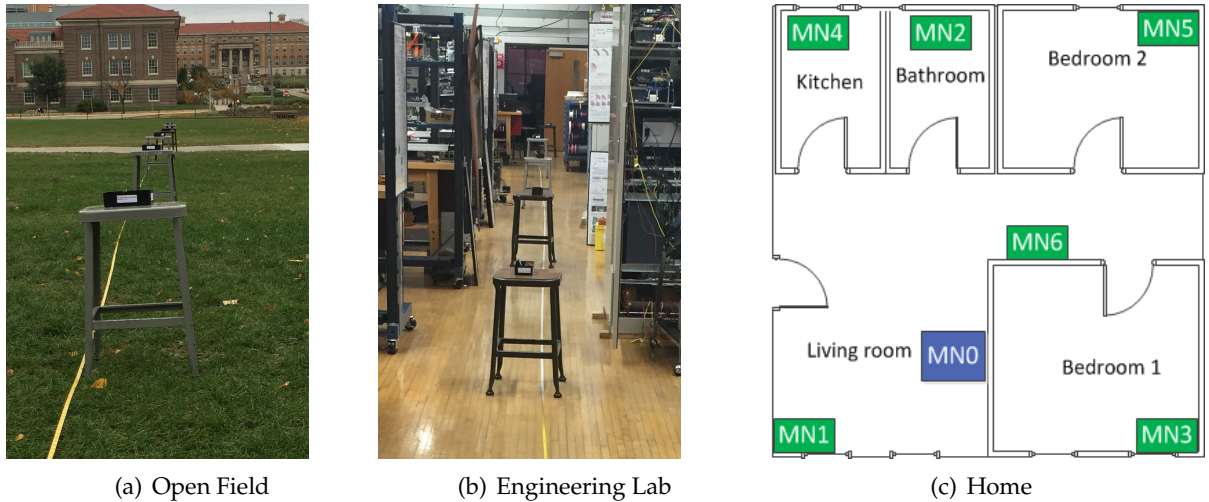


FIGURE 5.5: Physical Environments

1. Sending a request packet to a MN to obtain voltage, current, frequency or energy production or consumption values of the energy source or load.
2. Sending operation set points to provide corrective control of the energy source or loads.
3. Sending command packets to MNs to remotely turn ON/OFF a source or load.

These activities are referred to as application level tasks in this microgrid framework. In case of packet loss, application level reliability is maintained by executing packet retries. The packet retry mechanism is enabled at both MN and MG level so that delivery of request and response packets can be ensured. Acknowledgements (ACKs) are requested by both the MG and MN. On sending a request packet to MN, MG waits n milliseconds for an ACK and on failure re-sends the request packet. The MN sends a response packet and waits m milliseconds for an ACK and on failure re-sends the response packet.

1. *Immediate Retry* - in the event of failure to receive an ACK, both MN and MG re-send the request or the response packet immediately. After a certain number of re-tries, the management system declares the node to be inactive and sends a notification to the user.
2. *Waited Retry* - when the ACK reception fails, MG ignores this and continues to process the packets to other MNs. It waits for a certain time period and then re-tries sending a packet to the MN. After a certain number of waited retries, the node is declared to be inactive. If the MN fails to receive an ACK for a response packet it sent, it waits for a certain time period before sending a response packet to MG.
3. *Hybrid Retry* - this implements both immediate retry and waited retry mechanisms. If MN or MG fail to receive an ACK, they re-send the packet immediately and in the event of failure in the second attempt, it switches to waited retries. After a certain number of waited retries, the node is declared to be inactive.

Packet Reception Ratio (PRR) and Response Reception Ratio (RRR) are used to evaluate the WSN in the traditional wireless networking context. Two correlation parameters RSSI (Received Signal Strength Indicator) and LQI (Link Quality Indicator) are also measured to evaluate their correlation with PRR and RRR.

- *Packet Reception Ratio (PRR)* - this is defined as the ratio of packets sent by the source node to the number of packets received by the destination node.
- *Response Reception Ratio (RRR)* - this study defines a new parameter RRR which is the ratio of packets sent by the source node to the destination node to the number of response packets received for the request packets. This parameter is particularly important in a microgrid framework where delivery of response packets is equally important for grid stability.

Correlation Metrics

- *Received Signal Strength Indicator (RSSI)* - This is the measure of the RF power in a channel.
- *Link Quality Indicator (LQI)* - This is a cumulative value usually used in multi-hop networks to assess the cost of the link. The source node assigns a LQI value to a packet it sends out and this is modified as it propagates through a multi-hop network.

Linear Topology Test

This experiment was conducted to analyze the performance of MSN in a laboratory (to emulate an industrial environment). 7 sensor sending request messages to receiver nodes. The data packets were sent at a rate of a packet per 2 seconds and the destination node was chosen randomly during each transmission. For this test, the nodes were placed in a linear arrangement as shown in *figure 5.6*. The adjacent nodes were placed 15.8 feet apart with MN6 at a distance of 95 feet from MN0. The lab houses electrical machines, power electronics equipment, electrical and mechanical tools and lab benches.



FIGURE 5.6: Linear Topology Test

Over the course of the experiment, a total of 555 data packets were sent by the central node (MN0). In response to these request data packets, 549 ACKs and 546 responses were received. *Figure 5.8* shows the individual node and overall system performance of the sensor network. Background noise was measured during every message reception and it remained constant at -90 dBm throughout the course of the experiment. Several interesting observations were made from this experiment. The constitution of the physical environment plays a big role in the performance of the nodes. MN6 was placed in an area which also housed a large metal cabinet, metal frames and a wooden door. On analyzing the performance of MN6 which experienced packet delivery failures, a major reason was found to be packet delivery failure at the physical medium level which can be attributed to the proximity of MN6 to the physical obstructions

and metal objects. Figure 5.7 shows the RSSI and LQI variation for each node. MN6 showed high variation in LQI values and this can be correlated with its poor performance in comparison with the rest of the MNs. Similar correlation can be seen for the LQI variation for MN3 and its PRR and RRR values. Although MN5 shows the greatest variation in RSSI values among MNs, it exhibits 100% PRR and RRR. On the contrary, MN6 shows almost constant RSSI value throughout the course of the experiment. For the laboratory environment, LQI served as a good indicator of network performance whereas RSSI does not provide any correlated behavior with network performance.

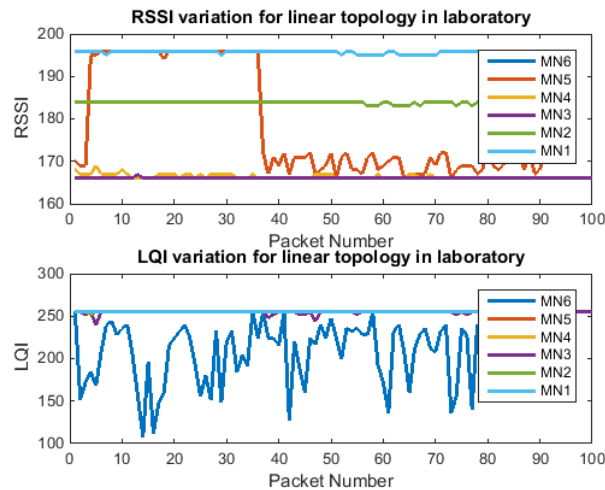


FIGURE 5.7: RSSI and LQI variation for linear topology in the laboratory

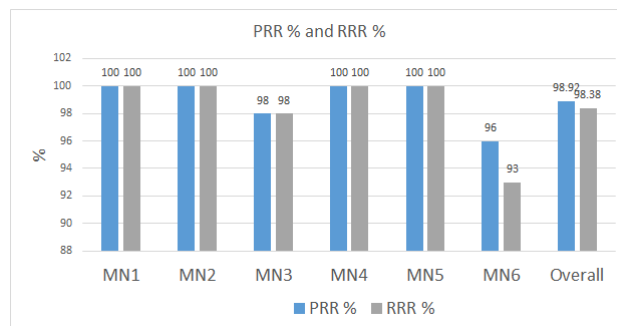


FIGURE 5.8: PRR and RRR for linear topology in the laboratory

Microgrid Reliability Test for Linear Topology

A series of five experiments were conducted to evaluate the Microgrid Reliability Factor (MRF) in WSN. The nodes were placed in a linear topology with a distance of 10 feet between adjacent nodes and 60 feet between the farthest two nodes. With each experiment, the nodes were re-arranged to evaluate effect of physical placement on the overall system and the individual node. The goal of these experiments is to evaluate the number of retries it takes for MG (MN0 in this case) to relay a message successfully and get back an ACK. These experiments implement a hybrid retry mechanism and ACKs are enabled at both MN and MG (MN0). Figure 5.9 shows the result for MN0

in all five experiments. Similar results can be generated for the rest of the MNs. Performance of MN0 is shown and discussed here as it performs the role of the central controller.

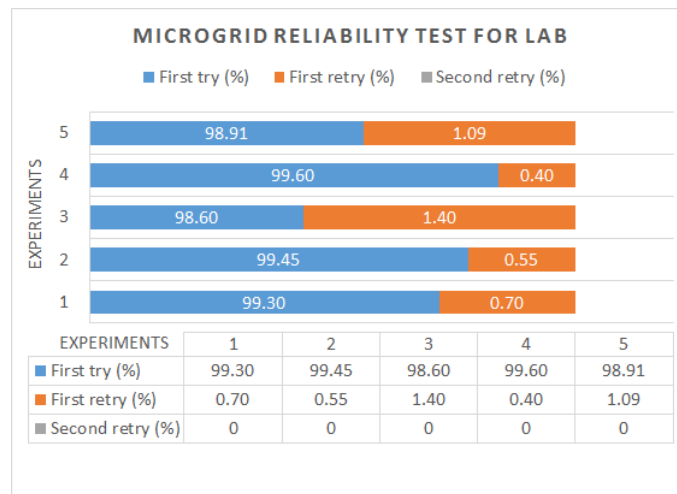


FIGURE 5.9: Microgrid Reliability Test for linear topology in the laboratory

The experiments show 100% application reliability with a hybrid packet retry system. All packets were successfully delivered to the MNs from MN0 either on the first attempt or on a re-try. It can be observed from the figure that nearly 99% of the packets were delivered in the first attempt. It can also be observed that all the packets were successfully delivered within the first retry.

Distributed Topology Test

In this experiment, the MN nodes were placed in a distributed arrangement in the laboratory. The nodes were spread across the lab as shown in *figure 5.10*. A total of 563 packets were sent by MN0 and it received 563 ACKs and 560 responses. The overall system PRR was 100% and RRR was 99.46%. Background noise was measured at the reception of every message and it remained constant at -90 dBm. It was found that LQI and RSSI values do not provide any correlated behavior with network performance. LQI remained constant at 255 throughout the experiment for all nodes with variation for MN4. This contradicts the 100% PRR and RRR observed for MN4. The PRR and RRR for all the nodes is visualized in *Figure 5.12*. The RSSI and LQI variation for this topology can be seen in *Figure 5.11*.

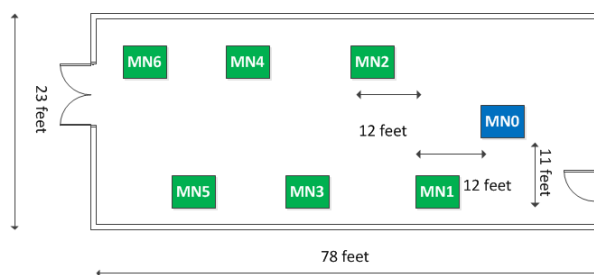
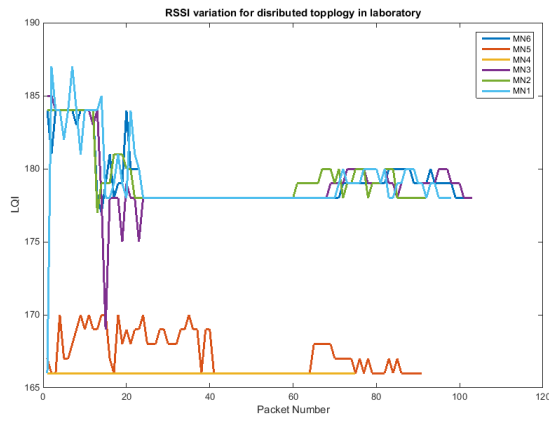
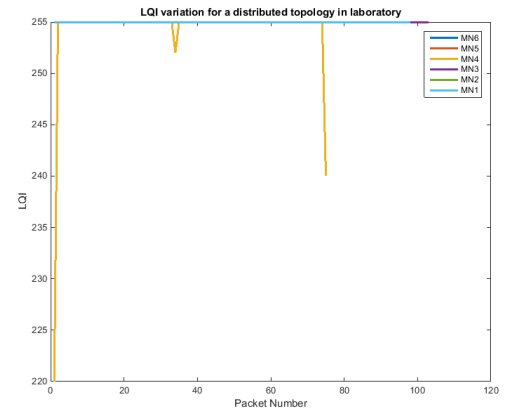


FIGURE 5.10: Distributed Topology in the laboratory



(a) RSSI for distributed topology in lab



(b) LQI for distributed topology in lab

FIGURE 5.11: RSSI and LQI for distributed topology in lab

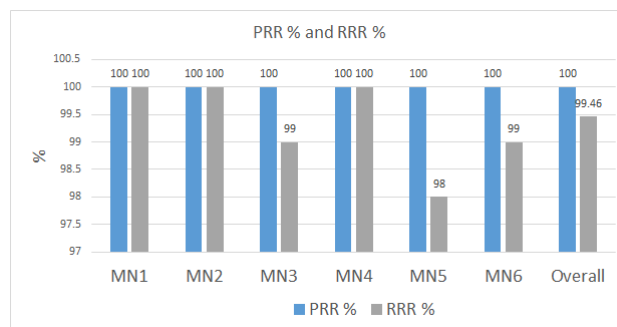


FIGURE 5.12: PRR and RRR for distributed topology in the laboratory

5.3.3 Home Environment

This experiment was conducted to evaluate the physical environment in a home. The physical configuration of MNs are shown in *figure 5.13*. A total of 647 packets were sent by MN0 and it received 528 ACKs and 520 responses. The overall system PRR was 82% and RRR was 80.3%. PRR and RRR for each node can be seen in *Figure 5.15*. Packet delivery failures were mostly observed due to failure at the physical medium level which can be attributed to obstructions due to walls and doors. The RSSI and LQI variation for this topology can be seen in *Figure 5.14*.

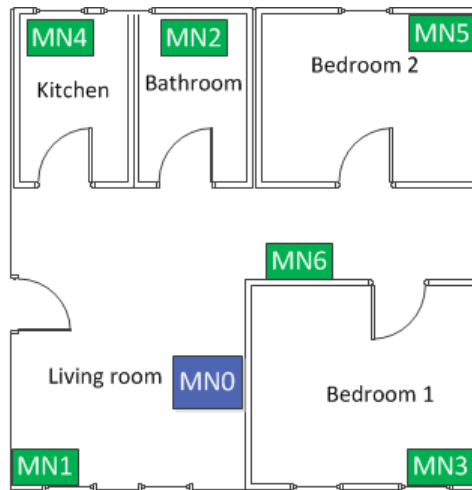


FIGURE 5.13: Distributed topology in home

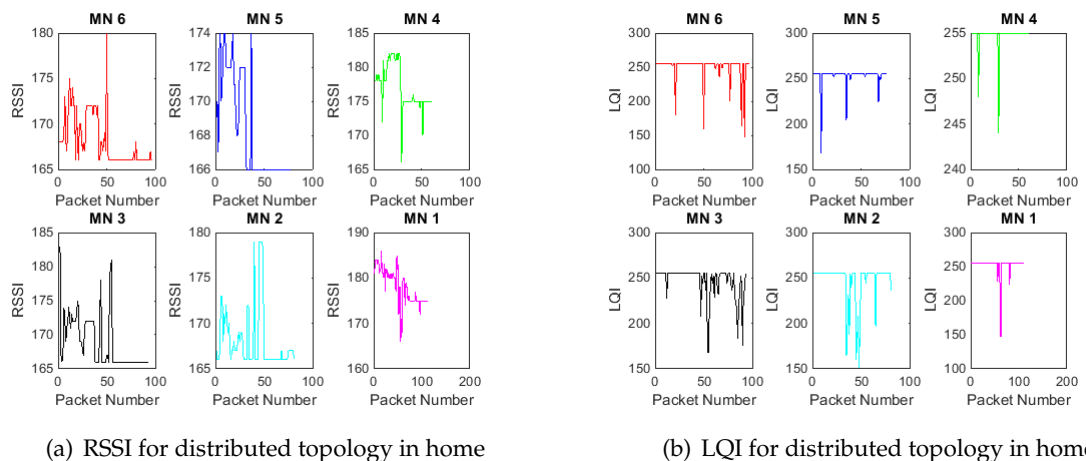


FIGURE 5.14: RSSI and LQI for distributed topology in home

MN0 and MN1 shared Line-of-Sight (LoS) configuration. The rest of nodes were separated by walls and closed doors. It was observed that both LQI and RSSI show high variation for all nodes and it is difficult to use them to estimate the performance of the network. In a home environment, the nodes may or may not share a LoS configuration. This depends on the home occupants and also the number of loads and sources. In the case of weak links between nodes, range extenders can be added to boost network

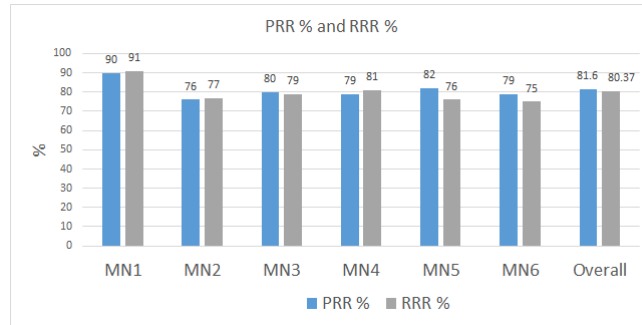


FIGURE 5.15: PRR and RRR for distributed topology in home

performance. The only objective of these range extenders will be to relay messages and boost range and performance. They will not serve as MN or MG.

Microgrid Reliability Test

A series of five experiments were conducted to evaluate the Microgrid Reliability Factor (MRF) in a home environment for a distributed placement topology. The nodes were re-arranged with each experiment to introduce variability. Typically each room in the house had a node with the living room having two due to its larger size. These experiments implement a hybrid retry mechanism and ACKs are enabled at both MN and MG (MN0). Figure 5.16 shows the result for MN0 in all five experiments.

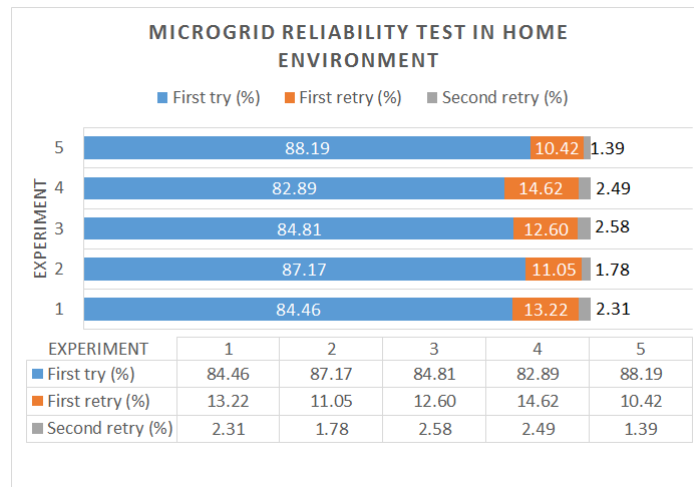


FIGURE 5.16: Microgrid reliability test for home environment

In a home environment, 100% application reliability was achieved. The percentage of packets delivered to MNs in the first attempt varied from 82% to 88% for the experiments. When the packet delivery fails at the first attempt, the MN0 retries to send the packet immediately. In the event of first re-try failure, it backs-off and re-sends the packet after a certain time period.

5.3.4 Field

Linear and distributed topology was tested for an outdoor environment. An open field was chosen to emulate the physical environment of an outdoor microgrid. 7 sensor

nodes were used with one node (MN0) acting as a central node. The packet transmission rate was set at 1 packet/2s and the destination node was chosen randomly at each transmission.

5.3.5 Range Test

This experiment was conducted to assess the maximum range between two nodes in an outdoor environment with PRR and RRR greater than 99% . In an open field this was found to be 225 feet when the two nodes are at an elevation of 2 feet from the ground.

Linear Topology Test

The sensor nodes were placed in a linear arrangement as shown in *Figure 5.5(a)*. Adjacent nodes were separated by distance of 15.8 feet and the farthest nodes were 95 feet apart. A total of 570 packets were sent by MN0 and it received 560 ACKs and 560 responses. The overall system PRR and RRR was 98.2% . PRR and RRR for each node can be seen in *Figure 5.18*. It is difficult to draw conclusive estimate of the network performance by looking at the LQI and RSSI values as they showed great variation which did not correlate with the performance. The RSSI and LQI variation for this topology can be seen in *Figure 5.17*.

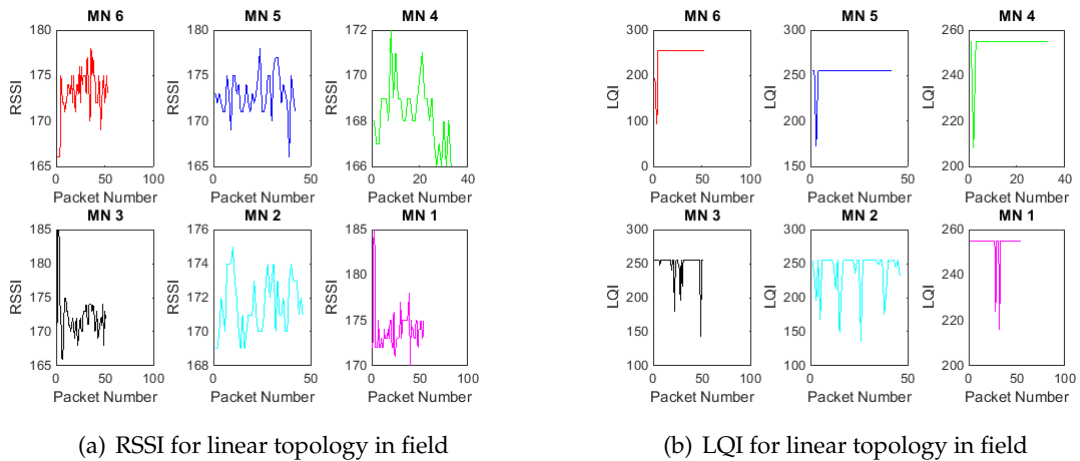


FIGURE 5.17: RSSI and LQI for linear topology in field

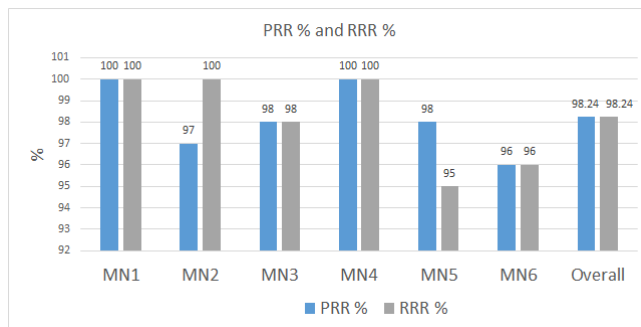


FIGURE 5.18: PRR and RRR for linear topology in field

Microgrid Reliability Test

A series of five experiments were conducted to evaluate the Microgrid Reliability Factor (MRF) in an outdoor environment. The nodes were placed in linear topology with a distance of 10 feet between adjacent nodes and 60 feet between the farthest. With each experiment, the nodes were re-arranged to introduce variability. These experiments implement a hybrid retry mechanism and ACKs are enabled at both MN and MG (MN0). *Figure 5.19* shows the result for MN0 in all five experiments.

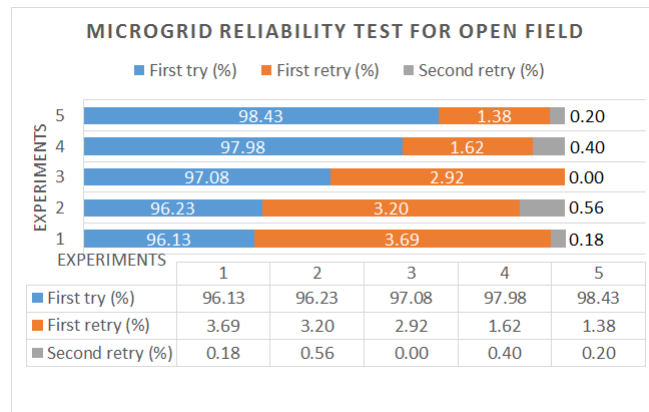


FIGURE 5.19: MRF for linear topology in an open field

Distributed Topology Test

In this experiment, the nodes were placed in a distributed arrangement as shown in *figure 5.20*. MN0 sent a total of 642 packets and received 618 ACKs and 600 responses with a 96.26% PRR and 93.45% RRR. Individual node and overall system performance can be seen in *Figure 5.22*. The RSSI and LQI variation is illustrated in *Figure 5.21*. It can be seen that both RSSI and LQI show great variation throughout the experiment and it is difficult to estimate network performance based on these parameters.

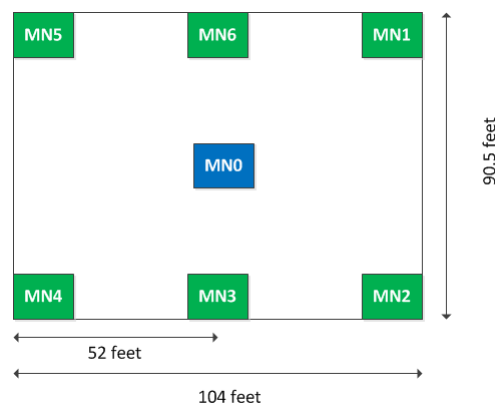


FIGURE 5.20: PRR and RRR for distributed topology in an open field

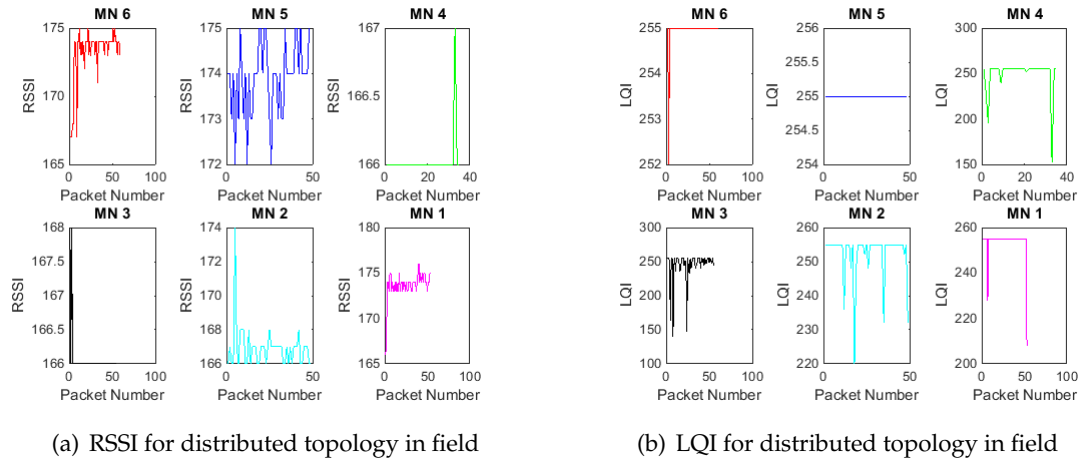


FIGURE 5.21: RSSI and LQI for distributed topology in field

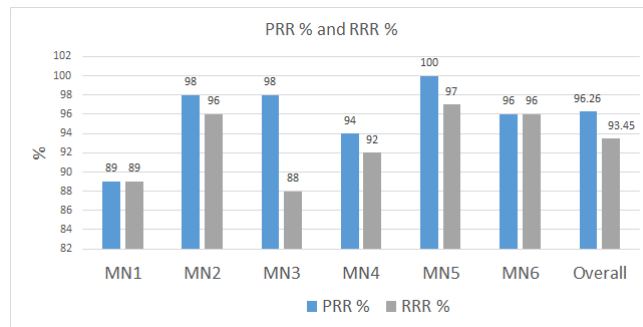


FIGURE 5.22: PRR and RRR for distributed topology in field

5.4 MSN Conclusion

This study introduces a new communication framework for microgrid control and management called Microgrid Network (MN) which consists of Microgrid Cloud (MC) and Microgrid Sensor Network (MSN). In-depth performance evaluation of MSN was conducted which implements an IEEE 802.15.4 based sensor network. An engineering lab, home and open field were chosen to emulate physical environments of microgrids with linear and distributed physical topologies. The performance of the MSN due to physical environment and spatial arrangement was studied. The correlation between LQI, RSSI and network performance was evaluated.

- Effect of physical environments on the network performance is significant. For both the spatial arrangement topologies, the engineering lab performed significantly better compared to an open field and a home environment.
- It was observed that elevation of the nodes have a huge impact on the performance of network. For outdoor environment tests, the packet transmission failed at a physical medium level when the nodes were placed on the ground. Raising the elevation of the nodes to about 2 feet from the ground increased PRR and RRR to greater than 97%
- The constitution of the physical environment also affected the performance. Nodes placed close to metal structures, wall corners, behind solid objects exhibited poor performance.
- While LQI showed correlation with the network performance for linear topology in the laboratory, it failed to show any correlation in other environments and topology. RSSI shows no correlation with the network performance in any topology or environment.
- The MSN framework achieved 100% application reliability through packet retry mechanisms for all environments and topologies.
- The rate of packet transmission was maintained at 1 packet/2s for all experiments. However, it was found experimentally that the rate could be increased to 1 packet/300ms maintaining the same network performance. This is particularly useful in case of sub-second operation for microgrids.
- Self healing and mesh capabilities of MSN framework has several advantages over traditional wireless capabilities. Introducing extender nodes (meant only for routing messages) increased the range and reliability of the network link between source and destination nodes. This was experimentally verified by placing a MN at relatively low elevation behind physical objects. As expected, the number of retries for successful delivery was high. A router node was placed between MN0 and the destination node and this improved the performance of the link drastically. Similar experiments were conducted to increase the range between nodes by placing intermediate router nodes.
- It was found experimentally that the communication range between 2 nodes (without multi-hop) depended on transmit power and the elevation. Elevation of the nodes to about 2-3 feet above the ground showed highest performance. The transmitter has different transmit power levels (-16.5 dBm to 3.5 dBm) which can be set by the user. It was observed that the communication range increased with increase in transmit power.

5.5 Cyberphysical System (CPS) for Microgrids

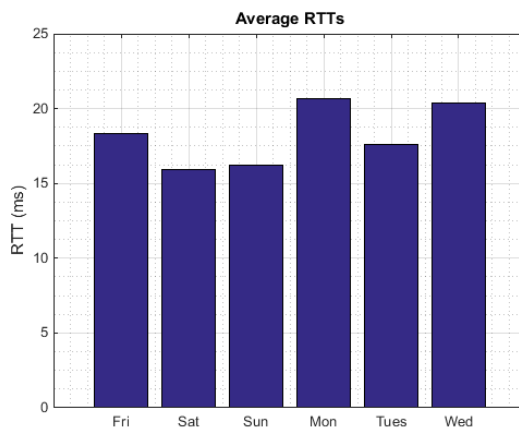
5.5.1 Objective and Importance

The objective of this study is to characterize parameters of a computer network and embedded computing system in an integrated environment. While studies [37], [38], [39], [40], [41] have been conducted to measure and assess network performance which include latency, packet loss and jitter, extensive studies have not been conducted to study the behavior of a cyberphysical system. Cyberphysical system consists of an integration of cyber components such as servers, wireless and wired networks, data storage and physical components such as measurement sensors, embedded systems, power systems etc. In some cases, these systems are time-sensitive: power systems, industrial control environments etc. The cyber system in this study consists of a cloud (server), Internet Service Provider (ISP) network/ university network, switches and routers. The embedded system platform consists of a low power RF System-on-Chip that is integrated with peripherals such as energy metering, storage, real time clock and wireless capabilities (MG). Tests were conducted to measure the RTT (Round Trip Time) between the cloud and the physical system which in this case is the embedded platform or MG. Second set of experiments were conducted where interference was introduced to assess the behavior of the system and identify the variation of the RTT. RTT is an important parameter for systems which are connected to the cloud or which run a local sensor network. For time sensitive applications, it is important for the RTT to be within the critical value to avoid failure of the system.

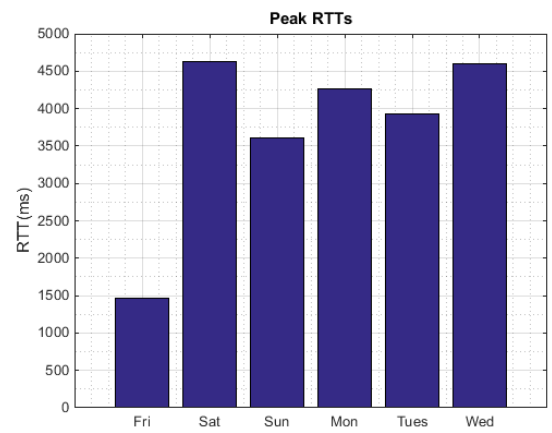
This study deals with introducing secondary and tertiary control for managing different entities in the microgrid. The central intelligence in this control scheme is a cloud (server) which makes intelligent decisions based on information relayed from different entities in the microgrid. The process of message transmission, processing and relaying back has to take place in the range of milliseconds or less than three-four seconds. This is critical to prevent grid failure. To achieve this kind of time sensitive performance, one has to understand individual subsystems behavior in a cyberphysical environment and its effects on overall system performance. The experiments conducted in this section help us assess important parameters in a cyberphysical system.

5.5.2 Round Trip Time (RTT) assessment without interference

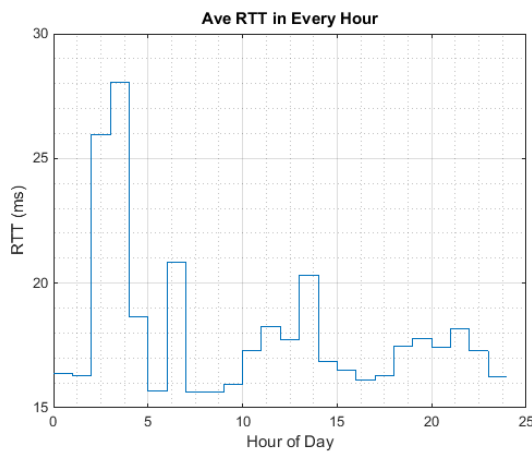
This experiment characterizes the RTT for a simple cyberphysical system. The physical system is a MEM gateway (MG). The cyber system consists of a router, university network and a cloud in WiNGS lab. The architecture of the remote server is described in *chapter 4*. The experiment was setup to measure RTT between MG and MC. MC sends a TCP packet (50 bytes) to MG every 5 seconds. The MG receives this packet and sends back a response. This RTT is recorded by the server. The objective of this performance is to assess how RTT varies for a cyberphysical system over hour, time of day and day of week. If the TCP connection fails at the physical or the server end, MEM gateway resets the connection immediately.



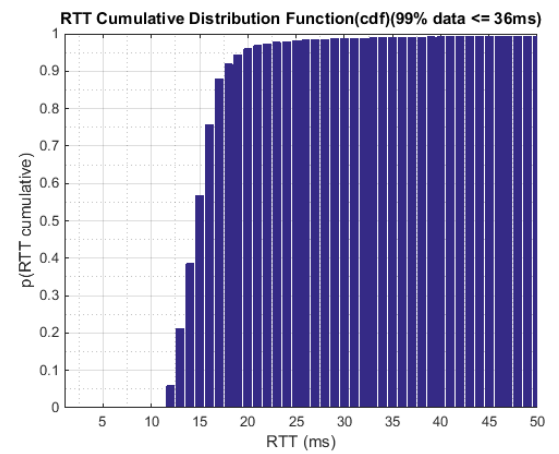
(a) Average RTT per day basis



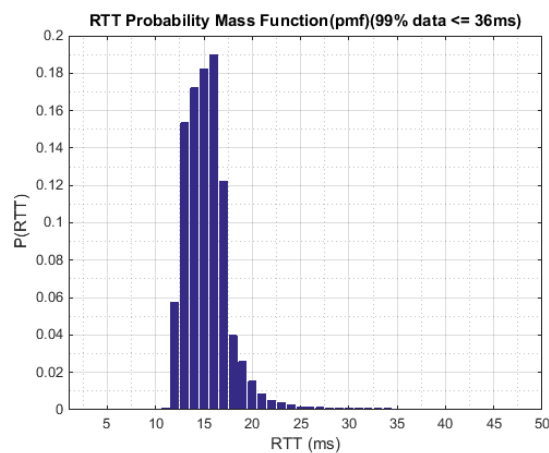
(b) Peak RTT per day basis



(c) Average RTT per hour basis



(d) RTT Cumulative Distribution Function



(e) RTT Probability Mass Function

FIGURE 5.23: RTT variation over the course of the experiment

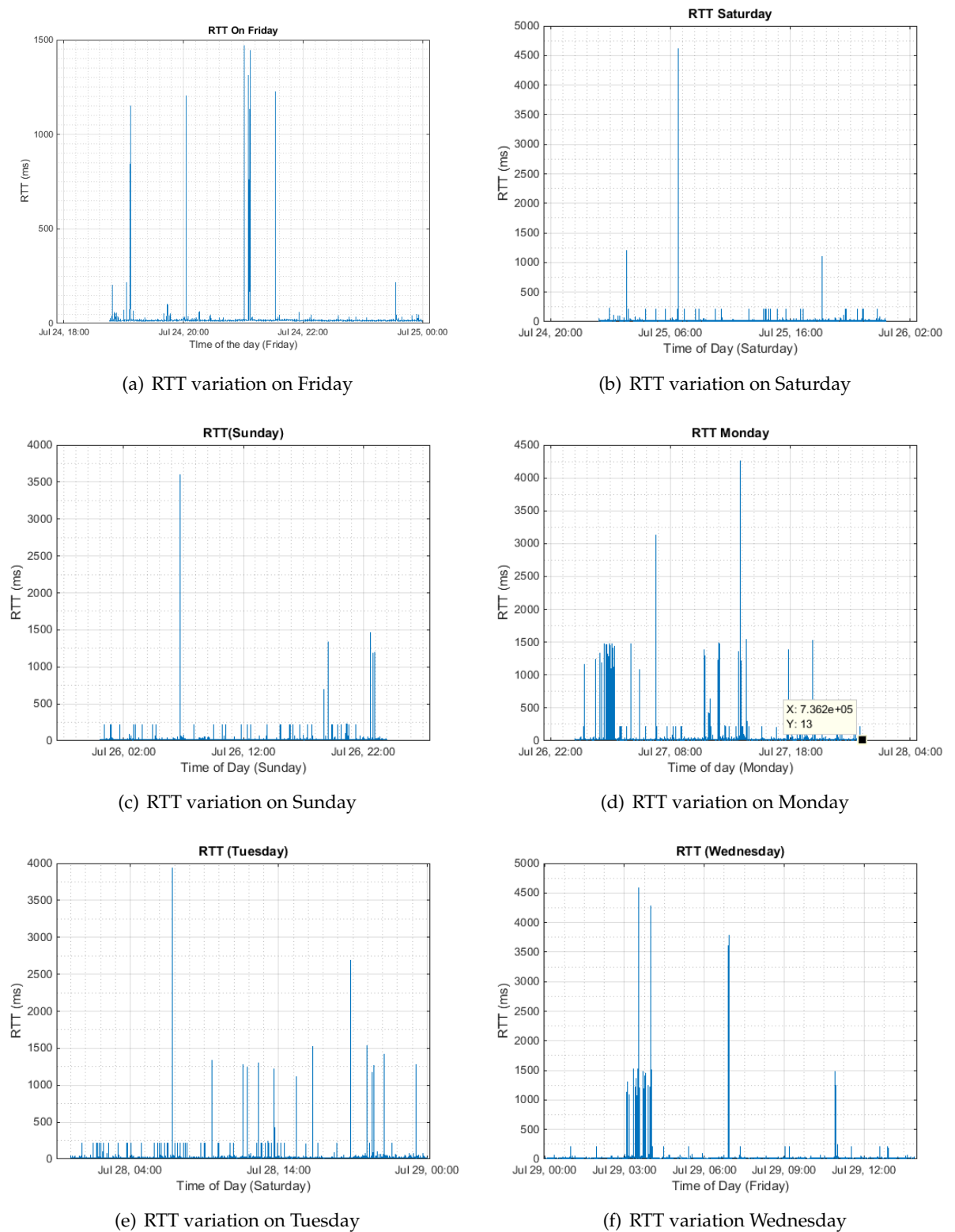


FIGURE 5.24: RTT variation per day basis

5.5.3 RTT assessment with microwave appliance interference

Home and industrial environments have a number of sources of radio interference. This might cause reliability issues for wireless links. This can affect wireless networks such as IEEE 802.11 or IEEE 802.15.4. Performance of IEEE 802.11 networks in home is studied in [42]. Interference due to microwave appliances was observed which caused packet loss as high as 60 percent when the appliance was placed at a distance of 0.5 feet from Wi-Fi. A number of studies have tried to characterize Wi-Fi performance due to both narrow and wide-band interference [43], [44], [45]. The study [45] observed that a residential microwave caused a Continuous Wave (CW) like interference which was centered around 2.45 GHz. It was observed that the total active interference period was about 8 ms (out of 20 ms power cycle at 50 Hz or 16 ms at 60 Hz). In order to assess how interference affects RTT in a cyberphysical system, an experiment was setup to measure the variation of RTT with a microwave close to the Wi-Fi on the MEM gateway. The experiment was setup similar to the previous section. During packet transmission and reception between MC and MG, the microwave was operated intermittently. A section of the experiment is shown in *figure 5.25(a)*.

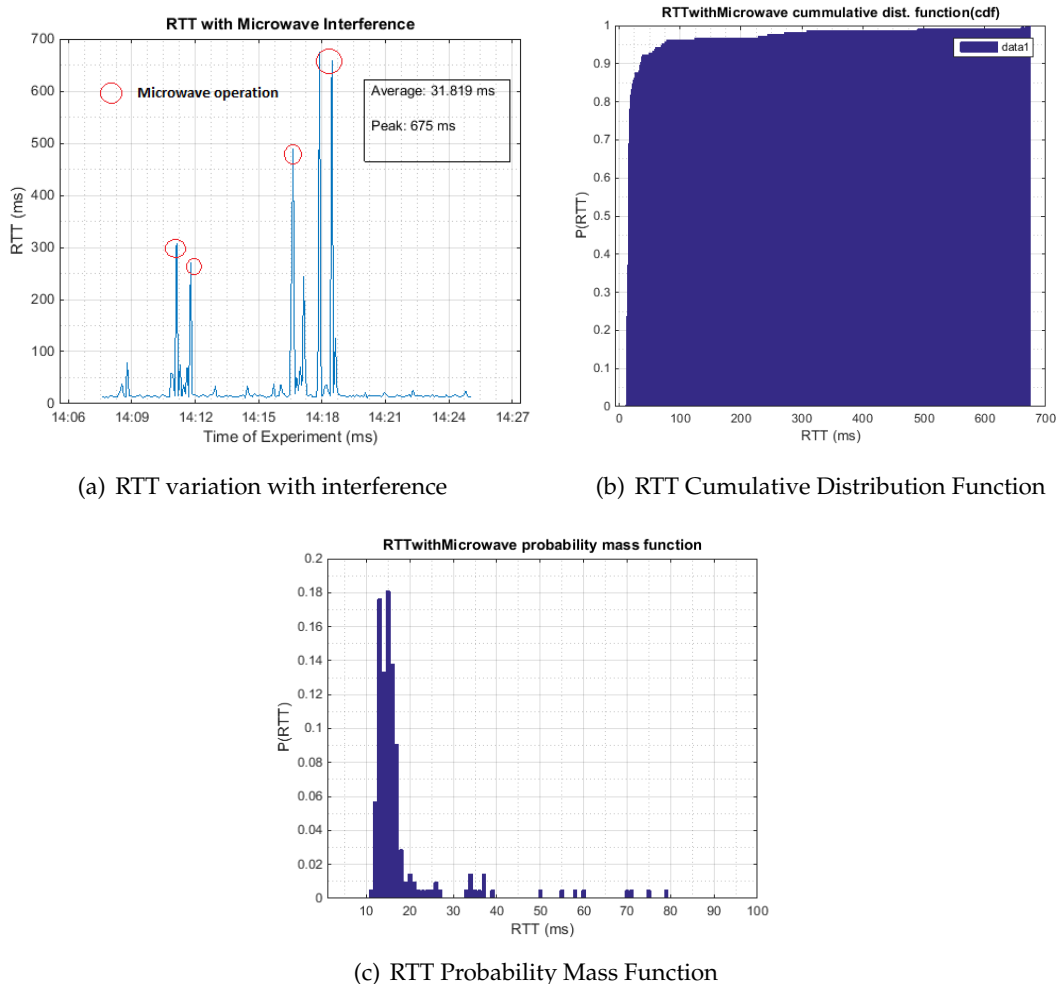


FIGURE 5.25: RTT variation due to interference

5.6 CPS Tests Conclusion

5.6.1 RTT without interference

- The average RTT over the course of 6 days was measured to be around 15- 20 ms. This is illustrated in *figure 5.23(a)*.
- Peak RTT variation was observed between 2 - 5 am. One of the factors could be due to regular network updates on the university network which are scheduled during this time.
- RTT variation was seen throughout the day for all 6 days of the experiment. This can be a combination of factors - increased network traffic, increased traffic on the access point to which the Wi-Fi module was connected to and higher bandwidth applications on connected devices.
- The peak RTT varied from 1468 ms - 4662 ms. This can be seen in *figure 5.23(b)*.
- From the probability cumulative distribution function, it can be observed that 99% of the RTT values occur within 37 ms.

5.6.2 RTT with interference

The microwave oven was placed in close proximity with the Wi-Fi module on MG. The microwave appliance was operated intermittently and it was observed that RTT increased drastically when the microwave oven was switched on. This can be seen in *figure 5.25(a)*. It was also observed that there was no loss of data at the application level. Possible reason for this behavior could be that the microwave appliance caused interference which resulted in packet loss at the Wi-Fi module. This caused TCP packet re-ordering which resulted in application level reliability. The cumulative distribution function and probability mass function plots can be seen in *figures 5.25(b)* and *5.25(c)* respectively.

Conclusion and Future Work

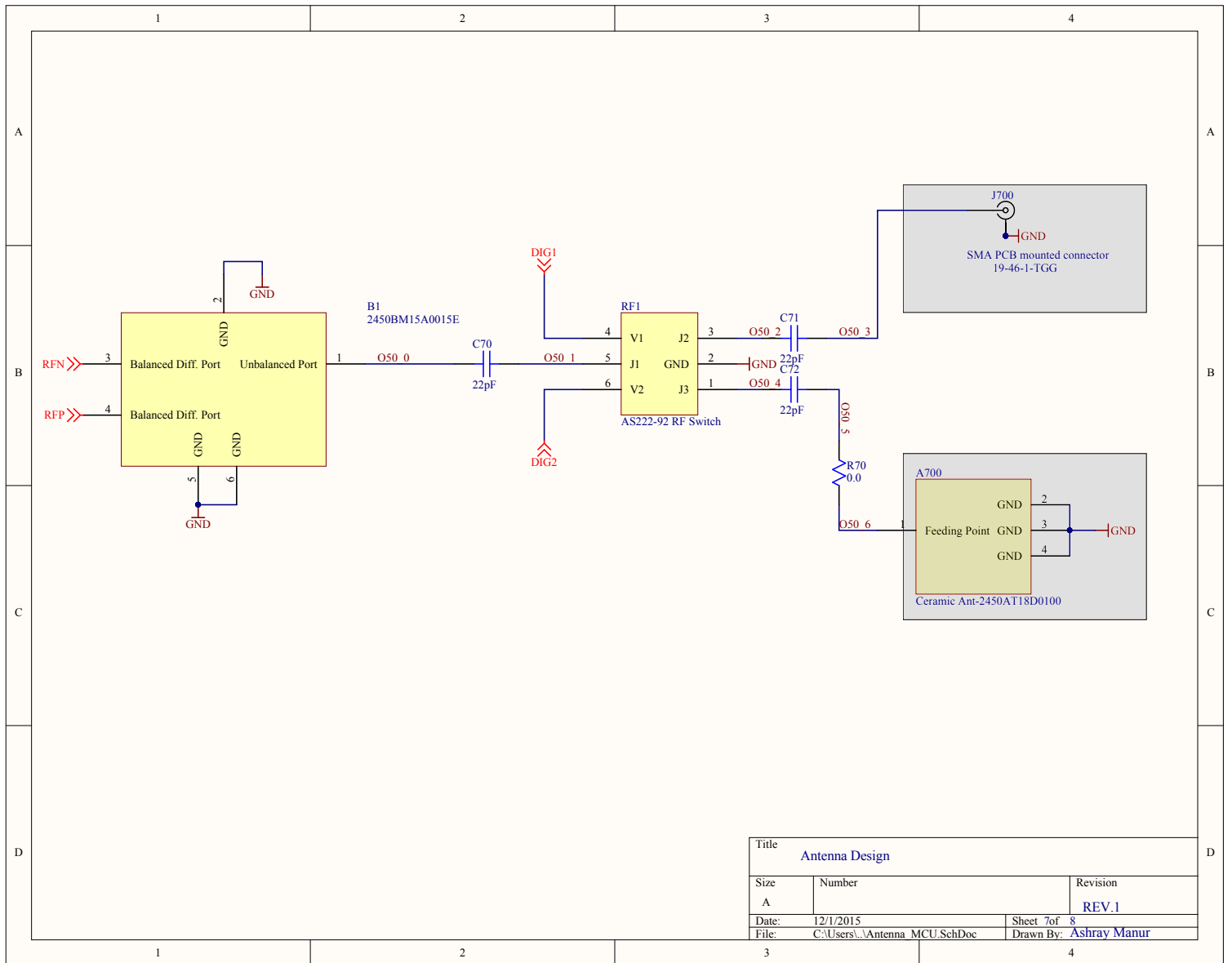
Advancements in power electronics, communication and a thrust to move towards a greener and decentralized power system has led to the popularity of microgrids. The microgrid global market is estimated to grow to a \$ 40 billion industry in 2020 with nearly 24000 industrial and commercial sites ready for microgrid installation. A core component of a microgrid is the energy management system which is responsible for ensuring reliable operation of the microgrids in grid-connected and island mode of operation. This study aims to develop a complete end-to-end framework for this management system. The proposed microgrid energy management system is built on the Internet of Things (IoT) and Wireless Sensor Network (WSN) paradigm. This unique framework of integrating a power system with advanced communication technologies like cloud computing, wireless mesh networks etc. gives better control, management and monitoring system for microgrids. This study aims to develop and test the infrastructure in this context. Microgrid cloud was developed with an event-based server framework with capability to handle thousands of connections in a time sensitive environment. The performance of wireless sensor networks and the cyberphysical infrastructure for a power system was studied in detail. With a goal of achieving 100 % application reliability in communication frameworks, the MSN was tested in various physical environments, spatial orientation and message transmission rates. 100 % application reliability was achieved using different types of retry mechanisms. The sensor network performance was also assessed with traditional parameters such as PRR, RSSI and LQI. Second part of the study focuses on assessing network performance when the power system is integrated with cyber components such as cloud, computer networks etc. It gives good insight on RTT variation over time of day or week and will help set design rules to deal with increased packet transmission or reception times. An embedded platform was designed and developed with capabilities such as energy metering, time-stamping, storage, RF network and Wi-Fi capabilities.

Future work includes developing intelligent algorithms for the energy management system which extends beyond monitoring capabilities. Secondary and tertiary control for microgrids have to be implemented using the infrastructure developed in this study. Another potential for future work lies in extending the functionalities of the web application built in this study to include rich visualization, energy pricing and scheduler. Another potential for future work lies in modeling a power system connected to a cyber environment and assessing if the practical implementation follows the theoretical and simulated models closely. While several studies have modeled power systems and communications separately, not much work has been to comprehensively model this integrated system.

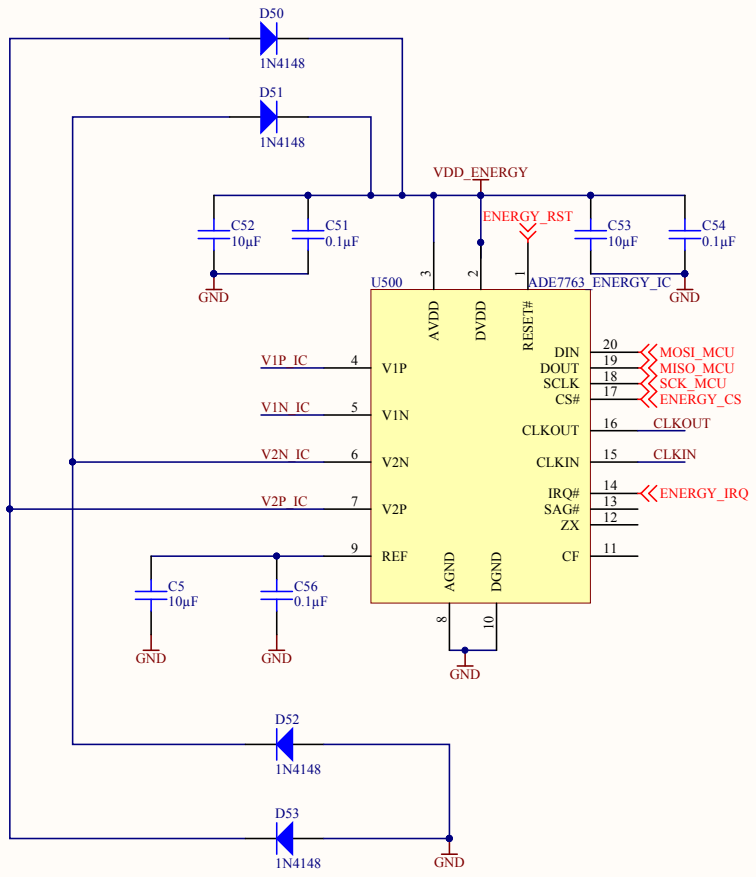
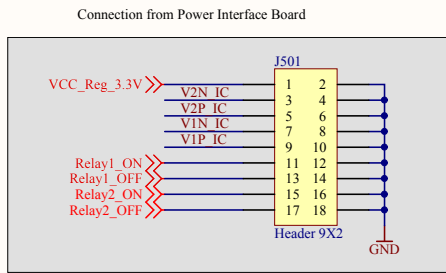
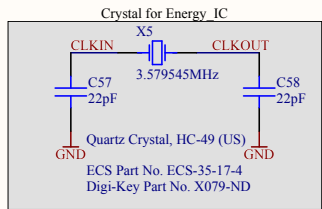
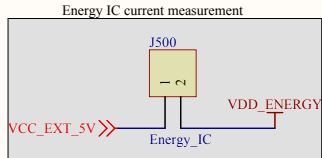
Appendix A

MEM Gateway and Node Schematics

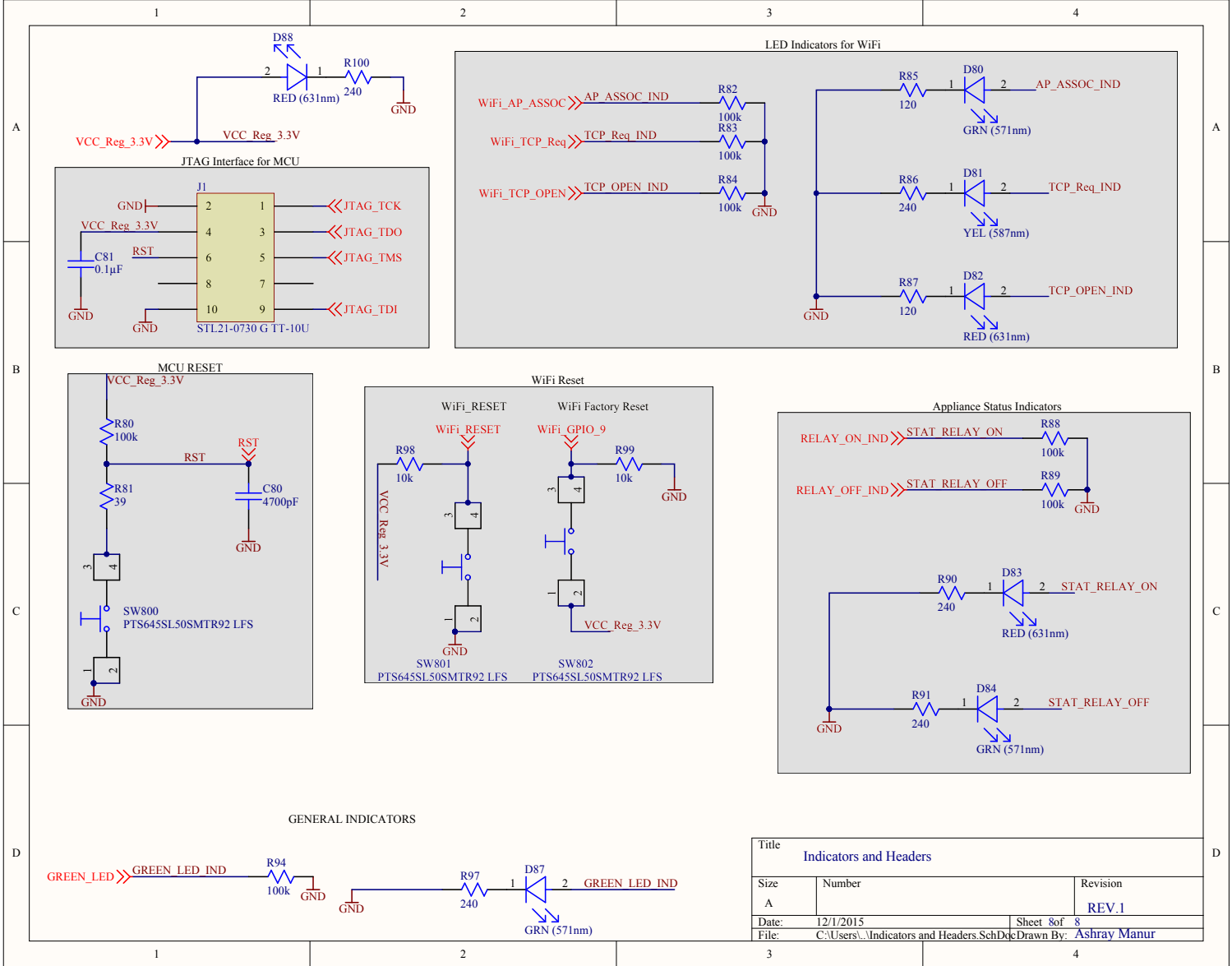
This section contains the schematics for the MEM node and gateway embedded platform. Altium Designer was used to layout the schematics and design the printed circuit board.



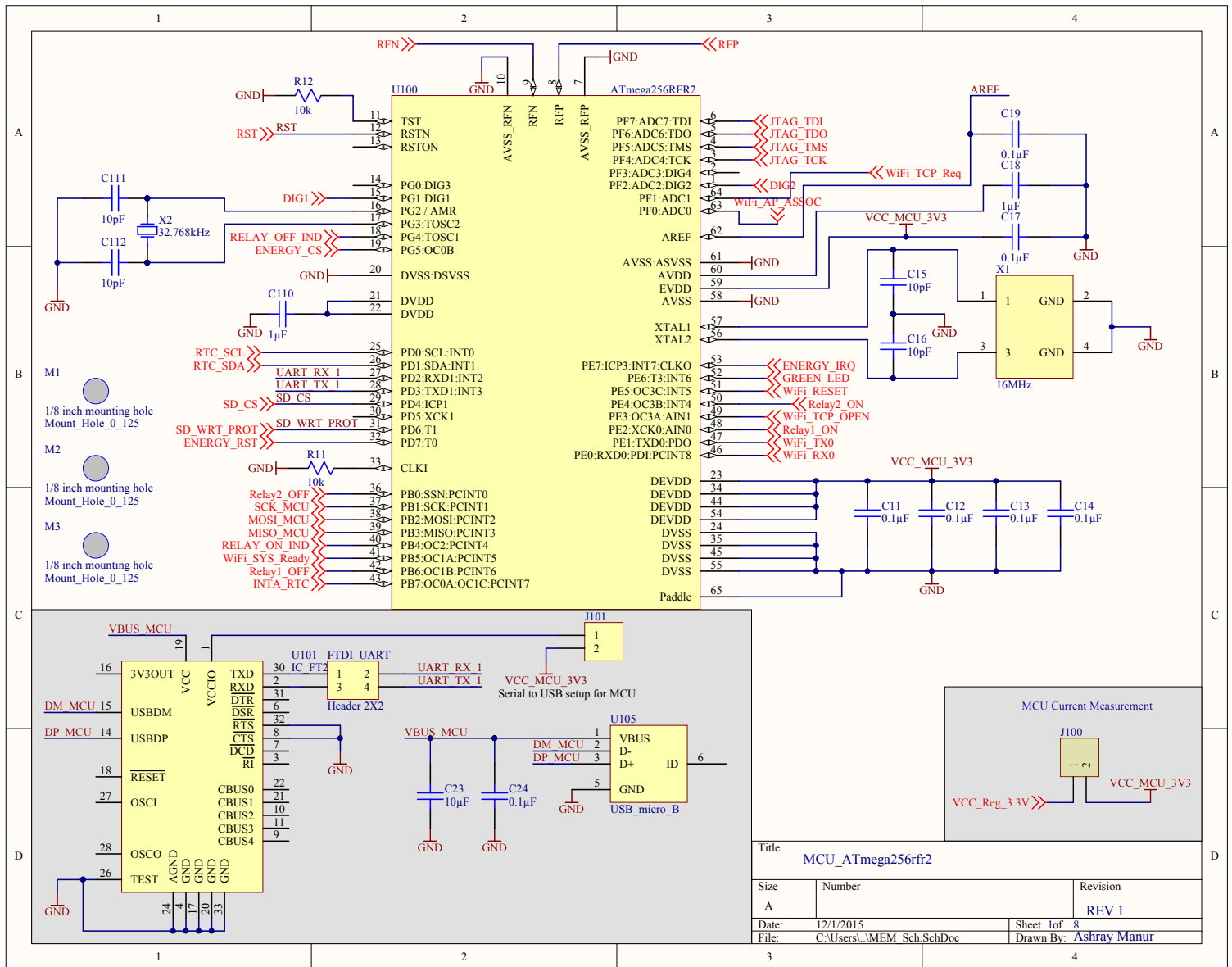
Title		
Antenna Design		
Size	Number	Revision
A		REV.1
Date:	12/1/2015	Sheet 7 of 8
File:	C:\Users\...\Antenna MCU.SchDoc	Drawn By: Ashray Manur



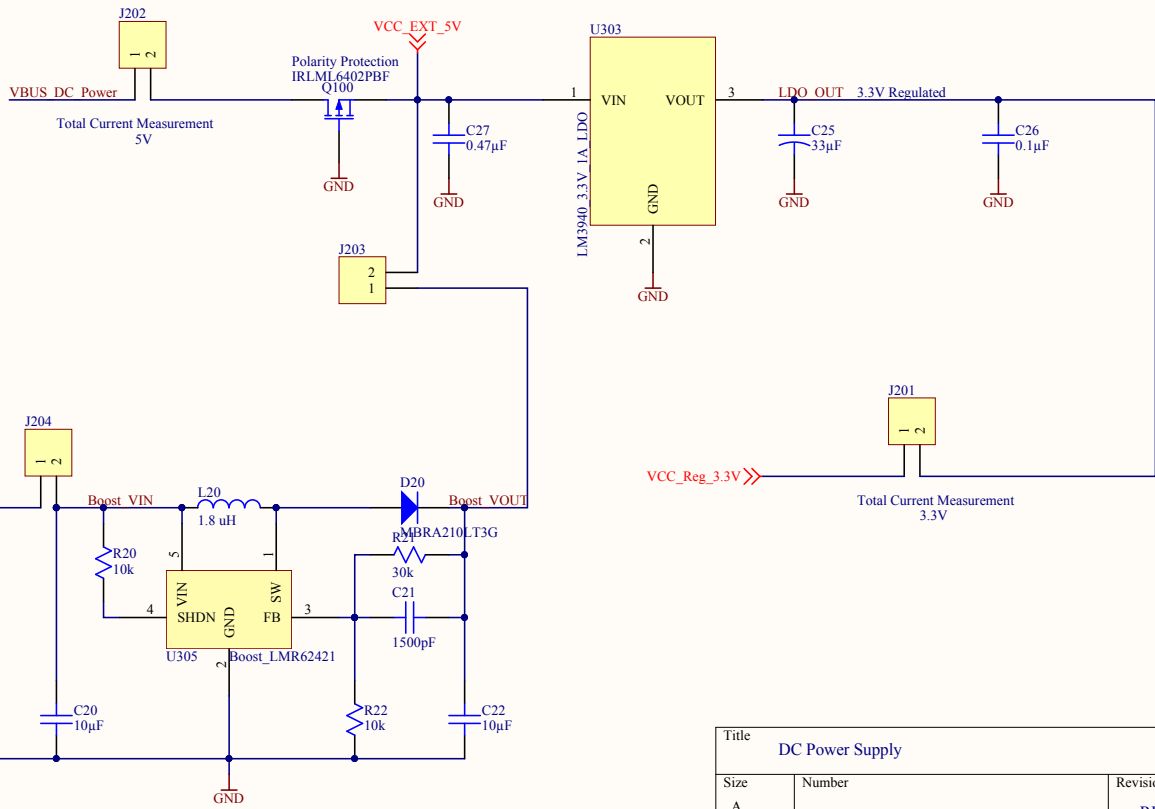
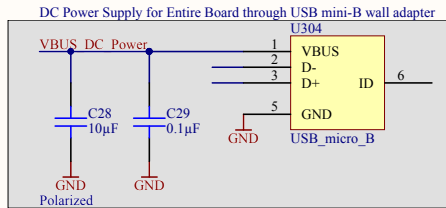
Title		
Energy_IC_ADE_7763		
Size	Number	Revision
A		REV.1
Date:	12/1/2015	Sheet 5of 8
File:	C:\Users\...\EnergyIC_ADE7763.SchDoc	Drawn By: Ashray Manur



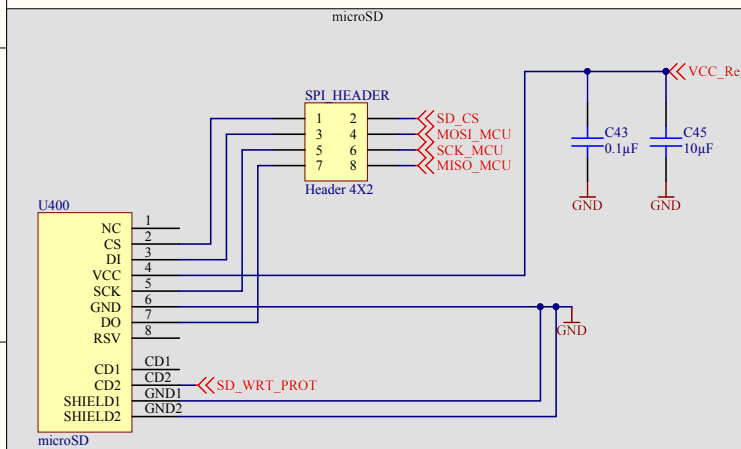
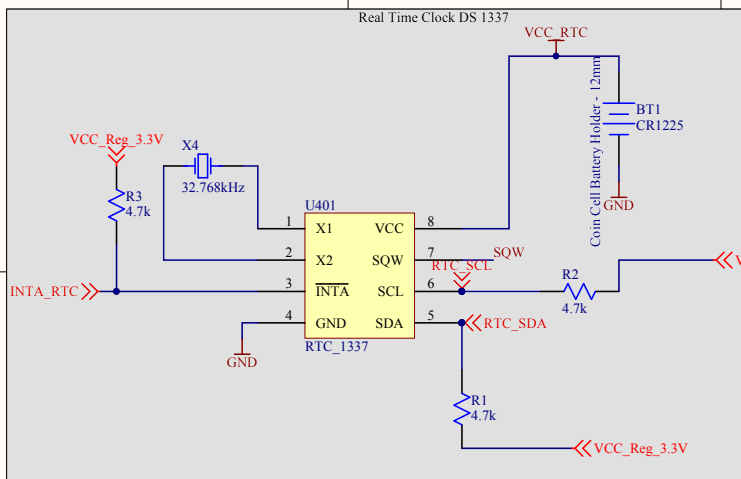
Title		
Indicators and Headers		
Size	Number	Revision
A		REV.1
Date:	12/1/2015	Sheet 8 of 8
File:	C:\Users\...Indicators and Headers.SchDoc Drawn By: Ashray Manur	



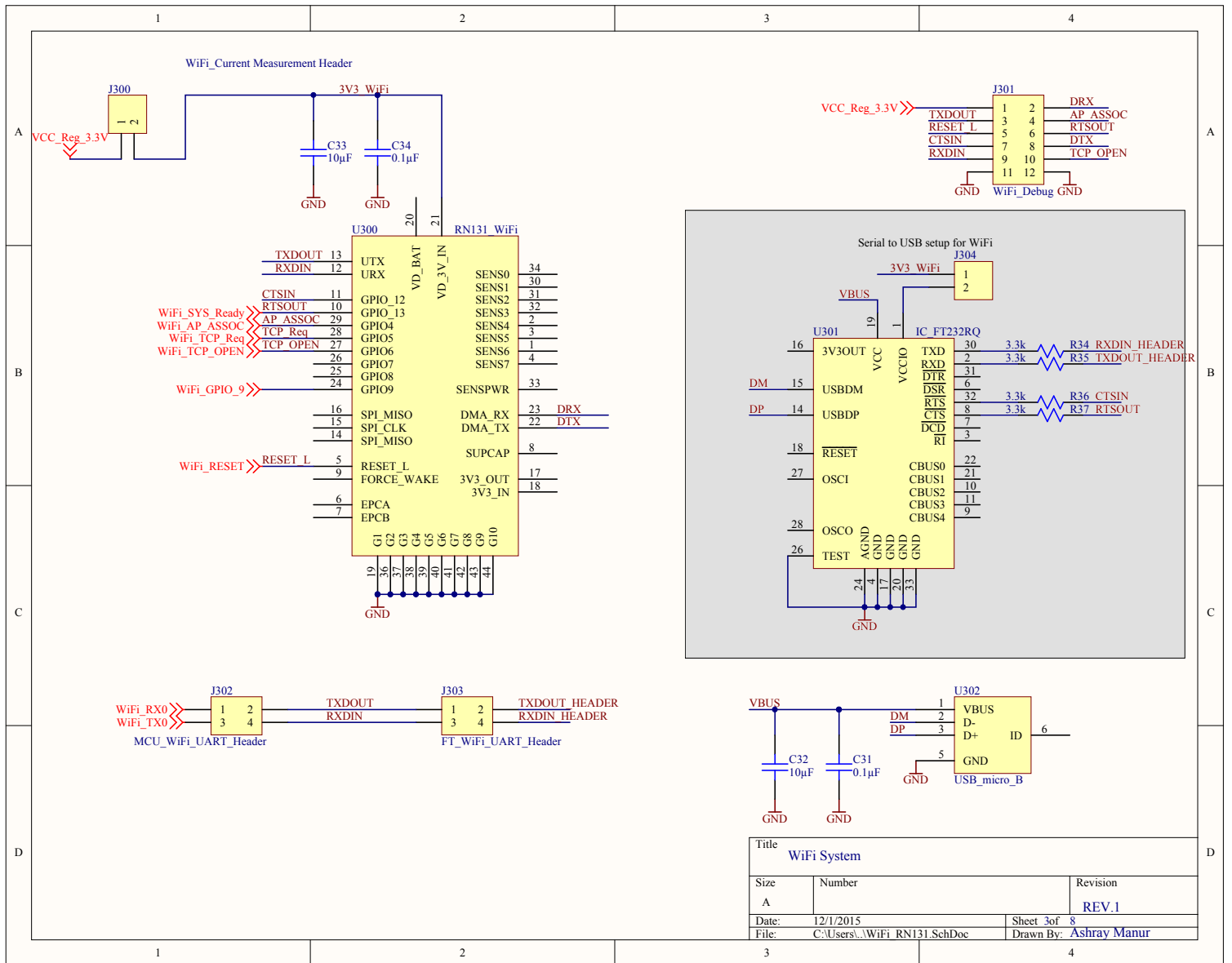
Title			MCU_ATmega256rfr2		
Size	Number	Revision			
A		REV.1			
Date:	12/1/2015	Sheet	1 of 8		
File:	C:\Users\...MEM_Sch.SchDoc	Drawn By:	Ashray Manur		



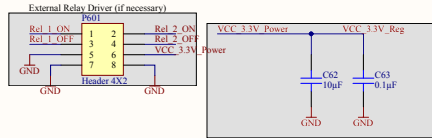
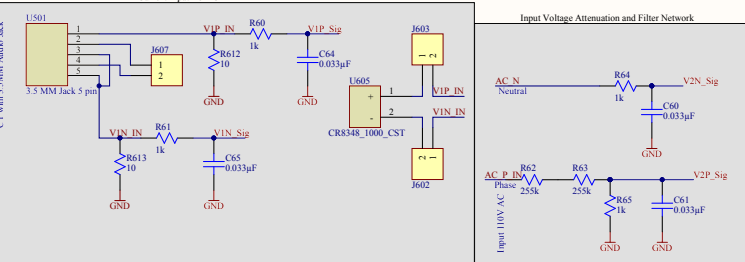
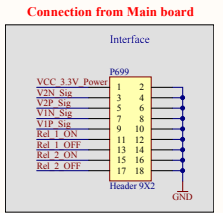
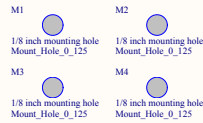
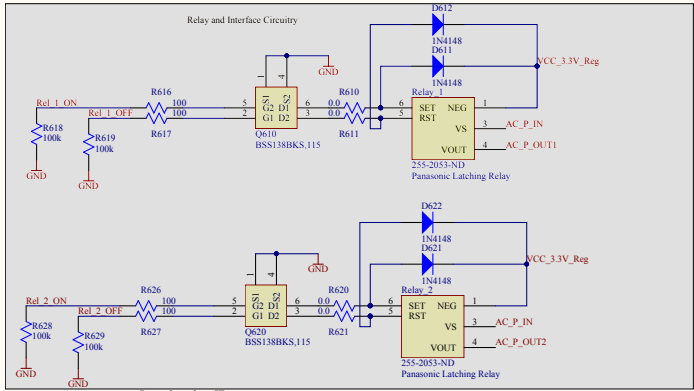
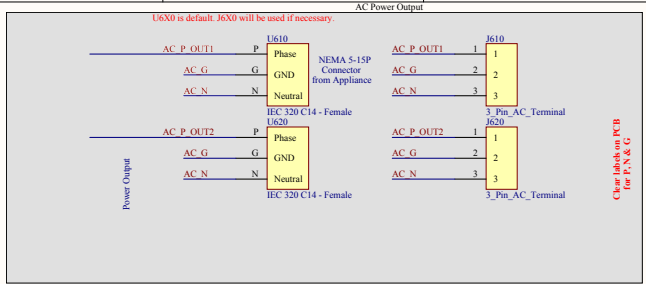
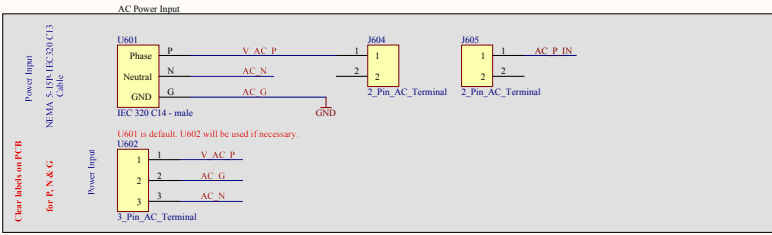
Title		
DC Power Supply		
Size	Number	Revision
A		REV.1
Date:	12/1/2015	Sheet 2of 8
File:	C:\Users\...\power supply.SchDoc	Drawn By: Ashray Manur



Title			RTC_DS1337 and microSD		
Size	Number		Revision		
A			REV.1		
Date:	12/1/2015	Sheet 4 of 8			
File:	C:\Users\...RTC.SchDoc	Drawn By:	Ashray Manur		



Title		
WiFi System		
Size	Number	Revision
A		REV.1
Date:	12/1/2015	Sheet 3 of 8
File:	C:\Users\...WiFi RN131.SchDoc	Drawn By: Ashray Manur



THIS IS A SEPARATE BOARD

Power Interface Board
REV.1
Ashray Manur

Title		
Size B	Number	Revision
Date: 12/10/2015	Sheet of	Drawn By:
File: C:\Users\...Interface SchDoc	6	6

Bibliography

- [1] C. Marnay and G. Venkataramanan, "Microgrids in the evolving electricity generation and delivery infrastructure," in *Power Engineering Society General Meeting, 2006. IEEE*, 2006, pp. 5 pp.–.
- [2] B. Kuri and F. Li, "Valuing emissions from electricity towards a low carbon economy," in *Power Engineering Society General Meeting, 2005. IEEE*, June 2005, pp. 53–59 Vol. 1.
- [3] R. H. Lasseter, "Microgrids," in *Power Engineering Society Winter Meeting, 2002. IEEE*, vol. 1. IEEE, 2002, pp. 305–308.
- [4] F. Katiraei, M. Iravani, and P. Lehn, "Micro-grid autonomous operation during and subsequent to islanding process," *Power Delivery, IEEE Transactions on*, vol. 20, no. 1, pp. 248–257, Jan 2005.
- [5] S. V. Iyer, M. N. Belur, and M. C. Chandorkar, "A generalized computational method to determine stability of a multi-inverter microgrid," *Power Electronics, IEEE Transactions on*, vol. 25, no. 9, pp. 2420–2432, 2010.
- [6] D. E. Olivares, A. Mehrizi-Sani, A. H. Etemadi, C. Canizares, R. Iravani, M. Kazerani, A. H. Hajimiragha, O. Gomis-Bellmunt, M. Saeedifard, R. Palma-Behnke *et al.*, "Trends in microgrid control," *Smart Grid, IEEE Transactions on*, vol. 5, no. 4, pp. 1905–1919, 2014.
- [7] X. Yu, A. M. Khambadkone, H. Wang, and S. T. S. Terence, "Control of parallel-connected power converters for low-voltage microgrid—part i: A hybrid control architecture," *Power Electronics, IEEE Transactions on*, vol. 25, no. 12, pp. 2962–2970, 2010.
- [8] J. Kim, J. Guerrero, P. Rodriguez, R. Teodorescu, and K. Nam, "Mode adaptive droop control with virtual output impedances for an inverter-based flexible ac microgrid," *Power Electronics, IEEE Transactions on*, vol. 26, no. 3, pp. 689–701, March 2011.
- [9] M. B. Delghavi and A. Yazdani, "An adaptive feedforward compensation for stability enhancement in droop-controlled inverter-based microgrids," *Power Delivery, IEEE Transactions on*, vol. 26, no. 3, pp. 1764–1773, 2011.
- [10] A. Hajimiragha and M. Zadeh, "Research and development of a microgrid control and monitoring system for the remote community of bella coola: Challenges, solutions, achievements and lessons learned," in *Smart Energy Grid Engineering (SEGE), 2013 IEEE International Conference on*, Aug 2013, pp. 1–6.
- [11] F. Ktiraei, R. Iravani, N. Hatziargyriou, and A. Dimeas, "Microgrids management-controls and operation aspects of microgrids," *IEEE Power Energy*, vol. 6, no. 3, pp. 54–65, 2008.

- [12] L. Siow, P. So, H. Gooi, F. Luo, C. Gajanayake, and Q. Vo, "Wi-fi based server in microgrid energy management system," in *TENCON 2009 - 2009 IEEE Region 10 Conference*, Jan 2009, pp. 1–5.
- [13] R. Mao, H. Li, Y. Xu, and H. Li, "Wireless communication for controlling microgrids: Co-simulation and performance evaluation," in *Power and Energy Society General Meeting (PES), 2013 IEEE*, July 2013, pp. 1–5.
- [14] L. Li, H. Xiaoguang, C. Ke, and H. Ketai, "The applications of wifi-based wireless sensor network in internet of things and smart grid," in *Industrial Electronics and Applications (ICIEA), 2011 6th IEEE Conference on*, June 2011, pp. 789–793.
- [15] V. Gungor, B. Lu, and G. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *Industrial Electronics, IEEE Transactions on*, vol. 57, no. 10, pp. 3557–3564, Oct 2010.
- [16] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *Industrial Electronics, IEEE Transactions on*, vol. 56, no. 10, pp. 4258–4265, 2009.
- [17] D. Son, B. Krishnamachari, and J. Heidemann, "Experimental study of concurrent transmission in wireless sensor networks," in *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems*, ser. SenSys '06. New York, NY, USA: ACM, 2006, pp. 237–250. [Online]. Available: <http://doi.acm.org/10.1145/1182807.1182831>
- [18] J. Zhao and R. Govindan, "Understanding packet delivery performance in dense wireless sensor networks," in *Proceedings of the 1st international conference on Embedded networked sensor systems*. ACM, 2003, pp. 1–13.
- [19] G. Zhou, T. He, J. Stankovic, T. Abdelzaher *et al.*, "Rid: radio interference detection in wireless sensor networks," in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, vol. 2. IEEE, 2005, pp. 891–901.
- [20] M. Erol-Kantarci and H. T. Mouftah, "Wireless sensor networks for cost-efficient residential energy management in the smart grid," *Smart Grid, IEEE Transactions on*, vol. 2, no. 2, pp. 314–325, 2011.
- [21] Y. Yang, F. Lambert, and D. Divan, "A survey on technologies for implementing sensor networks for power delivery systems," in *Power Engineering Society General Meeting, 2007. IEEE*, June 2007, pp. 1–8.
- [22] R. Leon, V. Vittal, and G. Manimaran, "Application of sensor network for secure electric energy infrastructure," *Power Delivery, IEEE Transactions on*, vol. 22, no. 2, pp. 1021–1028, April 2007.
- [23] M. Erol-Kantarci and H. T. Mouftah, "Wireless multimedia sensor and actor networks for the next generation power grid," *Ad Hoc Netw.*, vol. 9, no. 4, pp. 542–551, Jun. 2011. [Online]. Available: <http://dx.doi.org/10.1016/j.adhoc.2010.08.005>
- [24] J. Pan, R. Jain, and S. Paul, "A survey of energy efficiency in buildings and microgrids using networking technologies," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 3, pp. 1709–1731, 2014.

- [25] J. Pan, R. Jain, P. Biswas, W. Wang, and S. Addepalli, "A framework for smart location-based automated energy controls in a green building testbed," in *Energetech, 2012 IEEE*, May 2012, pp. 1–6.
- [26] Y. Simmhan, S. Aman, A. Kumbhare, R. Liu, S. Stevens, Q. Zhou, and V. Prasanna, "Cloud-based software platform for data-driven smart grid management," *IEEE/AIP Computing in Science and Engineering*, 2013.
- [27] S. Bera, S. Misra, and J. J. Rodrigues, "Cloud computing applications for smart grid: A survey," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 26, no. 5, pp. 1477–1494, 2015.
- [28] H. Kim, Y.-J. Kim, K. Yang, and M. Thottan, "Cloud-based demand response for smart grid: Architecture and distributed algorithms," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*. IEEE, 2011, pp. 398–403.
- [29] L. Ji, W. Lifang, and Y. Li, "Cloud service based intelligent power monitoring and early-warning system," in *Innovative Smart Grid Technologies-Asia (ISGT Asia), 2012 IEEE*. IEEE, 2012, pp. 1–4.
- [30] C.-T. Yang, W.-S. Chen, K.-L. Huang, J.-C. Liu, W.-H. Hsu, and C.-H. Hsu, "Implementation of smart power management and service system on cloud computing," in *Ubiquitous Intelligence Computing and 9th International Conference on Autonomic Trusted Computing (UIC/ATC), 2012 9th International Conference on*, Sept 2012, pp. 924–929.
- [31] V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," *Computer Networks*, vol. 50, no. 7, pp. 877–897, 2006.
- [32] *IEEE Standard for Information Technology Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Std 802.15.4, 2006.
- [33] AVR2130: *Lightweight mesh developer guide*, Atmel Corporation, 2014. [Online]. Available: http://www.atmel.com/Images/Atmel-42028-Lightweight-Mesh-Developer-Guide_Application-Note_AVR2130.pdf,
- [34] V. Cervenka, L. Mraz, and D. Komosny, "Comprehensive performance analysis of lightweight mesh and its comparison with zigbee pro technology," *Wireless Personal Communications*, vol. 78, no. 2, pp. 1527–1538, 2014.
- [35] M. Armbrust, O. Fox, R. Griffith, A. D. Joseph, Y. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica *et al.*, "M.: Above the clouds: a berkeley view of cloud computing," 2009.
- [36] <https://nodejs.org/en/>, [Online; accessed 30-November-2015].
- [37] S. Sundaresan, W. De Donato, N. Feamster, R. Teixeira, S. Crawford, and A. Pescapè, "Broadband internet performance: a view from the gateway," in *ACM SIGCOMM computer communication review*, vol. 41, no. 4. ACM, 2011, pp. 134–145.

- [38] R. Shea, F. Wang, H. Wang, and J. Liu, "A deep investigation into network performance in virtual machine based cloud environments," in *INFOCOM, 2014 Proceedings IEEE*. IEEE, 2014, pp. 1285–1293.
- [39] S. K. Barker and P. Shenoy, "Empirical evaluation of latency-sensitive application performance in the cloud," in *Proceedings of the first annual ACM SIGMM conference on Multimedia systems*. ACM, 2010, pp. 35–46.
- [40] J. C. Mogul, R. R. Kompella, and X. HotOS, "Inferring the network latency requirements of cloud tenants," in *15th Workshop on Hot Topics in Operating Systems (HotOS XV)*. USENIX Association, 2015.
- [41] S. Narayanan and A. Sivakumar, "Monitoring latency sensitive enterprise applications on the cloud."
- [42] M. Yarvis, K. Papagiannaki, and W. S. Conner, "Characterization of 802.11 wireless networks in the home," in *1st workshop on Wireless Network Measurements (Winmee)*. Citeseer, 2005.
- [43] K. Lakshminarayanan, S. Seshan, and P. Steenkiste, "Understanding 802.11 performance in heterogeneous environments," in *Proceedings of the 2nd ACM SIGCOMM workshop on Home networks*. ACM, 2011, pp. 43–48.
- [44] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of rf interference on 802.11 networks," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 4, pp. 385–396, 2007.
- [45] A. Kamerman and N. Erkocevic, "Microwave oven interference on wireless lans operating in the 2.4 ghz ism band," in *Personal, Indoor and Mobile Radio Communications, 1997. Waves of the Year 2000. PIMRC'97., The 8th IEEE International Symposium on*, vol. 3. IEEE, 1997, pp. 1221–1227.