Energy-Efficient Device Architecture and Technologies for the Internet of Everything

by

Chinmaya Mahapatra

B.Tech., National Institute of Technology, Rourkela, India, 2009

M.A.Sc., The University of British Columbia, Vancouver, Canada, 2013

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

Doctor of Philosophy

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

(Electrical and Computer Engineering)

The University of British Columbia
(Vancouver)

December 2018

The following individuals certify that they have read, and recommend to the Faculty of Graduate and Postdoctoral Studies for acceptance, the thesis entitled:

Energy-Efficient Device Architecture and Technologies for the Internet of Everything

submitted by **Chinmaya Mahapatra** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy** in **Electrical and Computer Engineering**.

Examining Committee:

Victor CM Leung, Electrical and Computer Engineering
Supervisor

Shahriar Mirabbasi, Electrical and Computer Engineering
Supervisory Committee Member

Juri Jatskevich, Electrical and Computer Engineering
University Examiner

Bhushan Gopaluni, Chemical and Biological Engineering
University Examiner

Additional Supervisory Committee Members:

Peyman Servati, Electrical and Computer Engineering
Supervisory Committee Member

Abstract

Around the globe, integrating information and communication technologies with physical infrastructure is a top priority in pursuing smart, green living to improve energy efficiency, protect the environment, improve the quality of life, and bolster economy competitiveness. Internet-of-Everything (IoE) is a network of uniquely identifiable, accessible, and manageable smart things that are connected through a network of heterogeneous devices and people, usually consisting of battery-operated nodes, and mostly working at remote places, without human intervention. This leads us to issues concerning IoE Systems such as network lifetime, battery efficiency, carbon emissions, low-power security and efficient data transmission, which have been analysed in this thesis and solutions have been proposed for them.

First, we investigate wireless energy harvesting (WEH), wake-up radio (WUR) scheme, and error control coding (ECC) as enabling solutions to enhance the performance of sensor networks-based IoE systems while reducing their carbon footprints. Specifically, a utility-lifetime maximization problem incorporating WEH, WUR, and ECC, is formulated and solved using a distributed dual sub gradient algorithm based on the Lagrange multiplier method. Discussion and verification through simulation results show how the proposed solutions improve network utility, prolong the lifetime, and pave the way for a greener IoE by reducing their carbon footprints.

Next, we introduce active radio frequency identification tags based cluster head selection, data-awareness and energy harvesting in IoE systems. The results show that such IoE systems are better equipped to deal with energy efficiency and data delivery problems. Simulation results support our data aware energy saving approach and show significant improvement over state-of-the art techniques. To design an energy-efficient and low-resource consuming security solution for IoE systems, we propose a Physically Unclonable Function based security scheme that exploits variations of physical sensor characteristics through a prototype printed circuit board design and challenge-response pair generation using the quadratic residue property. Through simulations and measurements, we show that our design scheme is better in terms of energy and computation requirements and provides a two-fold secure data transfer. Finally, we apply our solutions to a home energy management system and find an optimal model to save energy in a broad IoE system application.

Lay Summary

It is projected that there will be more than 50 billion smart objects connected to the Internet of Everything (IoE) within the coming decade. These smart objects connect the physical world with the world of computing and people are expected to revolutionalize all aspects of our daily lives and transform a number of application domains such as healthcare and transportation, etc. In this thesis, we present an overview of the challenges involved in designing and implementing energy-efficient IoE devices and propose promising solutions to address these challenges. Our solution takes a holistic system design approach considering all the critical elements of the system architecture, by implementing lightweight networking layer on sensor devices, which has energy-efficient cross-layer data driven architecture, power-efficient security and error resilient schemes. Most of the data will be stored and fetched through the cloud, thus concentrating on enhancing the system's performance and saving energy.

Preface

I am the primary researcher and author for all the research contributions made in this thesis. I conducted the literature review to identify the research problems. I formulated the research problems, gathered data, performed mathematical analysis and experiments, and carried out the numerical simulations, lab and field measurements. I also wrote the manuscripts for each publication.

The contributions of the co-authors of my papers are as follows. Prof. Victor C.M. Leung is my supervisor. He has provided valuable guidance, technical suggestions, and constructive feedback for identifying the research problem, making the research progress, and preparing the associated manuscripts. Prof. Shahriar Mirabbasi, Prof. Thanos Stouraitis, Prof. Y.L. Guan and Prof. Zhenguo Sheng helped me in my research during my PhD. Prof. Shahriar Mirabbasi is a committee member of my PhD supervisory committee whereas Prof. Thanos Stouraitis and Prof. Zhenguo Sheng are research collaborators in my supervisor's Natural Sciences and Engineering Research Council (NSERC) projects related to my research. I have consulted them during all my research works and they have provided valuable guidance, constructive technical feedback, and also helped in editorial corrections while preparing the corresponding manuscripts for publication. Prof. Y.L. Guan suggested improvements to improve technical contents in my chapter 2.

Dr. Pouya Kamalinejad was a former post-doctoral fellow in my lab. His PhD work on wireless energy harvesting integrated circuit design helped me formulate and test my model for energy harvesting and network lifetime. Peter Woo is a System Validation Design Engineer at Microsemi Corporation, Vancouver, Canada. He was the one who helped me fabricate my circuit board for my energy-efficient PUF security circuit in Chapter 4. Dr. Roberto Rosales is a test lab manager at the University of British Columbia(UBC), he helped me with my lab setup and PUF prototype circuit measurements. Dr. Akshaya Moharana is an engineer at PowerTech Labs, BC, Canada. He helped me with the data for power consumption of British Columbia's residents for the last 15 years, which aided my research in Chapter 5.

Publications that resulted from the research presented in this thesis are as follows:

[1] C. Mahapatra, Z. Sheng, V. C.M. Leung, and T. Stouraitis, "A reliable and energy efficient iot data transmission scheme for smart cities based on redundant residue based error correction coding," in *Sensing, Communication, and Networking - Workshops (SECON Workshops), 2015 12th Annual IEEE International Conference on*, June 2015, pp. 1–6. (Linked to Chapter 2)

[2] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C.M. Leung, and Y. L. Guan, "Wireless energy harvesting for the internet of things," *Communications Magazine, IEEE*, vol. 53, no. 6, pp. 102–108, June 2015. (Linked to Chapter 2 and Chapter 3)

[3] C. Mahapatra, Z. Sheng, P. Kamalinejad, V. C.M. Leung, and S. Mirabbasi, "Optimal power control in green wireless sensor networks with wireless energy harvesting, wake-up radio and transmission control," *IEEE Access*, vol. 5, pp. 501–518, 2017. (Linked to Chapter 2)

[4] C. Mahapatra, Z. Sheng, and V. C.M. Leung, “Energy-efficient and distributed data-aware clustering protocol for the internet-of-things,” in *Electrical and Computer Engineering (CCECE), 2016 IEEE Canadian Conference on*. IEEE, 2016, pp. 1–5. (Linked to Chapter 3)

[5] C. Mahapatra, P. Kamalinejad, T. Stouraitis, S. Mirabbasi, and V. C.M. Leung, “Low-complexity energy-efficient security approach for e-health applications based on physically unclonable functions of sensors,” in *2015 IEEE International Conference on Electronics, Circuits, and Systems (ICECS)*, Dec 2015, pp. 531–534. (Linked to Chapter 4)

[6] C. Mahapatra, S. P. Woo, R. Rosales, T. Stouraitis, V. C.M. Leung, and S. Mirabbasi, “Energy-efficient, puf-based security design for Internet-of-Things (iot) infrastructure,”, in IEEE Internet-of-Things Journal, 2^{nd} revision 2018. (Linked to Chapter 4)

[7] C. Mahapatra, A. K. Moharana, and V. C.M. Leung, “Energy management in smart cities based on internet of things: Peak demand reduction and energy savings,” *Sensors*, vol. 17, no. 12, p. 2812, 2017. (Linked to Chapter 5)

Table of Contents

List of Tables

List of Figures

List of Abbreviations

µp	Microprocessor
ACK	Acknowledgement
ADC	Analog-To-Digital Converter
ARQ	Automatic Repeat Request
BCH	Bose-Chaudhuri-Hocquenghem
BRL	Batch Reinforcement Learning
BS	Base Station
CCM	Community Cloud Management Panel
CH	Cluster Head
CIPK	Carbon Intensity Per KWh
COAP	Constrained Application Protocol
CRC	Cyclic Redundancy Check
DAC	Digital-To-Analog Converter

DAEECI	Data Aware Energy Efficient Clustering Protocol For IoT
DC	Direct Current
DEEC	Distributed Energy Efficient Clustering
DoS	Denial Of Service
DR	Demand Response
DyR	Dynamic Range
DSM	Demand Side Management
ECC	Error Correction Coding
EDEEC	Enhanced Distributed Energy Efficient Clustering
EH	Energy Harvesting
FIPS	Federal Information Processing Standards
GWSN	Green Wireless Sensor Network
HEED	Hybrid Energy-Efficient Distributed Clustering
HEMaaS	Home Energy Management As A Service
HMAC	Hash Message Authentication Code
IBSG	Internet Business Solutions Group
IC	Integrated Circuit
ICT	Information And Communication Technology

IETF	Internet Engineering Task Force
IoE	Internet Of Everything
IoT	Internet Of Things
KNN	K-Nearest Neighbor
KRLE	Krun-Length Encoding
LEACH	Low-Energy Adaptive Clustering Hierarchy
LTE	Long Term Evolution
LUT	Look-Up-Table
M2M	Machine-To-Machine
MCCU	Main Command And Control Unit
MDP	Markov Decision Process
MQTT	Message Queue Telemetry Transport
MRC	Mixed Radix Conversion
MWh	Mega-Watt-hour
NAT	Network Address Translation
NFQI	Neural Fitted Q-Iteration
OOK	On-Off Keying
P2M	Person-To-Machine

P2P	Person-To-Person
PCB	Printed Circuit Board
PCE	Power Conversion Efficiency
PEGASIS	Power Efficient Gathering In Sensor Information Systems
PMU	Power Management Unit
PUF	Physically Unclonable Function
QoS	Quality Of Service
QR	Quadratic Residue
RAS	Resume All Services
RBF	Radial Basis Functions
RBFNN	Radial Basis Function Neural Network
RF	Radio-Frequency
RFID	Radio Frequency Identification
RL	Reinforcement Learning
RNS	Residue Number System
RPL	Routing Protocol For Low Power And Lossy Networks
RRNS	Redundant Residue Number System
RSA	Rivest-Shamir-Adleman

SAS	Stop All Service
SHA-1	Secure Hash Algorithm 1
SoC	Sensors On Chip
TIA	Trans-Impedance Amplifier
TOU	Time-Of-Use
UC	Convenience
UI	User Interface
UIP	User Input Preferences
WEH	Wireless Energy Harvesting
WSN	Wireless Sensor Network
WU	Wake-Up Command
WUR	Wake Up Radio

Acknowledgments

Firstly, I would like to express my sincere gratitude to my advisor Prof. Victor Leung for the continuous support during the course my Ph.D. His knowledge, work ethic and perseverance are truly inspiring and his guidance has helped me in every stage of my research and in the writing of this thesis. I could not have imagined having a better advisor and mentor for my Ph.D work.

I would like to express my regards to Prof. Shahriar Mirabbasi, Prof. Thanos Stouraitis and Dr. Zhenguo Sheng for helping me with their immense technical knowledge and experience on specific subject matter related to my PhD. reasearch and thesis. I would also like to thank Dr. Roberto Rosales, Dr. Pouya Kamalinejad and Peter Woo for help with my lab measurements, PUF prototype circuit design and journal writing. I an very grateful to Dr. Akshaya Moharana for helping me with power-demand data for British Columbia homes. I thank my labmates for their insightful discussions and all my friends for their encouragement. I would like to thank my family: my parents and my wife, who have been the biggest support pillars of my life.

I am very grateful to Natural Sciences and Engineering Research Council of Canada (NSERC) and University of British Columbia for their support for my doctoral work through Canada Graduate Scholarships-Doctoral (CGS D) scholarship and Four-year fellowship (FYF) scholarship respectively.

Dedication

To my parents and my wife.

Chapter 1

Introduction

The Internet-of-Things (IoT) started in 2009 with a vision of connecting devices to devices and persons to devices. Technologies like Radio Frequency Identification (RFID) and wireless sensor networks (WSNs) form the backbone of such interactions. The industrial sector estimates that by 2020 more than half billion devices will be connected with each other [1–3]. When virtually every device is connected with each other and all manual commands are replaced by intelligent machines and automation, the system will be enormous and complex spanning across a varied range of protocols and standards. IoT aims to make the Internet ubiquitous and pervasive, and has the potential to affect many aspects of users' quality of life. To monitor their environment and send/receive data, the networked heterogeneous devices connected in an IoT structure are typically equipped with sensors, controlling processors, wireless transceivers, and an energy source (e.g., a battery) . Applications envisioned for IoT span a wide range of fields including home automation, healthcare, surveillance, transportation, smart environments, and many more [4, 5].

The Internet of Everything (IoE) as a concept first came out from the CISCO Inter-

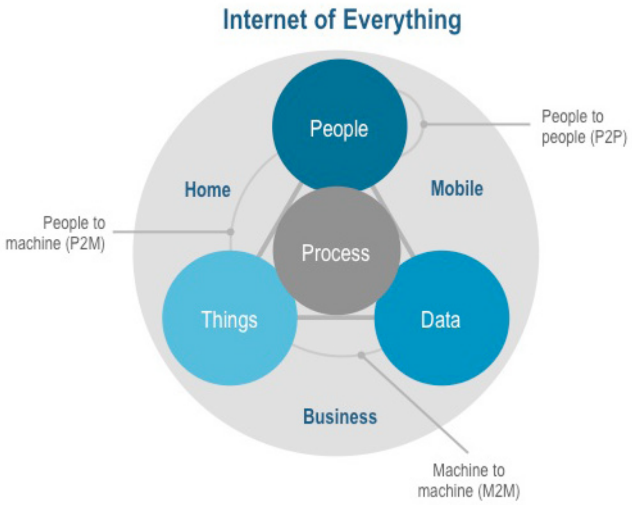


Figure 1.1: Interconnections in components of Internet-of-Everything.[1] ©CISCO-IBSG

net Business Solutions Group (IBSG) [1]. It is an extension of IoT that encompasses people, data, things and processes to give a meaningful, energy-efficient, intelligent, relevant and secure insight to connections between the layers interconnected together in an agile and iterative flow. Its technologies, including heterogeneous WSNs, are used to monitor many aspects of an ecosystem ranging from a small office space to a city, in real time. In this thesis, we will be using the terms IoE and IoT interchangeably. Fig. 1.1 shows the flow process of IoE and a brief summary of the individual components of its ecosystem is as given below.

People: People are an integral part of any IoE ecosystem as they are the ones who generate the enormous amount data through the usage of devices. Nowadays, connectivity to the world of Internet can be established through numerous devices including personal computers, smartphones, tablets, wearables and many more. Apart from the traditional ways, there are other paths of connectivity with the world through social networking sites such as Facebook and Twitter, entertainment on demand hubs like Youtube, Netflix and Amazon Prime. As the Internet evolves toward IoE, we will be connected in more relevant and valuable ways. This way people themselves are the most important nodes of this ecosystem for whom the IoE exists and the research is geared towards providing smooth technological flow for them.

Data: The widespread proliferation of internet-connected devices as described above used by people in the era of IoE coupled with increasing fidelity and data acquisition modality generates 2.5 quintillion bytes of data each day [6]. As the devices used to generate data become more intelligent, these vast amounts of data will produce deeper insights into managing the relevant data for the people.

Things: These are physical devices including smart sensors, connected objects, consumer devices and many more. In IoE, these things will sense more data, become context-aware, and provide more experiential information to help people and machines make more relevant and valuable decisions.

Process: Processes are the ways in which the people, data and things work with each other to provide meaningful insights for the overall structure of the IoE. Following the right process will make sure that the right information is delivered to the right person at the right time in an appropriate way.

In the next section we describe the layered architecture of an IoE system, its open issues and possible solutions.

1.1 Elements of an Internet of Everything System

With the rapid development of big data and IoE, the number of networking devices and data volume are increasing dramatically. Since portable and battery operated systems like smartphones, tablets, and cameras will always be connected, enormous amounts of user data will be generated and their energy consumption will dramatically increase.

One of the important challenges is supplying adequate energy to operate the network in a self-sufficient manner without compromising quality of service (QoS). In order to tackle these challenges, the Internet Engineering Task Force (IETF) has taken the lead in standardizing protocols for resource constrained devices such as Routing Protocol for Low Power and Lossy Networks (RPL) and Constrained Application Protocol (CoAP) [3]. But, to develop them in a large scale, a considerable insight and development is required. IEEE P2413 [7], the standard for an architectural framework for the IoT, aims to provide an architecture framework which captures the commonalities across different domains and provides a basis for instantiation of concrete IoT architectures.

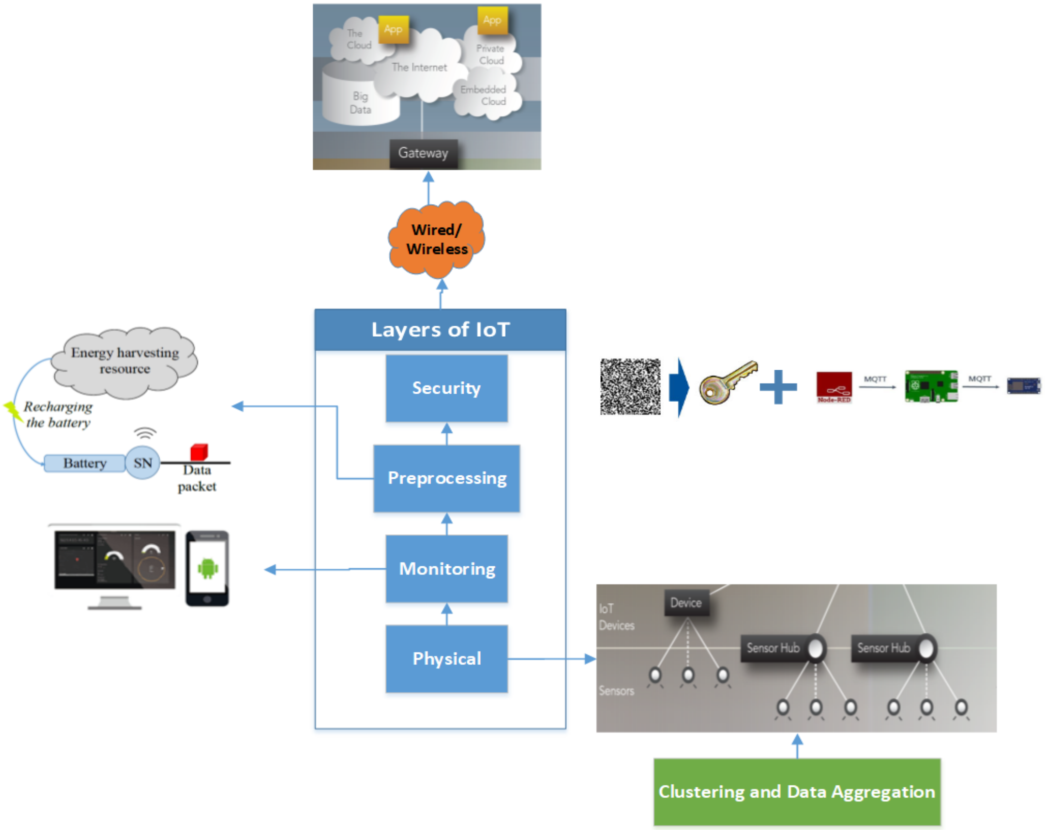


Figure 1.2: Layered IoT architecture.

Fig. 1.2 shows a layered architecture of a resource-constrained IoT system. The layers of the IoT system represent different processes through which data pass before being sent to cloud servers via the wireless/wired media [8, 9]. The layers of IoT represent the different stages of processing the data coming from the interconnected system as described in Fig. 1.1.

Physical layer

The physical layer consists of end-devices of the IoT system such as sensors, smartphones, smart devices. These are energy-constrainted, small in size and have limited hardware capability. Enormous amount of data is generated from these devices. As more and more devices are connected to the Internet, data generation has reached the order of thousands of exabytes. These devices consist of a limited energy source (e.g., a battery) to monitor their environment and send/receive data.

Monitoring and Preprocessing

Monitoring and pre-processing are essential parts of energy-efficient data management. Monitoring of user data is important from the point of view of data management as well as network security. Routing and clustering of data from the lower layer to the upper layer also needs constant monitoring of data, which consumes energy and needs network resources. Hence, preprocessing of data is important to extract the relevant data for transmission, thereby reducing the transmission delay of the network.

Security

As we gradually move toward using some of the smart devices for critical operations, security will become a primary driver. Due to the IoT devices carrying critical data in many applications and being in an unsecured environment security is paramount for IoT devices. This is achieved in this layer and it applies to both the wired as well as wireless networks.

Gateway Layer

The gateway architecture is designed in a way to support many operating systems and several versions of other similar operating system types. Gateways connect the network of the end-devices and core networks to the cloud servers. When the end nodes generate resource requirements for IoT applications, they will send the data processing or storage tasks to the cloud servers.

1.2 Open Issues in IoE Systems

Several open issues in the layered architecture are related to limited battery capacity of the devices, their network lifetime, secure data transfer in limited energy devices and energy-efficient data management. Since energy efficiency is of utmost importance to the battery constrained IoT devices, IoT-related standards and research works have focused on the device energy conserving issues [10–12]. Although the size of end physical nodes is falling fast, the energy-storage devices are improving in a slower pace as shown in Fig. 1.3, leading to a reducing amount of available energy in smaller nodes. Including a battery means increased deployment cost and more importantly maintenance cost (to change the battery periodically). Since the node's lifetime is generally significantly higher than the battery-lifetime, it is desirable to develop energy sensor nodes with increased node lifetime, that perpetually run on harvested energy, is data-aware and uses energy resources intelligently. The goal of IoT systems is to pack more and more functionality for energy-constrained nodes in a wireless environment. This leads to an energy-gap and calls for significant improvements in energy-efficiency for computing and communication in energy-constrained nodes [10, 11].

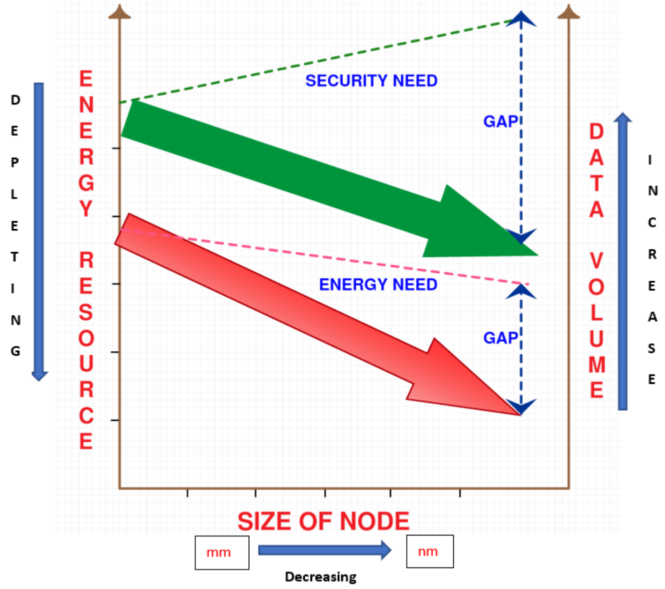


Figure 1.3: Energy gap generated with decreasing size of IoT nodes with reduced energy availability and increased security vulnerabilities as well as increased data generation.

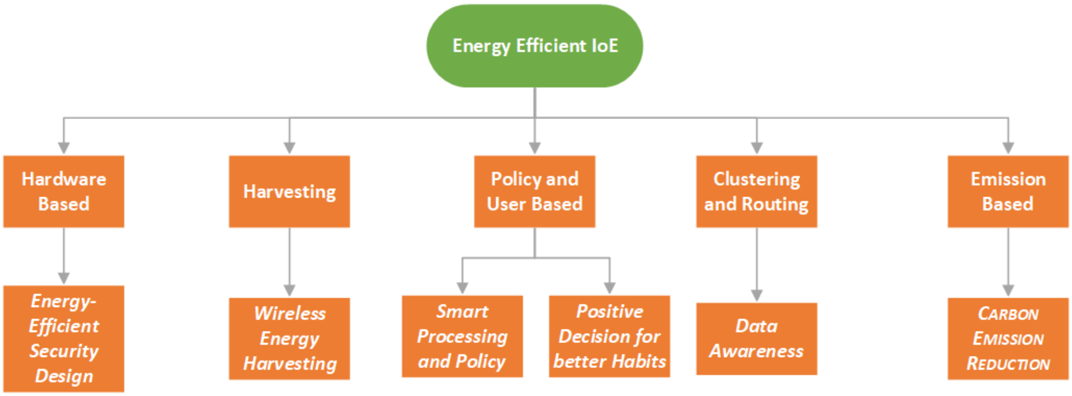

Energy Efficient IoE
Hardware Based
Harvesting
Policy and User Based
Clustering and Routing
Emission Based
Energy-Efficient Security Design
Wireless Energy Harvesting
Smart Processing and Policy
Positive Decision for better Habits
Data Awareness
Carbon Emission Reduction

Figure 1.4: Energy efficiency models on the basis of their technologies used.

In Fig. 1.4, we categorize the energy efficiency models on the basis of the technologies used in them. Building an energy-efficient architecture for IoE systems is a gigantic task and is not limited to only areas defined in Fig. 1.4. However, in this thesis we have analyzed and proposed solutions for the blocks and scopes of the IoE system that can lead to a significant energy improvement. The specific issues considered are divided into hardware-related, harvested energy related, policy and user based, data awareness and carbon emission reduction based. Below, these open issues in the context of energy efficiency in IoE systems are reviewed.

1.2.1 Hardware-Based Issues in IoE

Design of integrated circuit (IC) in an IoE network is vital in conserving energy. A concept of energy-efficient sensors on chip (SoC) [13, 14] improves the design of IoE networks by combining sensors, processing power on a single chip to reduce the data traffic, increase security, reduction in carbon footprint as well as the energy consumption of the overall infrastructure. Energy-sparse, size-constrained end nodes have limited resources to guarantee strong security and hence are often considered as the weakest link in an end-to-end system. While the resource available for security is reducing (Fig. 1.3) with reducing size, the security requirements of these leaf nodes are increasing, creating a strong need for research in lightweight, resource-constrained security technologies [15, 16]. Embedded hardware security techniques could be a potential solution to preserve the highest level of security within this infrastructure.

1.2.2 Issues Related to Wireless Energy Harvesting

The large scale growth in the number of wirelessly connected devices however come at the cost of a critical challenge in large scale implementation of WSNs technology and in a greater scope, IoE, in providing energy to the nodes. In most applications, wireless nodes which solely rely on an energy storage device (e.g., battery) need to be deployed in very large numbers and in hard-to-reach locations. Maintaining such a network through replacing the batteries is a cumbersome process and is uneconomical especially when a long life-time is desired. Energy harvesting is a promising remedy to cope with the energy challenge. A wireless node can harvest energy from different forms of environmental sources such as thermal, wind, solar, vibration [17]. Among these resources, wireless energy harvesting is an attractive candidate and provides key advantages in virtue of being controllable and having lower cost and smaller form factor implementations [18, 19]. Incorporation of energy harvesting is a promising remedy to cope with the energy challenge. Energy harvesting enables easier deployment of nodes in remote areas aiding in virtually maintenance-free operation and significant reduction in the carbon footprint associated with manufacturing and replacing batteries. Scavenging energy form the aforementioned environmental sources is an opportunistic process, i.e., it highly relies on the presence of the source and environmental conditions. In the context of our system, the wireless energy sources fall into two categories of *dedicated sources* and *Ambient sources* [18]. A dedicated RF source is deliberately deployed to supply energy to the nodes at a designated rate and optimum frequency (e.g., sink node). An ambient source, on the other hand, is a less predictable energy source happens to exist within the operation area of the network, but are not designed as a part of the network. Examples of ambient sources include TV and radio towers (static ambient source) and WiFi access points (dynamic ambient source). Due to their unpredictable nature, harvesting energy from ambient sources is an opportunistic process which requires some level of adaptivity and entails a more sophisticated design both at circuit and system levels.

1.2.3 Poilcy Based Issues

Policies and techniques based on real time usage data in IoE systems can help reduce the energy consumption significantly [20]. Monitoring, preprocessing, making intelligent decisions based on user feedback and behaviour can play an important role in making these policies for energy-efficiency a success. The biggest challenge in managing such an ecosystem also known as a smart IoE based environment is to make efficient and informed decisions from user data, behaviour and feedback. This task is not easy to implement in a big ecosystem interconnect such as cities, homes, industries. Automation alone would not be enough and require the models for user feedback and analysing behavioural patterns [21, 22]. This can save the energy in the range of 3-6%. Management of smart systems with optimized policy for saving energy often requires analyzing IoT data to optimize efficiency, comfort, safety, and to make decisions faster and in a more precise manner.

1.2.4 Data Related Issues

Data collected from different sources in IoE systems have a huge amount of information. Processing these vast amounts of data for analysis can be resource intensive and time consuming and hence, a large amount of energy is required. A challenging task for IoE systems is the low power data acquisition of sensed data. The main challenge is due to the fact that different query-driven user command generate varied sized data. Some of them are sparse in nature, some have higher rates and some are periodic. There have been several lossy compression algorithms devised specifically for resource constrained wireless motes (sensor nodes). These algorithms include: Krun-length encoding (KRLE) [23], lightweight temporal compression (LTC) [24], wavelet quantization thresholding and RLE (WQTR) [25], and compressive sampling (CS) [26], [27]. Since the radio on a wireless device consumes orders of magnitude more power than other components (e.g., ADC, CPU) [28], streaming all the data may consume too much power to be viable. As such, using data-awareness i.e dividing the data demand between critical and non-critical data, to reduce radio transmissions will help increase system longevity, decrease overall system power requirements, and decrease system costs. Not only their size but their behavior also varies. Some are random in nature with no correlation to the previous datasets while others are heavily correlated versions of their previous time samples. Several solutions like K-nearest neighbor (KNN) and Radial basis functions (RBF) have been investigated to predict the behavior of data [29]. But the data variability and different service quality requirements of IoE systems are not taken into consideration yet. Thus their is a need to analyze, investigate and develop models to utilize the data efficiently in low power motes.

1.2.5 CO_2 Emissions in IoE Systems

Today, 15 billion interactive devices are exchanging information about many aspects of our lives, and the IoT is bound to become even more ingrained in our world as 200 billion devices are expected to be actively used by 2030 [30]. If the growth of sensors and IoT-enabling technology continues at today's pace, 30% of the information and communication technology (ICT) market will be made up of IoT, data, and devices in 2030. The internet releases around 300m tonnes of CO_2 a year – as much as all the coal, oil and gas burned in Turkey or Poland, or more than half of the fossil fuels burned in the UK. Enourmous amount of data generation in IoT systems, use of multiple batteries, electricity accounts for around 40% of the total ICT energy demand and 0.8% of global CO2 emissions [30]. With ever increasing IoE devices, CO_2 emissions are bound to increase. Hence, a challenging task is to efficiently handle the factors affecting the carbon-footprint increase to save on carbon emissions, thereby making the enviroment green.

1.3 Related Works

Here, the prior works regarding the open issues related to energy efficiency as described in the Section 1.2 are reviewed. The shortcomings in the existing literature are highlighted to provide the motivations and objectives of our research.

1.3.1 Prior Work on Optimal Energy Control in Wireless Sensor Networks Based IoE Systems

In this section, we discuss the existing works in the literature concerning the problems and solutions related to the increase in a WSN system lifetime. WSN system forms the backbone of an IoE system. Energy efficiency with traffic dynamics have been an active area of research in the WSN community since last two decades. Hence we focus on developing a complete energy efficient framework for WSN based IoE systems through the existing work.

Optimization methods have been extensively used in previous research works to solve for network lifetime of wireless sensor networks. Network lifetime maximization with flow rate constraint have been studied in many prior works. Kelly *et al.* was the first to propose two classes of distributed rate control algorithms for communication networks [31]. Madan *et al.* [32] solved the lifetime maximization problem with a distributed algorithm using the subgradient method. In [33], Ehsan *et al.* propose an energy and cross-layer aware routing schemes for multichannel access WSNs that account for radio, MAC contention, and network constraints, to maximize the network lifetime. But, the problems formulated and solved in all these approaches neither does take into account a proper energy model incorporating all the transceiver resources nor it involves the application performance trade-off due to increase in lifetime by decreasing rate flows.

System utility and network lifetime are problems that are related to each other in a reciprocal relationship meaning maximizing one will degrade the other. Chen *et al*. [34] analyzed the utility-lifetime trade-off in wireless sensor network for flow constraints. He *et al*. [35] followed a cross-layer design approach. Both of these papers take transmission rate as the sole indicator of the system throughput, which is not true as the reliability plays a vital role in determining the system performance. Reliability in the system can be improved by introducing error control schemes into the sensor nodes with multipath routing introduced by lun *et al*. [36]. In [37], Yu *et al*. analyses the automatic repeat request (ARQ) as well as a hybrid ARQ scheme for WSNs. The ARQ scheme requires re-transmission if there is a failure of packet delivery which increases energy consumption of node. Xu *et al*. [38] describes a rate-reliability and lifetime trade-off for WSNs by taking theoritical end to end error probability of packets. Similarly, Zou *et al*. [39] has taken a joint lifetime-utility-rate-reliability approach for WSNs taking a generic error coding processing power model. Both [38] and [39] lack the inclusion and analysis of an error control scheme with their encoding/decoding powers as well as the delay performance of the overall system with error correction employed.

Energy harvesting is proposed as a possible method to improve the network lifetime and rechargeable batteries in WSNs by He *et al*. [40] ,Magno *et al*. [41] ,Deng *et al*. [42] and Kamalinejad *et al*. [43]. Practically, energy can be harvested from the environmental sources, namely, thermal, solar, vibration, and wireless radio-frequency (RF) energy sources [17]. While harvesting from the aforementioned environmental sources is dependent on the presence of the corresponding energy source, RF energy harvesting provides key benefits in terms of being wireless, readily available in the form of transmitted energy (TV/radio broadcasters, mobile base stations and handheld radios), low cost, and small form factor implementation. Recently, dynamics of traffic and energy replenishment incorporated in the network power model has been an active research topic. Some of the challenges are addressed by [44], [45] and [46]. They assume battery energy to be zero at start, which may not be practical for many application scenarios that has sensors with rechargeable batteries. challenges caused by packet loss due to interference has also not been addressed.

Green networking of late in the past four to five years has attracted a lot of attention. Koutitas *et al*. [47] has analyzed a maximization problem based on carbon footprints generated in terrestrial broadcasting networks. In [48] Naeem *et al*. have maximized the data rate while minimizing the CO_2 emissions in cognitive sensor networks. But it is yet to be seen how much carbon emissions can be minimized while maximizing the utility and lifetime with reliability and energy harvesting constraints.

1.3.2 Prior Work on Energy-efficient and Distributed Data-Aware Routing and Clustering Protocol

As explained in the beginning of this Chapter, IoE plays an important role by bringing together people, process, data, and things to make networked connections more relevant and valuable. Its technologies, including heterogeneous WSNs, are used to monitor many aspects of an ecosystem ranging from a small office space to a city, in real time. Routing is one of the critical technologies in IoE as opposed to traditional ad-hoc WSNs. It is more challenging due to constrained resources in terms of energy supply, processing capability, frequent topology changes and reliable data delivery within a limited time period. Based on network structure, routing protocols can be sub-divided into two categories, flat routing and hierarchical routing. In a flat topology, all nodes perform the same tasks and have the same functionalities in the network. Whereas, in a hierarchical topology, nodes perform different tasks and are typically organized into lots of clusters according to specific metrics. In clustering, members of the clusters elect a cluster head (CH) [49]. All nodes belonging to the same cluster send their data to CH, where, CH aggregates data and sends aggregated data to base station (BS).

Clustering algorithms in the literature are divided based on their energy efficiency in two types of networks i.e., homogeneous and heterogeneous WSNs. Homogeneous WSNs considers that the all sensor nodes in the system have the same energy level and all the nodes takes turn according to a given probability to become CH. Low-Energy Adaptive Clustering Hierarchy (LEACH) [50], Power Efficient Gathering in Sensor Information Systems (PEGASIS) [51] and Hybrid Energy-Efficient Distributed Clustering (HEED) [52] are examples of cluster based protocols which are designed for homogenous WSNs. However, these techniques perform poorly in heterogeneous WSNs scenario as nodes having less energy expire faster than higher energy nodes.

Heterogeneous WSN topology takes into account that the nodes have different initial energy. Thus they perform better than homogeneous WSNs in a real application scenario with variety of sensors such as warehouses, home monitoring and surveillance. Distributed Energy Efficient Clustering (DEEC) [53], Developed DEEC (DDEEC) and Enhanced DEEC (EDEEC) [54] are some of the heterogenous WSN protocols. These distributed clustering algorithms for heterogeneous WSNs have similar topological structure to an IoT system. Although multi-hop routing and residual energy for selecting CHs are considered, they neither incorporate the intricacies nor the benefit of a diversified and event driven IoT system.

1.3.3 Prior Work on Energy-Efficient, Security Design for IoE Infrastructure

As one of the most crucial blocks of the system (Section 1.1), which provides authentication, authorization, and data integrity, energy-efficient security implementation is one of the major concerns for the wide adaptation of IoE [15, 16]. As IoE systems are typically portable and energy and/or hardware-resource limited, and thus require low-complexity and energy-efficient implementation of security protocols in the hardware which would work on its own. This exposes IoE systems to a number of attacks, like frequency prediction, replay, denial-of-service, and eavesdropping. These attacks can compromise the system security, in terms of its confidentiality, privacy, and data integrity. without much human-intervention [55, 56]. Several cryptographic mechanisms and protocols have been proposed and successfully implemented in conventional systems [15, 55–58] without any stringent energy, cost, speed, memory, or computing resource restrictions. There are a number of energy-efficient implementations of cryptography in sensor systems [59, 60], but they are relatively easy to compromise.

Physically unclonable functions (PUFs) are among the potential solution to data security and counterfeiting problems [61, 62]. On-chip security can be implemented during chip production utilizing chip integration techniques. A physically unclonable function (PUF) refers to a structure's physical characteristic that is usually easy to measure but hard to model or predict [62, 63]. Instead of storing the secret key into a digital system, a PUF-based security approach derives its keys from inherent natural features of the system. A PUF-based output behaves like a random function and is unpredictable even for an attacker with physical access to the device. Furthermore, in contrast with conventional digital architectures, the PUF-based approaches intertwine cryptography and sensor properties, making the attack to such systems more challenging. Various types of PUFs, each with its *challenge/response* pair generation capability have been categorized broadly into three categories in the existing literature [63, 64]. These are *Weak PUFs*, *Strong PUFs*, and *Controlled PUFs*.

Weak PUFs

They have a small number of *challenge/response* pairs. The response R_C to a given challenge C is used to derive a secret key, which is never shared with anyone in public. Once an attacker gains full access to the physical device, all the *challenge/response* pairs can be modeled in a short time and the security of the device can be compromised. Some common Weak PUF designs are include SRAM PUF [65], Butterfly PUF [66], and Coating PUF [67].

Strong PUFs

They have a complex hardware mapping to generate *challenge/response* pairs in a way that makes it hard for the adversary to easily predict their behavior in a short time. Some applications of *Strong PUFs* are in device authentication [68] and key formation [69]. Typical security features of *Strong PUFs* are:

(a) Impossible to be cloned or physically duplicated. This means it is impossible to design a PUF with same physical imperfections that are originally present in the PUF to be cloned.

(b) The *challenge/response* pairs generated by the PUF should come in large numbers, making it difficult for an adversary to launch a brute-force attack on the PUF to determine the *challenge/response* pairs in limited time.

(c) Even with known *challenge/response* pairs, if the distribution of the responses comes from a polynomial distribution, the adversary will not be able to predict the responses to a given challenge.

One strong-PUF design [70] described a physical one-way random function-based optical PUF. Although PUF-based, this design does not integrate a PUF into its challenge/response system. Also, it requires a large external setup to validate the system and it is difficult to integrate into a resource-constrained sensor circuit. In [71], the authors proposed an Arbiter PUF (APUF) implementation that uses the *XOR* of responses from the Arbiter PUFs implemented on the same chip to decrease the predictability of the responses. However, APUFs are susceptible to modeling attacks [64]. To address the problems in APUFs, several other PUF-based designs were introduced to counter the modeling attacks; these are XOR PUF [72], feed-forward PUF [73], and ROPUF [74], which addresses stability issues with APUF outputs.

Controlled PUFs

Controlled PUFs satisfy all the unique features of *Strong PUFs*, and, in addition, implement a controlled logic based on those features to formulate a more advanced functionality on the system, making it more secure. Recently, public PUFs, SIMulation Possible but Laborious (SIMPL) PUF, device-aging- and process-variation-based security primitives and public key protocols have been proposed that provide security by exploiting the difference between actual execution and simulation times [61]. However, they generally require large computational efforts that result in high energy requirements.

State-of-the art PUF designs have been proposed in recent years for the resource constrained IoT systems. Authors in [75] present a way to use the fuzzy commitment on unmanned IoT devices that utilizes two noisy factors from the inside and outside of the IoT device. This work is based on input and output noise data and is very different from our proposed method which utilizes physical variations. Another recent work in

[76] utilizes the TERO-PUF metastable structure and is implemented in FPGA. In the [77] paper, it is argued with experimental results that model-building machine learning attacks can be successful in compromising security of FPGA-based PUFs. In [77] and [63], it has been described that controlled PUFs, where physical variations are used to hide challenge-response pairs successfully from the attackers, are able to provide a stable and long term security solution for the IoE systems.

1.3.4 Prior Work on Policy-based Energy Management in Smart Home IoE Ecosystem

In this section, we explain the existing state-of-art about the energy management in a smart home IoE ecosystem. The literature shows the various solutions as to how and to what extent user policies and feedbacks affect the IoE system.

Recent developments in the area of information and communication technologies have provided an advanced technical foundation and reliable infrastructures for the smart house with a home energy management system [78, 79]. Development of low power, cost-efficient and high performance smart sensor technologies have provided us with the tools to build smart homes [80, 81]. As a result, a service platform can be implemented in a smart home to control the demand Response (DR) intelligently. This type of system should also give the users enough flexibility to input their choices while deciding on control of home devices [82] This makes the system more coherent, user friendly and scalable. While different hardware, software, communication architectures have been proposed and compared by their power consumption, performance, etc. [83–85], the cost of implementing the infrastructure like: hardware devices, software framework, communication interfaces, etc. are still high enough that hinder the process of implementing the smart home technology for ordinary users. Moreover, the hardware and software architectures may not be able to handle the growing number of sensors and actuators with their heterogeneity.

Many authors have attempted to address the way to reduce peak energy based on an agent-learning framework using multiple tools such as model predictive control [86], particle swarm optimization [87], iterative dynamic programming based [88] and gradient-based methods [89]. However, these models are probabilistic and do not constitute learning from interaction with the environment. Further, these models are mostly price based, where cost saving instead of user preferences is a predominant factor. Some other solutions proposed in [90] and [91] consider Q-learning based agent interaction system, however they target only particular appliances like air conditioners and LED lights.

In [92], authors have proposed a fully-automated energy management system based on the classical Q-learning based Reinforcement Learning (RL). The modelling is delay based, where users have a way of inputting their energy requests via time-scheduling and the agent learns gradually with time to find the optimal solution. However, this approach has several limitations. The author assumes mathematical disutility fuction and consumer initiated energy usage. Finding disutility function for each home or residence is costly and difficult and too much user interaction is not desired for a interoperable energy management system. [93] focuses on applying a batch RL algorithm to control a cluster of electric water heaters. A more relevant work is reported in [94], which proposes device-based Markov Decision Process (MDP) models. It assumes that the user behaviour and grid control signals are known. However, these assumptions are not realistic in practice. In [95], authors use a discrete-time MDP based framework to facilitate the use of adaptive strategies to control a population of heterogenous thermostatically controlled loads to provide DR services to the power grid using Q-learning.

Again the application here is specific to load controlled by ambient temperature.

1.4 Research Focus and Goals

In this section, we summarize the inferences and shortcomings from the existing literature to clarify the focus of our thesis. The summary is drawn with respect to various layers of energy-efficient architecture of IoE infrastructure.

On Optimal Energy Control in Wireless Sensor Networks Based IoE Systems

As evident from the existing literature, achieving energy savings through battery replenishment and traffic dynamics optimization in a network power model of sensor systems is an active research problem. The shortcomings of the existing literature which motivated us to provide solutions to address them in our thesis are oulined as below:

- Network lifetime and utility formulation in the existing work neither takes into account the energy consumption model nor the system performance trade-off with lifetime increase.

- Joint lifetime- utility-rate-reliability approach for WSNs in state-of-art incorporates a generic error coding processing power model without re-transmission energy requirements or energy savings due to enhanced error correction capability.

- The existing work assumes the battery energy to be zero at start. This assumption will not work for the scenario of an IoE system which contains rechargeable batteries.

- The utilization of the network varies with listening power of the receiver block. This is a major energy consuming block and whose analysis have been missing from the existing literature.

- Existing solution models address the needs of a narrow class of applications in specific areas, and are not suitable for a broad range of applications.

On Energy-efficient and Distributed Data-Aware Routing and Clustering Protocol

IoT and heterogeneous WSNs systems are similar in being equipped with sensors, base station (data gathering and decision making node) and wireless transceivers. But IoT system is more diversified in involving some notable variations like interaction between multiple protocols, sensing systems having varied energy values, asynchronous event driven processing and gateway node in between sensors and BS to route data more efficiently. Moreover, due to the evolution of active RFID tags [96] with reading capability in the range of meters and various energy harvesting mechanisms [43, 97], prudent techniques in IoE systems using them are better equipped to handle the energy efficiency and network lifetime problem.

On Energy-Efficient, Security design for IoE Infrastructure

As evident from the existing literature, design of energy-efficient and resource-optimized security system is a challenge for IoE systems. We address the shortcomings of the existing literature to design such a energy-efficient security system in Chapter 4. The inferencs and challenges from the existing literature are oulined below :

- The existing security solutions for the IoE systems focuses on incorporating software oriented solutions. This demands extra hardware resources for the already resource constrained systems.

- The PUF solutions for the IoE systems focuses on FPGA-based system implemetation and is not an optimised solution for a broad range of IoE systems.

- Other existing solutions have minimal circuitry implementation but compromise on the security and energy-efficiency problems.

On Policy-based Energy Management in Smart Home IoE Ecosystem

As evident from the existing literature, peak energy demand reduction by maximizing user convenience in a smart home based IoE ecosystem is the major goal of Chapter 5. The smart home system is a broad application scenario for an IoE implementation. The existing literature lacks a comprehensive IoE system analysis. Specifically,

- Models proposed in state-of-art literature are probabilistic and do not constitute learning from interaction with the environment. Further, these models are mostly price based, where cost saving instead of user preferences is a predominant factor.

- The cost of implementing the infrastructure like: hardware devices, software frame- work, communication interfaces, etc. are still high enough that hinder the process of implementing the smart home technology for ordinary users.

- Security is a major issue in the successful implementation of an IoE system, analysis and model of which is missing from the smart home systems.

- Time-of-Use (TOU) models of smart meters in the existing technology mostly help the local distribution company and in order to take advantages of the TOU, each household has to adopt a change in the use of the appliances which may cause signicant discomfort to the consumers.

1.4.1 Broad Goals of the Thesis

To fulfill the shortcomings of the existing literature, here we broadly define the objective of our thesis.

- Data is generated at a rapid pace and nodes of an IoE system are diminishing in size. The energy resources are insufficient with decreasing size of nodes, increasing number of nodes, volume of data and demand for embedded security. Hence, the major goal of this thesis is to fill the energy gap required for an IoE system as depicted in Fig. 1.3.

- The prime objective to fulfil our goal is to find an energy efficient model implementation which would consume the least amount of hardware resouces while maintaining a high quality of service for the end users.

- To analyze the effect different techniques such as error control coding, wireless energy harvesting and event driven data listening, has on the IoE system. And validating their effects through simulations and experiments.

- Analyze and validate through design and meaurements, the effect of designing a energy-efficient security block for the IoE system. As this is one of the most important blocks for the successful implementation of the IoE system, it is imperative to analyze this blocks through the trade-offs of energy and security.

- Testing and validating the designed energy-efficient model for the IoE system through a broad application scenario is also incorporated into the objective. This is to give the users a viable and practical criteria along with its pros and cons for their own implementation of the system.

1.4.2 Key Contributions and Results

The contributions of the thesis are described in this section for each chapter which follows our broad goals.

Optimal Energy Control in Wireless Sensor Networks Based IoE Systems

Our work in Chapter 2, focuses on solving the research problems mentioned above. We achieve our goal of increasing network lifetime through incorporating a wireless energy harvesting, error correction coding and wake-up-radio model into our system while maintaining the quality of service requirements. We substantiate our system through thorough simulations of various network lifetime-utility trade-offs. The details of our objectives are as follows:

- We solve the data-utility lifetime trade-off problem by taking an approximated lifetime function as well as the energy harversting, wake up radio duty cycling and retransmissions into the utility function. This solves the problem of incorporating a proper energy model for the system. This also focuses on reducing the reciever power (the major power hungry block of sensing system) through wake-up radio based duty cycling approach. Through a system parameter variation in the simulation of data-utility lifetime trade-off problem, we provide the user more flexibility in chosing the appropriate trade-off for a broad range of applications.

- We incorporate a redundant residue number system based error correcting technique and compare it with ARQ and Bose-Chaudhuri-Hocquenghem (BCH) to solve the problem of achieving better retransmission rate, thus enhancing energy savings of the netowrk. Innovatively, the packet error rate and delay are being included while computing lifetime and performance of the sensor network. This solves the re-transmission problem in the existing literature and through simulation the error-correction coding schemes' network lifetime enhancing benefits have been established in common sensor nodes.

Energy-efficient and Distributed Data-Aware Routing and Clustering Protocol

Our main solutions with respect to the shortcomings in the existing literature are as follows:

- The system is distributed in two-levels based on their initial energy as normal nodes with standard battery energy and advanced nodes with *a* times more energy than normal nodes [54]. We use the RFID tagging and reading mechanism to reduce the energy consumption during the cluster head (CH) selection phase till all the advanced nodes (also called gateway nodes) have their energy exhausted. Thereby prolonging lifetime of the network.

- We validate data awareness by dividing the sensor based on urgent and regular data demand and switch nodes between high/low power state based on data requirement at the user side. The solution expects to save energy in the nodes and improving battery life.

- We additionally incorporate RF energy harvesting for normal nodes with a power management unit (PMU) to further improve network lifetime.

Energy-Efficient, Security design for IoE Infrastructure

Our solution described in Chapter 4 falls in the controlled-PUF category which tries to provide long term energy efficient secure solution for the IoE systems. The focus of our thesis is in the energy efficiency and minimal resource design. Thorough measurements and testing leads to a Strong PUF design with integrated control logic to further consolidate the security of the system. Specifically, our objectives are summarized as below:

- Our approach focuses on finding a challenge/response pair to authenticate the system with minimal circuitry addition to the already resource constrained system.

- Energy efficient implementation is the main focus of our approach. Hence a solution is proposed which is hardware based instead of traditional software based solutions.

- Rather than implementing complex computations and hardware circuitry, we focus on building a simple circuit which provides the desired security solutions.

Policy-based Energy Management in Smart Home IoE Ecosystem

In summary the contributions addressing the issues described in Section 1.4 are as follows:

- **User interface** : Using a node-red development framework[1] and message queue telemetry protocol secure broker, a user interface has been designed. It incorporates intelligent energy management capability and provides user input options. Temperature control of appliances, operation rescheduling and *On/Off* commands are initiated through the interface.

- **Peak demand reduction** : Using the proposed HEMaaS methodology, a reward matrix is generated for each peak reduction threshold. There are four peak reduction thresholds considered in Chapter 5: $5\%, 10\%, 15\%$ and 20%. Based on the user convenience suitable load reduction decisions are obtained.

[1] Node-RED is a web-based programming tool for wiring together hardware devices, APIs and online services. [Online] Available : https://nodered.org/.

- **Fault tolerance and user privacy** : Taking different random combinations of robustness measure, it has been shown how the user convenience is affected when user privacy is compromised and system has hardware fault.

- **Energy saving and Carbon-footprint reduction** : The energy savings and carbon emmission reduction has been shown for a community of 85 houses over a year.

1.5 Thesis Outline

Below, we summarize the achieved solutions for the thesis objectives in different chapters of the thesis:

- In Chapter 2, we formulate and solve a joint maximization problem of system performance (measured by data utilization) and lifetime for wireless sensor network. Apart from throughput, packet loss and retransmissions and data utilization of a network also has a major impact on the performance of a WSN system. Retransmissions affects the throughput of the system depending on the amount of packet loss a network suffers in a given time slot. Data utilization for a node is dependent on the time frame in which the node is active. Therefore packet loss and data utilizations are incorporated in the system model to provide a more realistic data loss and utilization model for the WSN system. As energy is scarce resource for a WSN system, energy harvesting is adapted in the system model to increase its lifetime. Energy harvesting is dynamic and varies as to how can be harvested in each time slot. We model the harvesting as a stochastically varying Gaussian i.i.d process. The problem throws challenges in finding an optimal solution as the time-variation combined with retransmissions, packet loss and harvesting makes it complex. We, then provide a distributed solution to the problem by solving the data-utility and network lifetime separately. We consider retransmissions as discrete, packet loss is varied as the system utility and the optimal energy is found out as a function of utility and lifetime of the network.

- In Chapter 3, we have proposed a Data Aware Energy Efficient distributed Clustering protocol for IoT (DAEECI) by saving cluster head (CH) selection energy using active RFID tags, cutting processing energy by incorporating data awareness factor in the system and improving lifetime by inculcating RF energy harvesting. The system is distributed in two-levels based on their initial energy as normal nodes with standard battery energy and advanced nodes with a times more energy than normal nodes. We use the RFID tagging and reading mechanism to reduce the energy consumption during the CH selection phase till all the advanced nodes (also called gateway nodes) have their energy exhausted. Thereby prolonging lifetime of the network. We propose data awareness by dividing the sensor based on urgent and regular data demand and switch nodes between high-/low power state based on data requirement at the user side. The solution expects to save energy in the nodes and improving battery life. We additionally incorporate RF energy harvesting through a power management unit for normal nodes to further improve network lifetime. Our simulation depict substantial improvement in lifetime of network and data delivery to the base station.

- In Chapter 4, we propose an IoT sensor security scheme that utilizes a physically unclonable function (PUF) of the sensor. As a proof of concept, we present the approach in the context of silicon photo diodes and use their dark current variations as a PUF. The challenge used for system authentication is generated by quadratic residues. In an effort to build a system prototype, we measure the dark current of photo-diodes in terms of noise and energy consumption, in order to identify an optimal configuration of the circuit. A prototype PUF circuit of the sensor node incorporating the current amplification circuitry was designed and tested to prove the feasibility of dark current measurements in a portable environment. We have proposed, implemented, and tested an authentication protocol using PUF and the quadratic residues. We have also proposed an asymmetric digital signature-based encryption scheme, using the PUF response-generated private key, and simulated it using parameters of the PUF circuit and the authentication protocol. Our approach is validated by using measured, simulated, and analyzed the currents, adversary attacks, and energy requirements, to validate the approach. This concept can be extended to IoT applications that use alternative types of sensors (beyond photo-diodes), as long as the sensors exhibit random-like physical property variations.

- In Chapter 5, a new method named as Home Energy Management as a Service (HEMaaS) is proposed which is based on neural network based Q-learning algorithm. Although several attempts have been made in the past to address similar problems, the models developed do not cater to maximize the user convenience and robustness of the system. Here, we have proposed an advanced Neural Fitted Q-learning method which is self-learning and adaptive. The proposed method provides an agile, flexible and energy efficient decision making system for home energy management. A typical Canadian residential dwelling model has been used to test the proposed method. Based on analysis, it was found out that the proposed method offers a fast and viable solution to reduce the demand and conserve energy during peak period. It also helps in reducing the carbon footprint of residential dwellings. Once adopted, city blocks with significant residential dwellings can significantly reduce the total energy consumption by reducing or shifting their energy demand during peak period. This would definitely help IoE network administrators to optimize their resources and keep the tariff low due to curtailment of peak demand.

- In Chapter 6, summary and concluding remarks are provided and possible future research directions are discussed.

Chapter 2

Optimal Energy Control in Wireless Sensor Networks Based IoE Systems

In this chapter, we formulate and solve a joint maximization problem of system performance (measured by data utilization) and lifetime for wireless sensor network. The packet loss and data utilizations are incorporated to provide a more realistic data loss and utilization model for the WSN based IoE system. As energy is scarce resource for a WSN system, energy harvesting is adapted in the system model to increase its lifetime. We model the harvesting as a stochastically varying. Contrary to articles [44–46], our model assumes that the battery starts with a initial energy and the network operations has to be sustained using harvesting and wake up radio (WUR), using harvesting from ambient RF energy rather than using a solar energy harvester which needs extra circuitry. The overall problem throws challenges in finding an optimal solution as the time-variation combined with retransmissions, packet loss and harvesting makes it complex. We, then provide a distributed solution to the problem by solving the data-utility and network lifetime separately. Motivated by the emerging concept of Green

Wireless Sensor Network (GWSN) in which the lifetime and throughput performance of the system is maximized while minimizing the carbon footprints, our goal is to build an sustainable WSN system by supplying adequate energy to improve the system lifetime and providing reliable/robust transmission without compromising overall quality of service.

The rest of this chapter is organized as follows. System model formulation is described in Section 2.1. In Section 2.2, we propose the WEH and WUR schemes for WSN system. In Section 2.3, we formulate the joint utility-lifetime trade-off problem and formulate a distributed solution based on subgradient method and Section 2.4 shows our simulation plots.

2.1 System Model and Problem Formulation

We consider a network of non-mobile and identical sensor nodes denoted by N. Sensor nodes collect data from the surrounding information field and deliver it to the sink node/collector node denoted by S. As in [98], sensors communicate either in an uniformly distributed ring topology or randomly in a multi-hop ad-hoc topology. We assume that the sensor devices in an WSN system are transmitting over a set of links L. We model the wireless network as a $\{$edge, link$\}$ connectivity graph $G(Z,L)$, where the set, $Z = N \cup S$, represents the source and sink nodes. The set of links, L, represent the communication link between the nodes. Two nodes i and j are connected if they can transmit packets to each other with $i \in N$ and $j \in N_i$. Fig. 2.1 shows a sample connectivity graph with three sensor nodes $(i1,i2,i3)$, one sink node $(s1)$ and six communication links $(l1,l2,l3,l4,l5,l6)$. The communication between node $i1$ and $s1$ is a single-hop transmission whereas between $i3$ and $s1$ denotes a multi-hop transmission with node $i2$ acting as relay for data of node $i3$. The set of outgoing links and the set of incom-

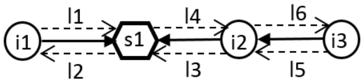


Figure 2.1: Connectivity graph

ing links corresponding to a node i are denoted by $O(i)$ and $I(i)$ respectively. Thus, in Fig. 2.1, $O(i2) = (l3, l6)$ and $I(i2) = (l4, l5)$. Table 2.1 delineates the parameters used for the analysis of our scenarios in Chapter 2.

Table 2.1: Notations used

Symbol	**Description**	**Symbol**	**Description**	**Symbol**	**Description**
$\|\|.\|\|_\infty$	∞-norm	E_{TX}	Transmit energy [J/bit]	P_e	Packet Loss Rate
$\|\|.\|\|_p$	p-norm	E_{RX}	Receive energy [J/bit]	P_s	Packet Success Rate
N	Set of Sensor Nodes	E_{PR}	Processing energy [J/bit]	P_b	Bit error rate
S	Set of Sink Nodes	E_{SN}	Sensing energy [J/bit]	L_P	Length of packet
i	Outgoing Sensor Node	P_{LS}	Ideal Listening power [W]	$E(T)$	Expected no. retransmissions
j	Incoming Sensor Node	E_B	Battery energy of Sensor	h	Number of hops
r_{ij}	Rate of Information Flow	P_H	Harvested power	$GF(2^b)$	Galois Field of b-bits
R_{ij}	Source rate	$W_U^{'}$	Wake-up-radio on-off signal	$U(.)$	Utility function
C_l	Capacity of Link	γ	Path loss exponent	α	System design parameter
$T_{network}$	Lifetime of Network	d	Communication distance	ε	Lifetime approx. constant

2.1.1 Routing and Flow Conservation

We model the data transmission rates and routing of data in the network using flow conservation equation. Let r_{ij} denote the rate of information flow from nodes i to node j. Let R_{ij} denote the total information rate generated at source node i to be communicated to sink node $j \in N_i$. It is assumed that no compression is performed at the source node and data transmission is lossless. Thus satisfying flow conservation constraint, we have the flow equations at the nodes for time slot t as

$$\sum_{j\in N_i}\big(r_{ji}(t)-r_{ij}(t)\big)=R_{ij}(t),\forall i\in N,j\in N_i \tag{2.1}$$

The maximum transmission rate of a link is also known as its capacity C_l. For a given transmit power of node and bandwidth of the channel, this value is fixed and is a upped bound of r_{ij} as $0\leq r_{ij}\leq C_l$.

2.1.2 Energy Cost Model

The network lifetime is dependent on the power consumption of the sensor node P_i per active duty cycle slot T_i of a node. This involves the combined operations of sensing, processing and communication (receive/transmit). If a sensor node goes out of the service due to energy deficiency, then all the sensing services from that node are affected till the battery is replaced. Radio transceiver is the one of the most power hungry block of a sensor device. The communication energy per bit per time slot $E_{comm}(t)$ consists of $E_{RX}(t)$ (receiver energy per bit per time slot) and $E_{TX}(t)$ (transmitter energy per bit per time slot). The computation energy includes $E_{PR}(t)$ (processing energy per bit per slot) and $E_{SN}(t)$ (sensing energy per bit per time slot). Let, $E_B(t)\geq 0$ is the total residual energy left in a sensor node operated by battery at time slot t. The power consumption in a time slot t is modeled as

$$\begin{aligned}P_i(t)=&\sum_{i\in N,j\in N_i}r_{ij}(t)E_{TX}(t)+\sum_{i\in N,j\in N_i}r_{ji}(t)E_{RX}(t)+\sum_{i\in N,j\in N_i}R_{ij}(t)E_{PR}(t)\\&+\sum_{i\in N,j\in N_i}R_{ij}(t)E_{SN}(t)+\sum_{l\in O(i)}P_{LS}(t)\end{aligned} \tag{2.2}$$

From the communication energy model in [32], we modify our transmitter energy for transmitting one bit of data from $i\in N$ to $j\in N_i$ across distance d as

$$E_{TX} = a_1 + a_2 \cdot d_{ij}^{\gamma} \tag{2.3}$$

Where γ is the path loss exponent varying from $\gamma \in [2,6]$, a_1 and a_2 are constants depending on the characteristics of the transceiver circuit.

2.1.3 Packet Loss and Data Re-transmission

As often as the packets are failed to be delivered to the sink node, the re-transmission consumes extra energy from the battery source of the sensor node, thereby decreasing its lifetime substantially. Therefore, a fundamental approach to reduce the packet loss is necessary to be integrated together with upper layer protocols to deliver reliable WSN management. Thus, we propose to use the approach of Error Correction Coding (ECC) to improve transmission reliability. ECC adds redundancy to improve the transmission reliability thereby reducing the efficiency, it is still a more preferable solution, because it helps to improve both reliability and latency. We derived a error coding scheme on the theoretical basis of Redundant residue number systems (RRNS) which have been introduced in [99, 100]. The performance is evaluated in terms of the packet error rate and compared with the state of the art Automatic Repeat reQuest (ARQ) scheme that is widely used in IEEE 802.15.4 radio. A preliminary analysis has been done in [19] that has been extended into our system model in this Chapter.

Analysis of packet error in ARQ scheme

In ARQ scheme, data is decoded by cyclic redundancy check (CRC) codes and the erroneous data is re-transmitted from the sender. Here we consider stop and wait ARQ method. Assuming the ACK bits are received without error, the packet error rate of the ARQ scheme is given by

$$P_e^{ARQ} = 1 - (1 - P_b)^{L_P} \tag{2.4}$$

where L_P is the packet length of the payload transmitted in a single transmission, P_b is the bit error rate. P_b for sensor nodes in IEEE 802.15.4 is given in [101].

Analysis of packet error in ECC schemes

For BCH and RRNS codes, let us assume that we use a (n,k,e) e-error control method with $n-k$ redundant bits appended to the k-data bits. We further assume that the transmission of the packets between the sensor node and sink node is in bursts of n-bit data. Therefore, the packet loss rate at the sink node is given as

$$P_e^{ECC} = 1 - \left(1 - \sum_{i=e+1}^{n} \left(\begin{array}{c} n \\ i \end{array}\right) P_b^i (1-P_b)^{n-i}\right)^{\left\lceil \frac{L_P}{k} \right\rceil} \tag{2.5}$$

Where $\lceil . \rceil$ is the ceiling function. We assume that due to poor channel conditions and interference, when a packet is unsuccessful in reaching its destination, it is counted as loss of packet and a re-transmission is required. The packet is assumed to be successfully delivered when the acknowledgement (ACK) for the delivery is received. Thus it takes one complete trip for the packet to be assured as successfully delivered. Let P_e be the probability of an event where the packet is lost in being delivered from sensor to sink or the ACK failed to reach the sensor from sink. Thus, for a single hop the expected number of re-transmissions is given by [32]

$$E(Tr) = \frac{1}{(1-P_e)} \tag{2.6}$$

Where, P_e is the packet loss rate of ARQ or ECC schemes. Accordingly, packet loss rate for end-to-end in a h-hop scenario is given as

$$E(Tr,h) = \frac{h}{(1 - P_e)} \tag{2.7}$$

Lemma 1. *Let P_e be the probability of an event where the packet is lost in being delivered from sensor to sink or the ACK failed to reach the sensor from sink. Thus, for a single hop the expected number of re-transmissions is given by*

$$E(Tr) = \frac{1}{(1 - P_e)} \tag{2.8}$$

Where, P_e is the packet loss rate of ARQ or ECC schemes. Accordingly, packet loss rate for end-to-end in a h-hop scenario assuming each node transmission is independent of the other as per the TDMA based MAC protocol.

$$E(Tr,h) = \frac{h}{(1 - P_e)} \tag{2.9}$$

Proof. *See [32].*

Redundant residue arithmetic based error correction scheme

A residue number system (RNS) is a non-weighted number system that uses relatively prime bases as moduli set over GF (2^b) [102]. Owing to the inherent parallelism of its structure and its fault tolerance capabilities, shows fast computation capability and reliability. RNS is defined by a set of β moduli $m_1, m_2, \ldots \ldots \ldots m_\beta$, which are relatively prime to each other. Consider an integer data A, which can be represented in its residues

$\Gamma_1, \Gamma_2, \ldots\ldots\Gamma_\beta$

$$\Gamma_i = A \; mod \; m_i, \; i\text{=}1\text{,}2\text{,}\text{....}l \tag{2.10}$$

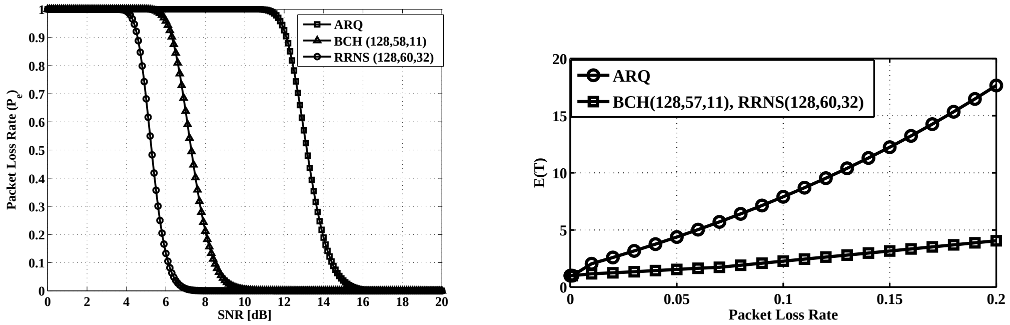
$$\Theta = \prod_{i=1}^{\beta} m_i \tag{2.11}$$

The maximum operating range of the RNS is Θ given by (2.11). The corresponding integer A can be recovered at the decoder side from its β residues by using the Chinese Remainder Theorem [102] as

$$A = \sum_{i=1}^{l} \Gamma_i \times M_i^{-1} \times M_i \tag{2.12}$$

where $M_i = \Theta/m_i$ and the integers M_i^{-1} are the multiplicative inverses of M_i and computed apriori. One common modulus set $(2^{b-1}-1, 2^{b-1}, 2^{b-1}+1)$ with a power of two in the set makes it relatively easy to implement efficient arithmetic units. A redundant residue number system (RRNS) is defined as a RNS system with redundant moduli. In RRNS, the integer data X is converted in β non-redundant residues and δ-β redundant residues. The operating range Θ remains the same and the moduli satisfy the condition $m_1 < m_2 < \ldots\ldots. < m_\beta < m_{\beta+1} < m_{\beta+2} < \ldots\ldots. < m_\delta$. RRNS can correct up to $\lfloor(\delta-\beta)/2\rfloor$ errors. If we consider the popular modulus set, mentioned above, and add the redundant modulus (2^b+1) to it, becomes the $(2^{b-1}-1, 2^{b-1}; 2^{b-1}+1, 2^b+1)$ RRNS with capability to detect one error, it is explained extensively in [102]. Since the Chinese Remainder Theorem approach require processing large-valued integers, a suitable method for avoiding this is invoking the so-called base-extension (BEX) method using mixed radix conversion (MRC)[103] that reduces the computation overhead by minimum distance decoding.

Based on RRNS, we propose an online error detection and correction scheme for the



(a) Packet loss vs. SNR for IEEE 802.15.4 based sensor at different coding schemes.

(b) Expected No. of Packet Retransmissions vs. packet loss rate at different coding schemes for IEEE 802.15.4 based sensor.

Figure 2.2: Analytical results of different coding schemes for IEEE 802.15.4 based sensor.

GWSN systems. A parallel to serial converter changes *A* into its decimal representation. In a look-up-table (LUT), we store the modulus values of numbers $0-9$ and 10^{χ} ($\chi \in 1, 2, ...\kappa$) with respect to the δ moduli (β non redundant moduli and δ-β redundant moduli). All operations are performed in parallel modulo channels without the need of transmission of information from one modulo channel to another. So, for l moduli, we have δ modulo channels operating in parallel, all operations in each performs modulo of the particular modulus till δ. Finally, we append the respective **MAC IDs** of the sensor devices at the front end of each set of packet data and transmit it to the gateway/sink node. **RRNS Algorithm** in [19] shows the decoding process at the sink node/gateway. It first receives the packet and tries to recover the data. After the recovery of the data and the error moduli, it appends a 1-bit **TRUE** flag with the *ACK* signal and sends it to the sensor node to notify the reception of data, else it sends a 1-bit **FALSE** flag with *ACK* to the sensor node signifying to resend the packet data again. The sensor node in turn transmits the δ-β redundant residues again instead of sending the full *n* bits of data again.

Packet loss statistics for different error correction schemes

We perform an analysis to find out the packet loss rate of the IEEE 802.15.4 based sensor. The systems signal to noise ratio is varied from 0dB to 20dB. The packet error rate is generated for BCH $(128,57,11)$ and RRNS $(128,60,32)$. These values of n are taken to correlate with the packet load of 133 bits (payload of 127 bits and 6 bits of header). From Fig. 2.2a, it can be inferred that ECC schemes provide approximately a gain of 4 dB in SNR as compared to ARQ scheme for the same packet loss rate. This is equivalent to a power gain of around 2 watts, which is essential savings in case of energy constrained GWSN systems. RRNS code provides slightly better gain of around 2 dB, owing to its better error correction capability compared to BCH code. Accordingly, in Fig. 2.2b we plot the values of re-transmissions required for ARQ, BCH codes, and RRNS codes. The plot depicts a similar nature as predicted in (2.5). As we can see, simple ARQ scheme in a packet loss rate varying from 0 to 20% requires expected number of re-transmissions of $\sim$ 1 to 17, whereas expected number of re-transmissions in BCH and RRNS coding schemes is $\sim$ 1 to 4 . The figure of merit for both BCH and RRNS shows average number of expected packet re-transmissions, even for a packet loss of 20% as $\approx$ 4, significantly outperforms the simple ARQ scheme. This can save a tremendous amount of energy leading to network lifetime enhancement.

2.1.4 Problem Definition : Network Lifetime Maximization through Energy Cost Model

The processing energy E_{PR} in (2.13) increases with redundancy $P' = (n-k)/k$. The re-transmissions consumes extra energy resources apart from the original transmission which is mandatory, hence incorporating the expected number of retransmissions

$E(Tr,h_i)$ for h_i-hops into (2.13), we get power consumption as in time slot t

$$P_i(P_e,h_i,t) = \sum_{i\in N, j\in N_i} r_{ij}(t)E_{TX}(t)(1+E(Tr,h_i)) + \sum_{i\in N, j\in N_i} r_{ji}(t)E_{RX}(t)(1+E(Tr,h_i))$$
$$+ \sum_{i\in N, j\in N_i} R_{ij}(t)E_{PR}(t)(1+E(Tr,h_i)P^{'}) + \sum_{i\in N, j\in N_i} R_{ij}(t)E_{SN}(t) + \sum_{l\in O(i)} P_{LS}(t) \tag{2.13}$$

packet success rate $P_s(t)$ affects the sample rate in the rate flow constraint as

$$\sum_{j\in N_i}\sum_{t=1}^{T_i}\big(r_{ij}(t) - r_{ji}(t) + P_s(t)R_{ij}(t)\big) \leq 0,\ \forall i \in N, j \in N_i \tag{2.14}$$

Let $T_{network}$ be the total number of active duty cycle slots representing the life-time of the network. We focus on maximizing the operation time of the whole network ($T_{network}$) until the first node fails,

$$T_{network} = \min \sum_{x=1}^{n} T_x, (n \in 1,2,....i) \tag{2.15}$$

The problem of maximizing the network lifetime can be stated as

$$\begin{aligned}
\mathbf{\max}_{t\geq 0, E_B(t)>0} \quad & T_{network} \\
\textbf{subject to} \quad & \sum_{t=1}^{T_i}\left(P_i(P_e,h_i,t) - \frac{1}{T_i}\cdot E_B(t)\right) \leq 0, \\
& \sum_{j\in N_i}\sum_{t=1}^{T_i}\big(r_{ji}(t) - r_{ij}(t) - P_s(t)R_{ij}(t)\big) \leq 0,\ \forall i \in N, j \in N_i \\
& E_{TX} = a_1 + a_2\cdot d^{\gamma},\ \gamma \in [2,6] \\
& 0 \leq r_{ij} \leq C_l
\end{aligned} \tag{2.16}$$

In our model, we have considered a battery with a finite maximum capacity E_{Bmax}, where $E_B(t){\leq}E_{Bmax}$. Further, due to hardware limitations the total power consumption is upper bounded by maximum consumption P_{max} (i.e $P_i(t)<P_{max}$, $\forall j \in N_i$,$\forall t \in T_i$). Problem in (2.16) is not convex. By substituting $s = 1/T_{network}$, we obtain a convex problem.

$$\begin{aligned} \min_{s\geq 0} \quad & s \\ \textbf{subject to} \quad & \sum_{t=1}^{T_i} (P_i(P_e, h_i, t) - s_i \cdot E_B(t)) \leq 0, 1 \leq t \leq T_i \\ & 0 < E_B(t) \leq E_{Bmax}, 1 \leq t \leq T_i \\ & \text{Constraints in (2.16)} \end{aligned} \tag{2.17}$$

2.2 Wireless Energy Harvesting and Wake-Up Radio Scheme

Block diagram of a generic wireless energy harvesting (WEH) enabled sensor node is shown in Fig. 2.3a. As shown in the figure, the nodes consists a rectifier, transceiver (RX, TX), sensors and sensor interface, storage unit (rechargeable battery), power management unit (PMU) [1] and the processor. An RF-to-DC converter (also known as rectifier) constitute the core of the wireless energy harvesting unit. The rectifier is in charge of converting the received RF power (by the receiver antenna) to a usable DC supply. This stable DC energy can be used to charge a battery and/or drive the electronic circuitry of the node. The conversion from RF to DC comes with some energy loss in the internal circuitry of the rectifier which quantified in terms of power conversion efficiency (PCE) of the rectifier. PCE being the ratio of the converted DC power to the RF input power, has significant implications on the overall performance of the power harvesting unit. This is further highlighted by reference to Friis free space equation which gives the available harvested power by [104]: The PCE is optimized for a designated in-

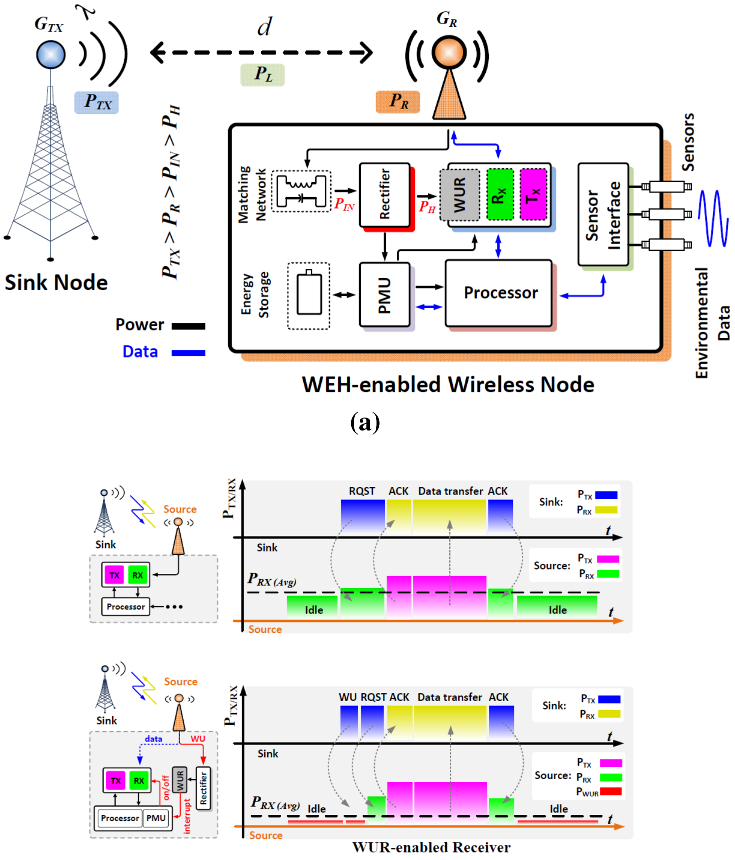
[1] 4.2.4

put power which corresponds to an specific communication distance. For longer (than optimal) distances (d_{ij}^2), the rectified power abruptly drops. When a receiver node i is in the energy harvesting mode, the power harvested (P_{H_i}) from base station server source in a time slot t can be calculated as follows

$$P_{H_i}(t) = \frac{\eta \cdot P_{TX} \cdot |H_i(t)|^2}{d_{ij}^2}, 1 \leq t \leq T_i \tag{2.18}$$

Where, η is PCE and H_i denotes the channel gain between between source and receiver at time slot t. As shown, the PCE is optimized for a designated input power (received form the antenna) which corresponds to an specific communication distance. Beyond this optimal point, the rectifier provides sufficient energy for storage or to drive the node circuitry. However, for longer distances from the sink node, the rectified power abruptly drops. In WEH-enabled nodes, PMU is in charge of managing the flow of energy to the storage unit, node circuitry and to the main receiver (RX). Aside from high efficiency, other key performance metrics of a WEH unit include high sensitivity (i.e., ability to harvest energy from small levels input power), wide dynamic range (i.e., maintaining high efficiency for a wide range of input powers), multi-band operation (i.e., ability to harvest wireless energy from wireless transmissions at different frequencies). Extensive studies exist in the literature investigating on techniques to improve the performance of WEH unit [18, 104]. The design presented in [105] studies techniques to enhance the efficiency of WEH unit and a muliti-band approach to enable harvesting and different frequencies.

In a wireless sensor node, although the receiver is practically called in to action only when its service is required, it has to constantly keep listening to the communication channel for the commands from the sink node. This so called *idle listening* mode power



(a)

(b)

Figure 2.3: WEH-enabled wireless sensor node . (a) Block diagram of WEH-enabled sensor node, (b) Timing diagram.

(P_{LS}) consumption when integrated over the lifetime of the node makes the receiver a significant energy consumer and is dependent on the amount of network utilized for given duty cycle. Let $\alpha \in (0,1)$ be the system parameter that defines the amount of network utilization. The amount of energy consumption modeled in terms of α in

(2.13) is

$$P_i(P_e,h_i,t) = \sum_{i\in N, j\in N_i} r_{ij}(t)E_{TX}(t)(1+E(Tr,h_i)) + \sum_{i\in N, j\in N_i} r_{ji}(t)E_{RX}(t)(1+E(Tr,h_i))$$
$$+ \sum_{i\in N, j\in N_i} R_{ij}(t)E_{PR}(t)(1+E(Tr,h_i)P^{'}) + \sum_{i\in N, j\in N_i} R_{ij}(t)E_{SN}(t) + \sum_{l\in O(i)} \alpha(t)P_{LS}(t) \tag{2.19}$$

In a wireless sensor node, the receiver unit despite not being the most power hungry block, constitutes a significant portion of the overall energy consumption of the system. While similar to other building blocks, the receiver is practically called in to action only when its service is required, it has to constantly keep listening to the communication channel for the commands from the sink node. This so called *idle listening* mode power consumption when integrated over the life time of the node makes the receiver a significant energy consumer.

An efficient solution to tackle the energy consumption during the idle listening mode is duty cycling (also known as *rendez-vous* scheme) in which the receiver maintains in deep sleep mode and only wakes up when there is a message to be received from the main transmitter (TX). There are three main classes of duty cycling, namely, synchronous, pseudo-asynchronous and asynchronous [106]. In the synchronous scheme, the transmitter and all the receivers pre-schedule designated time slots in which the receivers wake up for to receive the commands and fulfill the transmission. Such scheme imposes considerable overhead in terms of complexity and power consumption in order to establish time synchronization and leads to idle energy consumption if there is no data to be received during the pre-scheduled time slots. In the pseudo-asynchronous scheme, the receivers wake up at designated time but a synchronization between the transmitter and receiver is not required. In the asynchronous scheme which the most energy efficient approach among the duty-cycling classes, the receivers spends most of their time in deep sleep mode and only wake up when interrupted by the transmitter. This interrupt message is generated by a wake-up radio (WUR). WUR is a simple and low-power receiver which keeps listening to the channel and only wakes up the main receiver when the is a request for transmission to the associated node [107]. Fig. 2.3b schematically compares the energy profile of a conventional transceiver versus that of a WUR-enabled transceiver. As shown in the figure, the main receiver (RX) in the WUR-enabled transceiver is activated less frequently and only upon receipt of the wake-up command (WU) which is followed by the interrupt message generated by the WUR.

Fig. 2.3b schematically compares the energy profile of a conventional transceiver versus that of a WUR-enabled transceiver. As shown in the figure, as compared to the conventional method, the main receiver (RX) in the WUR-enabled transceiver is activated only upon receipt of the wake-up command (WU) which is followed by the interrupt message generated by the WUR. The infrequent activation of RX facilitates a substantial energy conservation over the life-time of the wireless node. Obviously, WUR scheme is favourable only if the power consumption of the WUR is much smaller than that of RX (i.e., $\mathrm{P_{WUR}} << \mathrm{P_{RX}}$ in Fig. 2.3b).

WEH-enabled nodes provide a good opportunity for a very efficient implementation of WUR [108]. Fig. 2.3, shows the block diagram of one such implementation for on-off keying (OOK) WU message. As shown in the figure, the rectifier block of the WEH unit can be re-utilized to perform as a simple envelope detector while also providing energy supply for the rest of WUR circuitry [108].

Let $P_{H_i}^{C}(t)$, denotes the cumulated harvested energy in all the slots of node i. For simplicity, we assume the harvested energy is available at the start of each interval t. We also assume that the battery has finite capacity and harvested energy can only recharge

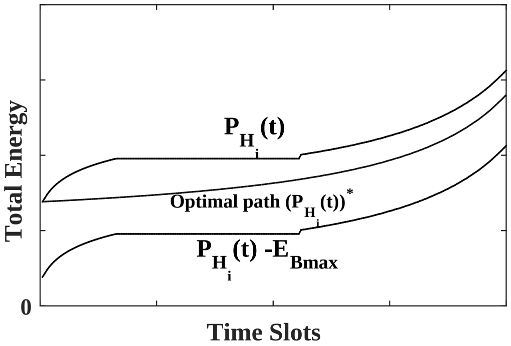


Figure 2.4: Feasible energy bound for harvested energy

till the maximum capacity of battery E_{Bmax}.

$$P_{H_i}^{C}(t) = \sum_{x=1}^{t} P_{H_i}(x), (t \in 1, 2, ...T_i) \tag{2.20}$$

$P_{H_i}^{C}(t)$ is a continuous increasing function that lies between points $(0,0)$ and $(T_i, P_{H_i}^{C}(T_i))$ as shown in Fig. 2.4. The cumulative node energy $P_i^C(t)$ for all $(t \in 1, 2, ...T_i)$ cannot be more than $P_{H_i}^{C}(t)$. Using this constraint, the dynamic charging and discharging of battery can be modeled as

$$\begin{aligned} &E_B(t+1) = E_B(t) - P_i(t) + P_{H_i}(t) \\ &P_i^C(t) \le P_{H_i}^{C}(t), \forall t \in 1, 2, ...T_i \end{aligned} \tag{2.21}$$

To find an optimal energy consumption $(P_i^C(t))^*$, we need to find the upper and lower bound of consumed energy. (2.21) gives the upper bound on the consumed energy. Further, $(P_i^C(t))^*$ must satisfy that, the residual energy of nodes at all time slots i.e. $(P_i^C(t))^* - P_{H_i}^{C}(t)$ cannot exceed the battery maximum capacity E_{Bmax}, forms the lower bound of $(P_i^C(t))^*$. Thus the problem in (2.17), can be reformulated as

$$\begin{aligned}
\min_{s \geq 0} \quad & s_i \\
\textbf{subject to} \quad & \sum_{t=1}^{T_i} \left(P_i(P_e, h_i, t) - s_i \cdot E_B(t) - P_{H_i}(t)\right) \leq 0, 1 \leq t \leq T_i \\
& 0 < E_B(t) \leq E_{Bmax}, 1 \leq t \leq T_i \\
& P_{H_i}^C(t) - E_{Bmax} \leq P_i^C(t) \leq P_{H_i}^C(t), \forall t \in 1, 2, ...T_i \\
& \text{Constraints in (2.15), (2.16), (2.18), (2.19) and (2.20)}
\end{aligned} \tag{2.22}$$

2.3 Joint Utility & Network Lifetime Trade-off and Distributed Solution

Solving standalone maximization of network lifetime problem by varying the source rates will result in allocation of zero source rates to the node. Thus, it results in application performance of the system to be worst. Therefore, it is optimal to jointly maximize the network lifetime with the system's application performance. We associate the network performance with the utility function $U_i(.)$. In [31], it has shown that each node $i \in N$ is related to a utility function and achieve different kind of fairness by maximizing the network utility. Thus the utility is a function of the node source rate R_{ij}. Apart from source rates, packet success rate P_s also affects the overall system performance. Thus, the utility function has to be modified to accommodate the packet success rate and the payload data efficiency as $U_i(R_{ij}, P_s)$. Max-Min fairness maximizes the smallest rate in the network whereas the Proportional fairness favors the nodes nearer to the sink node. As given in [31], by aggregating the utility, the network lifetime can be solved in a distributed way with an approximated approach as $F_s^{\varepsilon}(.) = \left(\frac{1}{\varepsilon+1}\right) \cdot s_i^{\varepsilon+1}$. Thus, the network lifetime problem in (2.22) becomes

$$\begin{aligned} \min_{s\geq 0} \quad & \left(\frac{1}{\varepsilon+1}\right)\cdot s_i^{\varepsilon+1} \\ \textbf{subject to} \quad & \text{constraints in (2.22), (2.19) \& (2.14)} \end{aligned} \tag{2.23}$$

Using (2.23), we can now formulate a joint trade-off between maximizing utility and network lifetime simultaneously. Our method differs from other approaches in Chapter 1-Section 1.3 as we consider a more realistic scenario, incorporating path loss, fairness, packet loss statistics for error control schemes as well as energy harvesting and a event driven radio wake-up scheme. Thus the cross-layer joint maximization problem is given as

$$\begin{aligned} \max_{(s,R_{ij},r_{ij})\geq 0} \quad & \sum_{t=1}^{T_i}\left(\alpha(t)\sum_{i\in N}\sum_{j\in N_i} U_i(R_{ij}(t),P_s(t)) - (1-\alpha(t))\left(\frac{1}{\varepsilon+1}\right)\cdot s_i^{\varepsilon+1}\right) \\ \textbf{subject to} \quad & \text{constraints in (2.22), (2.19) \& (2.14)} \end{aligned} \tag{2.24}$$

We have introduced a system parameter $\alpha\in[0,1]$ in (2.19). It gives the trade-off between the utility and network lifetime. For α=0, the utility is zero and for α=1, network lifetime is maximum with worst application performance. The maximization objective function is concave as $U(.)$ is concave and network lifetime problem $F_s^{\varepsilon}(.)$ is convex. We try to solve the primal problem via solving the dual problem [98]. We keep the expected number of transmissions $E(Tr,h_i)$ in hops h_i as constant and vary the rate r_{ij}. The constraint set in (2.24) represents a convex set. According to slater's condition for strong duality, if the non-linear constraints are strictly positive, duality gap between primal and dual problem is small. Thus the primal can be solved by solving the dual problem and the desired primal variables can be obtained. The dual-based approach leads to an efficient distributed algorithm.

2.3.1 Dual Problem

To solve the problem in a distributed manner, we formulate the Lagrangian in terms of the Lagrange Multipliers λ and μ by relaxing the inequality constraints in (2.24).

$$\begin{aligned}&\mathbf{L}(\lambda,\mu,\mathbf{s},\mathbf{r_{ij}},\mathbf{R_{ij}},\mathbf{U}(\mathbf{R_{ij}},\mathbf{P_s}),\mathbf{t}) = \\ &\sum_{t=1}^{T_i}\left(\alpha(t)\sum_{i\in N}\sum_{j\in N_i}U_i(R_{ij}(t),P_s(t)) - (1-\alpha(t))\left(\tfrac{1}{\varepsilon+1}\right)\cdot s_i^{\varepsilon+1}\right) \\ &+\sum_{j\in N_i}\sum_{t=1}^{T_i}\lambda_l(t)\big(r_{ij}(t)-r_{ji}(t)+P_s(t)R_{ij}(t)\big) \\ &+\sum_{i\in N}\sum_{j\in N_i}\sum_{t=1}^{T_i}\mu_i(t)(P_i(P_e,h_i,t)-s_i\cdot E_B(t)-P_{H_i}(t))\end{aligned} \tag{2.25}$$

The corresponding Lagrange dual function $D(\lambda,\mu)$ is given by

$$\begin{aligned}&\mathbf{D}(\lambda,\mu) = \sup_{\mathbf{s},\mathbf{r_{ij}},\mathbf{R_{ij}},\mathbf{U}} \mathbf{L}(\lambda,\mu,\mathbf{s},\mathbf{r_{ij}},\mathbf{R_{ij}},\mathbf{U}(\mathbf{R_{ij}},\mathbf{P_s}),\mathbf{t}) \\ &\textbf{subject to} \;\; \text{constraints in (2.22), (2.19) \& (2.14)}\end{aligned} \tag{2.26}$$

The solution is given by F^*

$$\mathbf{F}^* = \min_{\lambda>\mathbf{0},\mu>\mathbf{0}} \mathbf{D}(\lambda,\mu) \tag{2.27}$$

The dual problem can be decomposed further into two different subproblems $D_1(\lambda,\mu)$ and $D_2(\lambda,\mu)$.

$$\begin{aligned}
\mathbf{D_1}(\lambda,\mu) = & \max_{(R_{ij},r_{ij})\geq 0} \sum_{i\in N}\sum_{j\in N_i}\sum_{t=1}^{T_i} \alpha(t)\cdot U_i(R_{ij}(t),P_s(t)) \\
& + \sum_{l\in L}\sum_{t=1}^{T_i} \lambda_l(t)\big(r_{ij}(t) - r_{ji}(t) + P_s(t)R_{ij}(t)\big) \\
& + \sum_{i\in N}\sum_{j\in N_i}\sum_{t=1}^{T_i} \mu_i(t)\cdot (r_{ij}(t)E_{TX}(t)(1+E(Tr,h_i)) + r_{ji}(t)E_{RX}(t)(1+E(Tr,h_i)) \\
& + R_{ij}(t)E_{PR}(t)(1+E(Tr,h_i)P^{'}) + R_{ij}(t)E_{SN}(t) + \alpha(t)P_{LS}(t)) \\
& \textbf{subject to } \; E_{TX} = a_1 + a_2\cdot d^{\gamma},\ \gamma\in[2,6] \\
& \qquad\qquad 0 \leq r_{ij} \leq C_l \\
& \qquad\qquad P^C_{H_i}(t) - E_{Bmax} \leq P^C_i(t) \leq P^C_{H_i}(t), \forall t\in 1,2,....T_i
\end{aligned} \tag{2.28}$$

$$\begin{aligned}
\mathbf{D_2}(\lambda,\mu) = & -\{ \max_{(s,E_B)\geq 0} \sum_{i\in N}\sum_{j\in N_i}\sum_{t=1}^{T_i} \mu_t\,(s_i\cdot E_B(t) + P_{H_i}(t)) + \sum_{t=1}^{T_i}(1-\alpha(t))\left(\frac{1}{\varepsilon+1}\right)\cdot s_i^{\varepsilon+1}\ \} \\
& \textbf{subject to } \; 0 < E_B(t) \leq E_{Bmax}, 1\leq t\leq T_i \\
& \qquad\qquad P^C_{H_i}(t) - E_{Bmax} \leq P^C_i(t) \leq P^C_{H_i}(t), \forall t\in 1,2,....T_i
\end{aligned} \tag{2.29}$$

Subproblem $\mathbf{D_1}(\lambda,\mu)$ is a rate control problem in the network and transport layer of the sensor networks. For all active links $l\in L$, we substituted $\sum\limits_{i\in L}$ with $\sum\limits_{i\in N}\sum\limits_{j\in N_i}$. Subproblem $\mathbf{D_2}(\lambda,\mu)$ gives the bound on the inverse lifetime. The objective function of the primal problem is not strictly convex in all its primal variables $\{s,R_{ij},r_{ij}\}$. The sub-dual problems $\mathbf{D_1}(\lambda,\mu)$ is only piecewise differentiable. Therefore, the gradient projection method cannot be used to solve the problem. We use the subgradient method [98] to solve the problem iteratively till a desirable convergence is reached.

2.3.2 Solution to GWSN Distributed Algorithm and Its Convergence Analysis

Let, $\{s^*(\lambda,\mu), R^*_{ij}(\lambda,\mu), r^*_{ij}(\lambda,\mu), (P^C_{H_i}(t))^*, P^*_s(t), P^*_{LS}(t)\}$ be the optimal solutions for problems (2.28) and (2.29). The Lagrange multipliers (λ_l,μ_i) have cost interpretation to them. λ_l represents the link capacity cost and μ_i denotes the battery utilization cost of sensor node i. The gradients $\nabla_\lambda D(\lambda,\mu)$ and $\nabla_\mu D(\lambda,\mu)$ denote the excess link capacity and battery energy respectively. Problems $\mathbf{D_1}(\lambda,\mu)$ in (2.28) represent the maximization of the aggregate utility of the network in presence of flow constraints and energy spent in the network. The network lifetime problem $\mathbf{D_2}(\lambda,\mu)$ in (2.29) maximizes the revenue from battery capacities subtracting the lifetime-penalty function, resulting in reduction of lifetime.The procedure for solving the algorithm is outlined as follows:

- Initialize all the inputs $(E_{TX}, E_{RX}, E_{SN}, E_{PR}, P_{LS}, E_B)$ and step sizes $\varphi_\tau \leftarrow 0.01$, $\psi_\tau \leftarrow 0.01/\sqrt{\tau}$, $\varepsilon \leftarrow 20$
- Although the problem in $\mathbf{D_1}(\lambda,\mu)$ and $\mathbf{D_2}(\lambda,\mu)$ is convex, the solution is complex and difficult to implement due to the intricacies introduced by incorporation of optimal energy consumption $((P^C_i(t))^*)$, packet loss $(P^*_s(t))$ and WUR $(P^*_{LS}(t))$. From (2.28) and (2.29), it is evident that $(P^C_i(t))^*$ is dependent on optimal lifetime (s^*_{ij}) and sample rate (R^*_{ij}). Therefore we take $(P^C_{H_i}(t))^*$ as some function g of lifetime and sample rate.

$$g(s^*_{ij}, R^*_{ij}) = f((P^C_{H_i}(t))^*) \tag{2.30}$$

- We model $P^C_{H_i}(t)$ w.r.t the channel gain $H_i(t)$ distributed as *i.i.d* with mean 0. Once the optimal s^*_{ij}, R^*_{ij} is found, $P^C_{H_i}(t)$ is found using $f^{-1}\left(g(s^*_{ij}, R^*_{ij})\right)$.
- The packet success rate $P_s(t)$ is varied $\in [80,100]$ and system utility parameter $\alpha(t)$ and overall node utilization $U_i(R_{ij}(t), P_s(t))$ determines the optimal listening power

$P^*_{LS}(t)$.

- Thus from all the previous assumptions mentioned above, the time coupling property of the node can be excluded and finding solution for $\lim_{t\to 1}\lambda(t),\mu(t)$ would be good $\forall t \in (1,2,3,....T_i)$.
- The Lagrange multipliers can be updated by

$$\lambda_l(t,\tau+1) = \left[\lambda_l(t,\tau) + \varphi_\tau \sum_{j\in N_i} \left(r_{ij}(t,\tau) - r_{ji}(t,\tau) + P_s(t,\tau)R_{ij}(t,\tau)\right)\right]^+,$$
$$\mu_i(t,\tau+1) = \left[\mu_i(t,\tau) + \psi_\tau \sum_{i\in N}\sum_{j\in N_i} (P_i(P_e,h_i,t,\tau) - s_i\cdot E_B(t,\tau) - P_{H_i}(t,\tau))\right]^+ \quad (2.31)$$

- From (2.31) , it can be seen that as the flow r_{ij} exceeds the capacity of link C_l, the link cost and node energy cost increases. Thus higher link and node-battery prices result in greater penalty in the objective function in (2.28) forcing source rates R_{ij} & flows r_{ij} to reduce. Although higher node-battery cost (2.29) allow greater revenue for the same increase in battery capacities (by increasing ’s’), there is a corresponding penalty incurred due to the consequent lower lifetimes.

Lemma 2. *When $\varepsilon\to\infty$, the network lifetime $T_{network}$ determined by the optimal solution s^* of problem* (2.24) *approximates the maximum network lifetime of the wireless sensor network.*

Proof. *See Appendix A*

Further, let us make the following two assumptions as below:

- **Assumption 1**: Let $U_i(R_{ij},P_s)$ be defined as $log_2(R_{ij}P_s)$ which is an increasing and concave function, and its inverse and hessian exists.
- **Assumption 2**: Hessian of $U_i(R_{ij},P_s)$ is negative semidefinite and $r^{min}_{ij}\leq r_{ij}\leq r^{max}_{ij}$.

Define $\overline{L}$ = max L as the maximum number of links that a sensor node uses. Let $\overline{U}$ = max $U_i^{'}(R_{ij}, P_s)$ and $\overline{R}$ = max r_{ij}, be the maximum rate flow of the node when transmitting information from $i{\rightarrow}j$.

Proposition 1. *If the assumptions 1 and 2 above hold and the step size satisfies* $0{<}\varphi_\tau, \psi_\tau{<}\frac{2}{\overline{L}^{1/2}\overline{U}\,\overline{R}}$*. Then starting from any initial rates* $r_{ij}^{min}{\le}r_{ij}{\le}r_{ij}^{max}$*, & price* $\lambda_l, \mu_i{\ge}0$*, every limit point of the sequence* $\{s(\lambda,\mu), R_{ij}(\lambda,\mu), r_{ij}(\lambda,\mu)\}$ *generated by* ***GWSN Algorithm****, is primal-dual optimal.*

Proof. *See Appendix B*

Proposition 2. *By the above distributed algorithm, dual variables (*λ_l*,*μ_i*) converge to the optimal dual solutions (*λ_l^**,*μ_i^**), if the stepsizes are chosen such that*

$$\varphi_\tau(i) \rightarrow 0, \sum_{i=1}^{\infty} \varphi_\tau(i) = \infty, \psi_\tau(i) \rightarrow 0, \sum_{i=1}^{\infty} \psi_\tau(i) = \infty \tag{2.32}$$

2.4 Simulation Results

To show the joint trade-off between maximizing utility and network lifetime in terms of system parameter α, path loss γ, packet loss statistics $\{P_e^i\}$,energy harvesting P_{H_i}, we consider a WSN as shown in Fig. 2.5 with seven nodes distributed over a square region of 100m × 100m. The node at the middle of the network is taken as the sink node and the other six nodes are either source or source/relay nodes. Nodes $\{i1, i2, i4, i5\}$ act as source nodes whereas nodes $\{i3, i6\}$ act as source node to deliver its own data and relay nodes for delivering nearest neighbor's data to the sink node. The parameters taken for the simulation are depicted in Table 2.2. The value of E_{TX}, $\{a_1, a_2\}$ are chosen from [32] with γ=4. E_{RX} and E_{SN} are taken from [109]. Processing energy E_{PR} is assumed

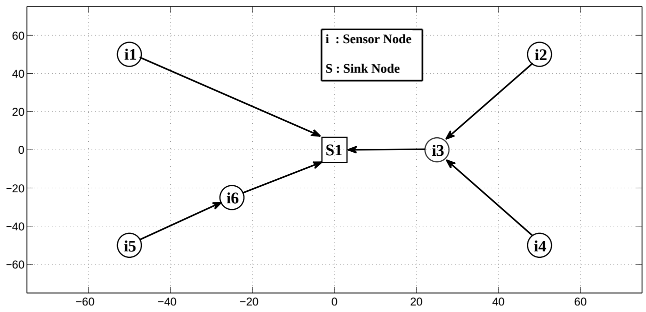


Figure 2.5: WSN topology.

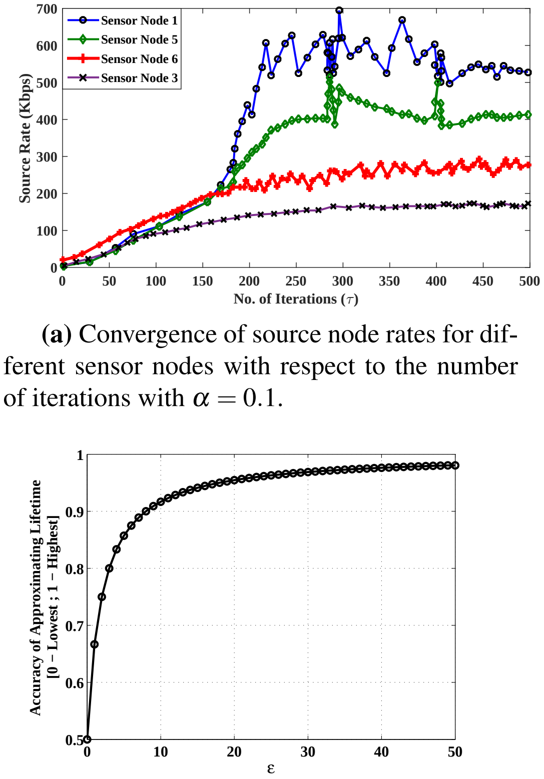
to be same as the sensing energy E_{SN}. Also, at start t_0 the initial battery energy E_B in all the nodes is taken as 1 J. We run our simulations till 500 iterations to get a desired solution for the system.

Table 2.2: WSN simulation parameters

Parameter	**Description**	**Value**	**Parameter**	**Description**	**Value**
a_1, a_2	Transceiver Constant	10^{-7}, $0.1 \cdot a_1$ J/bit	E_{SN}	Sensing energy	$5 \cdot 10^{-8}$ J/bit
γ	Path Loss Exponent	4	E_{PR}	Processing energy	$5 \cdot 10^{-8}$ J/bit
ε	Lifetime Approx. Constant	20	P_{LS}	Idle listening power	1 mW
E_{RX}	Receiver energy	$1.35 \cdot 10^{-7}$ J/bit	E_B	Battery energy	1 J

2.4.1 Convergence Plots

To show the convergence of our GWSN algorithm, we plotted in Fig. 2.6a, the convergence of source node rates for different sensor nodes with respect to the number of iterations. We have chosen sensor node $\{i1, i3, i5, i6\}$, where $\{i1, i5\}$ act as only sensor nodes and $\{i3, i6\}$ act as both sensor and relay node. The step size is taken as $\varphi_\tau = 0.01$, where τ is the index of iteration. It can be observed that the step size plays a vital role as it controls the magnitude of oscillations near the optimal solution. The larger the step size, the faster the convergence but with more variations near the point of optimality whereas smaller step size reach a stable optimal solution with lesser fluctuations near the optimal. As predicted by our algorithm, sensor nodes that have lower



(a) Convergence of source node rates for different sensor nodes with respect to the number of iterations with $\alpha = 0.1$.

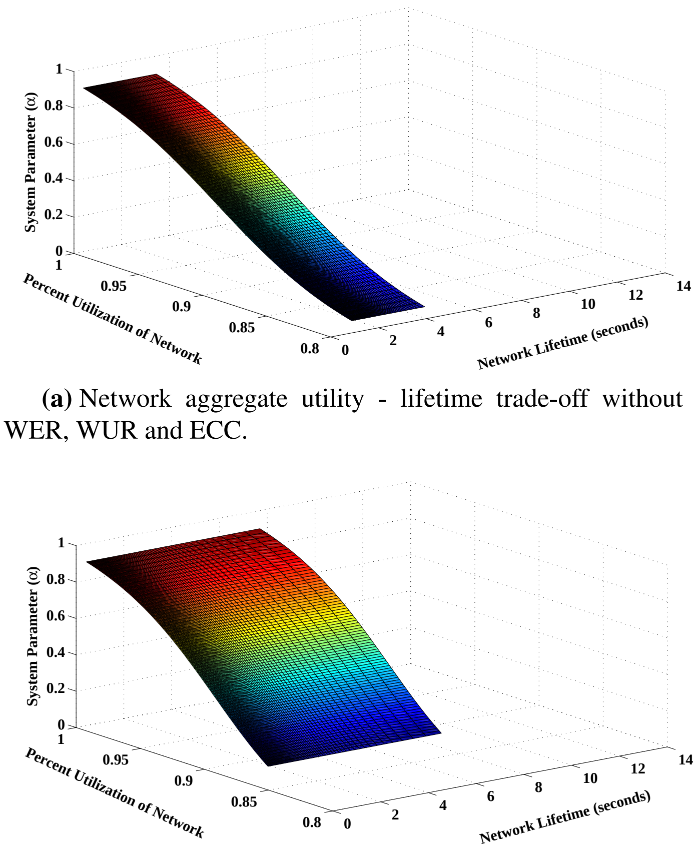
(b) Error in measuring the lifetime with respect to the lifetime approximation coefficient.

Figure 2.6: Simulation plots of convergence of GWSN algorithm.

lifetime $\{i1, i5\}$ are assigned higher rates, whereas nodes with higher lifetime $\{i3, i6\}$ have lower rates being assigned to them. Fig. 2.6b shows the error in measuring the lifetime with respect to the coefficient ε.

$$Errror\ in\ Approximating\ Lifetime = \left| s - \frac{1}{\varepsilon + 1} s^{\varepsilon+1} \right| \tag{2.33}$$

According to Appendix A, if the coefficient ε is large enough then the lifetime approximated by (2.24) is the maximum lifetime. Fig. 2.6b validates the point, as it can be seen that at $\varepsilon = 10$, we get less than 10% error in measurement of lifetime. For our



(a) Network aggregate utility - lifetime trade-off without WER, WUR and ECC.

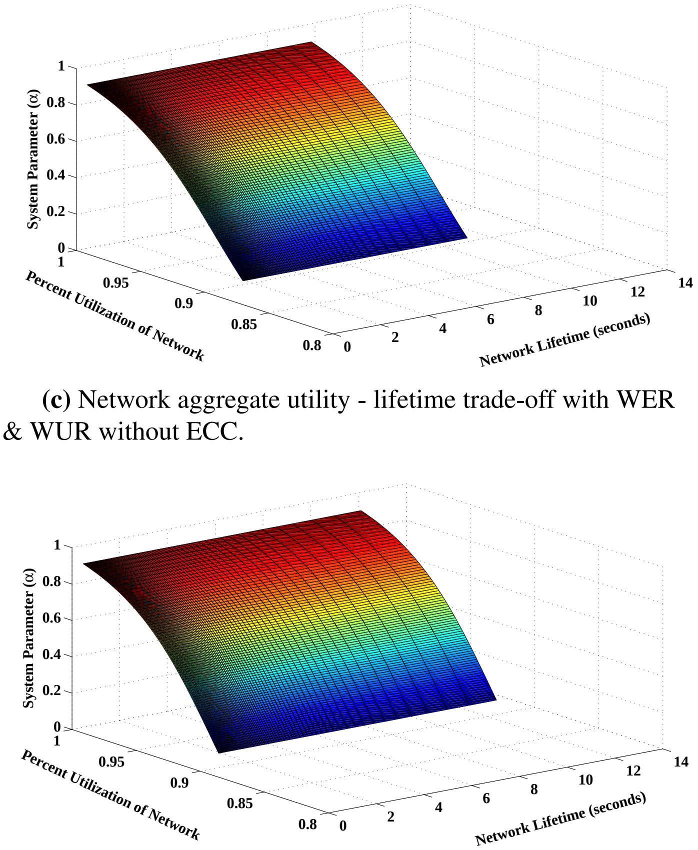
(b) Network aggregate utility - lifetime trade-off with WER and without WUR & ECC.

Figure 2.7: Simulation plots of network aggregate utility - lifetime trade-off for different α.

Algorithm, we have initialized the value of ε as 20 with less than 5% error in lifetime prediction.

2.4.2 Utility and Lifetime Trade-off with WEH and WUR Constraints

The impact of the system design parameter $\alpha(t)$ is shown in Fig. 2.7a, 2.7b & 2.7c. $\alpha(t)$ is varied between 0.1 to 0.9. The network utility is computed as $(\sum_{i=1}^{6} log_2(R_{ij}P_s))$ which is the aggregate utility of all the nodes not including the sink node $s1$. The aggre-

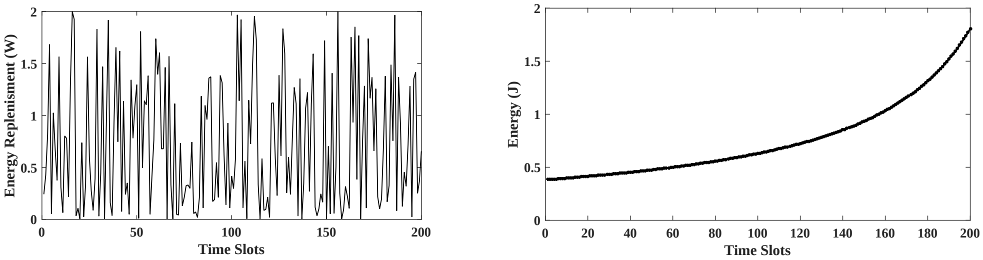


(c) Network aggregate utility - lifetime trade-off with WER & WUR without ECC.

(d) Network aggregate utility - lifetime trade-off with WER, WUR & ECC.

Figure 2.7: Simulation plots of network aggregate utility - lifetime trade-off for different α.

gate utility have been normalized with respect to the maximum utility of the network. Fig. 2.7a shows that the network lifetime decreases and the utility increases as the increment of α. On the contrary, we can observe that as the weighted system parameter α decreases, the corresponding optimal network lifetime increases. It can be seen in Fig. 2.7b that the lifetime increases to 8.5s from 4.5s. Fig. 2.8a shows the harvested energy profile from (2.18) for the farthest node in the network. Replacing the optimal s^*_{ij}, R^*_{ij} in (2.30), $P^C_{H_i}(t)$ is found using $f^{-1}\left(g(s^*_{ij}, R^*_{ij})\right)$ as shown in Fig. 2.8b. Further, if wake-up radio scheme is applied with energy harvesting, the lifetime increases to



(a) Replenishment profile for harvested energy.

(b) Energy resource allocation.

Figure 2.8: Energy harvesting profile and allocated energy plots.

$\sim$10s as in Fig. 2.7c. The network utility of the system also increases to 0.87 with energy harvesting and 0.97 with both harvesting and WUR. Hence, based on the desired performance, designer can chose the value of α and solve the set of equations for optimal lifetime and source node rates.

2.4.3 Impact of Error Control Coding on Performance and Lifetime

Fig. 2.7d shows the utility-lifetime trade-off with error coding applied. The system lifetime is further increased as compared to Fig. 2.7a-(c), to 14s and the network is more utilized at 91%. To visualize the impact of error coding on the performance of the system, we plot the network lifetime versus the packet loss rate P_e^i at $\alpha = 0.1$. Fig. 2.9a shows the plot of network lifetime for different cases with packet loss rate varying from 0 to 20%. For a packet loss rate between 10% to 20% ,the network lifetime increases more than 3 times with only energy harvesting and wake-up radio scheme. Whereas with the coding scheme applied, it doubles further giving a 6 times improvement. We evaluate the network lifetime of nodes $\{i1, i3, i5, i6\}$, where $\{i1, i5\}$ act as only sensor nodes and $\{i3, i6\}$ act as both sensor and relay node. The network lifetime is shown in Fig. 2.9b versus the system parameter α incorporating harvesting and coding at packet loss rate of 20%. As expected from (2.25), the lifetime of node $i1$ is the least. Relaying of data from $i5$→$i6$ improves the lifetime of node $i5$. Nodes $i3$ and $i6$ have a huge improvement in their lifetime owing to their proximity to the sink node from where they harvest energy according to (2.18). Even though the total energy consumption is increased, the harvested energy increase is sufficient enough to boost its lifetime.

2.4.4 Effect of Energy Harvesting and Error Correcting Codes on TelosB Sensor Node

For analyzing the effect of our error correcting codes performance on node lifetime, we have taken real time sensor energy cost from [110] for different sensors as shown in Table 2.3. The Table shows different commonly used sensing devices, their E_{PR} and E_{SN} energy cost normalized w.r.t communication energy E_{comm} for common sensor mote **TelosB** (TelosB is a IEEE 802.15.4 compliant sensor mote that runs a TinyOS operating system with a CC2420 radio.). The battery power is taken as 9000 milli-Amphere-Hour (capacity of 2 standard $1.5-volt$ batteries used in sensors). Fig. 2.10a is drawn for RRNS, BCH, and ARQ for a packet loss rate of 20% showing the estimated lifetime in days for the **TelosB** mote versus the total average power consumption P_i from (2.13). For low power sensors i.e $acceleration, pressure, light, proximity$ given in Table 2.3, TelosB motes lifetime increases by ∼1.7 times with BCH error scheme and more than ***doubles*** with RRNS error scheme. Whereas for power hungry sensor such as $Temperature$, the processing energy is higher, thus overpowering the effect of small number of retransmissions in error coding schemes. One of the major overheads of error correcting codes in addition to transmission and reception of redundant bits is the delay associated with encoding and decoding of packets. Let us assume that t^{ARQ} is the total time required for sending the packets to the sink node and receiving an ACK back.

Table 2.3: Energy cost for TelosB mote w.r.t $E_{comm} = 1mW$

Sensors Type & Model No.	$\frac{\mathbf{E_{PR}}}{\mathbf{E_{comm}}}$	$\frac{\mathbf{E_{SN}}}{\mathbf{E_{comm}}}$	**Sensors Type & Model No.**	$\frac{\mathbf{E_{PR}}}{\mathbf{E_{comm}}}$	$\frac{\mathbf{E_{SN}}}{\mathbf{E_{comm}}}$
Acceleration (MMA72600Q)	0.044	0.000027	Proximity (CP 18)	0.047	0.267
Pressure (2200/2600 Series)	0.044	0.00013	Humidity (SHT 1X)	0.043	0.4
Light (ISL 29002 18)	0.047	0.00068	Temperature (SHT 1X)	0.94	1.5

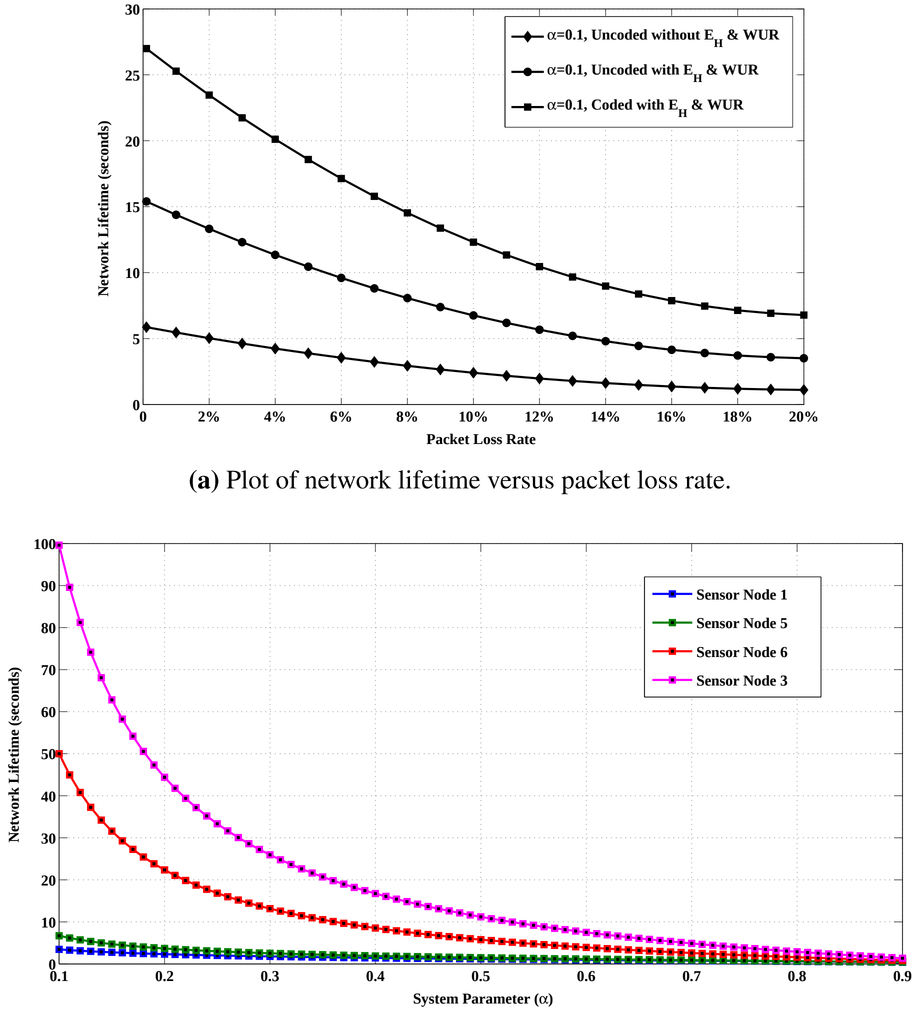
Further, if the decoding latency of a block code like (n,k,e) BCH is t_{dec}^{BCH}. From [101], the decoding latency is given by

$$t_{dec}^{BCH} = (2ne + 2e^2)(t_{add} + t_{mult}) \left\lceil \frac{b}{b_m} \right\rceil \tag{2.34}$$

Here, t_{add} and t_{mult} are time required for additions and multiplications in GF (2^b), and b_m is the number of bits of micro controller used in sensor nodes. In an 8-bit micro controller, t_{add} take one cycle and t_{mult} takes two cycles as computation time. The number of cycles depends on the frequency of the micro controller. RRNS codes of form $((2^{b-1}-1, 2^{b-1}; 2^{b-1}+1, 2^b+1))$ needs $\frac{t^{ARQ}}{(k/n)}$ as the total time required for sending the packets to the sink node and receiving ACK back. The decoding latency depends on the total additions and multiplications in the number of iterations $\binom{\delta}{\beta}$. Depending on the value of β for each step there are 2β multiplications and β additions involved. Further, there are $\binom{\delta}{\beta}$ number of moduli operations involved. Thus, the decoding latency for RRNS codes is

$$t_{dec}^{RRNS} = \left(\binom{\delta}{\beta} t_{add} + \binom{\delta}{\beta} t_{mult}\right) \left\lceil \frac{b}{b_m} \right\rceil + \left(\binom{\delta}{\beta} e\right) \left\lceil \frac{e}{b_m} \right\rceil \tag{2.35}$$

To analyze the effectiveness of the coding schemes, we have plotted the delay in sending one packet of data versus the packet loss rate of 10% and 20%. If we take $t^{ARQ} = 50ms$, from (2.34) and (2.35), delays of BCH$(127,57,11)$ and RRNS$(128,60,32)$ can

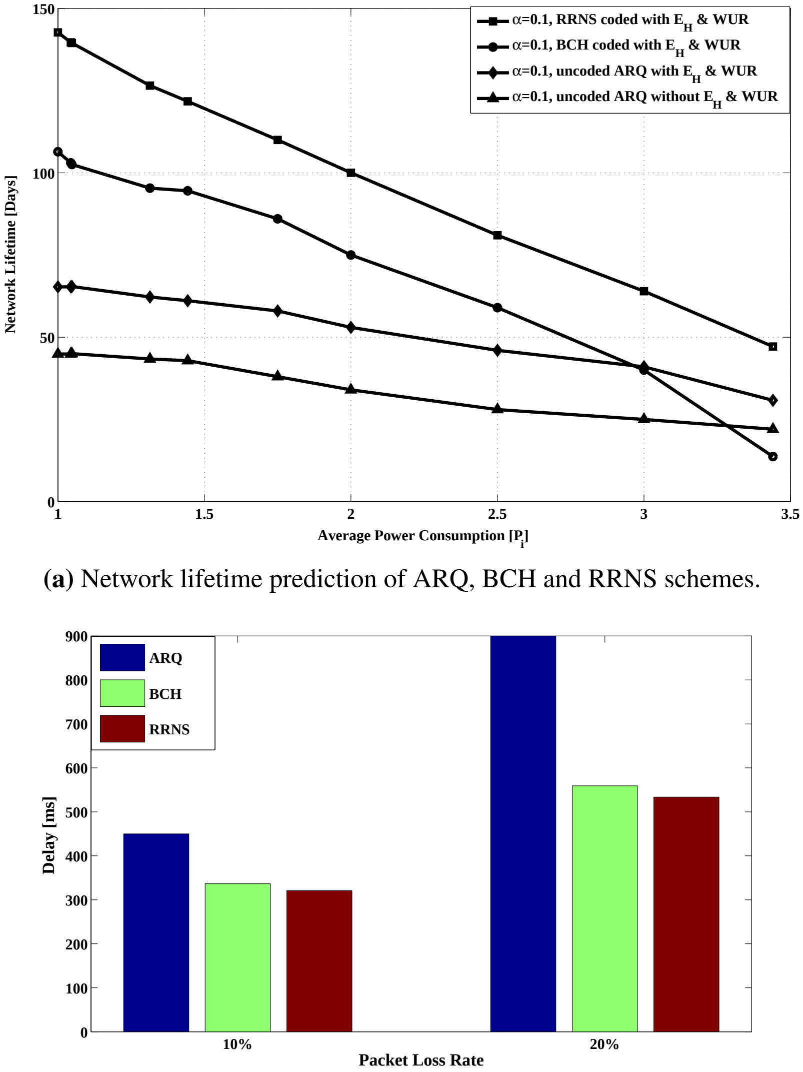


(a) Plot of network lifetime versus packet loss rate.

(b) Network lifetime of different sensor nodes versus system parameter α.

Figure 2.9: Impact of ECC on lifetime of sensor nodes.

be found as $t_{delay}^{BCH} = t^{ARQ} * (n/k) + t_{dec}^{BCH}$ and $t_{delay}^{RRNS} = t^{ARQ} * (n/k) + t_{dec}^{RRNS}$. **TelosB** has a 16-bit microcontroller and its clock frequency is 8MHZ. Fig. 2.10b shows the delay in milliseconds. It can be inferred that the coding schemes outperforms the ARQ sheme in terms of total transmission delay. RRNS scheme has less delay compared to BCH coding due to its better coding rate and faster decoding. It can also be seen that as the packet loss rate increases, the delay gap between the three schemes increases. Thus RRNS has better performance in terms of lifetime improvement as well as lower delay



(a) Network lifetime prediction of ARQ, BCH and RRNS schemes.

(b) Transmission delay performance of ARQ, BCH and RRNS schemes.

Figure 2.10: Impact of WEH & ECC on **TelosB** mote.

as the packet loss rate increases in bad channel conditions.

2.4.5 Green Networking : Reduction in Carbon Footprint

For network to be green, the carbon emissions has to be reduced. The index of measure of carbon emissions is Xgr of CO_2 per year. For each packet loss in the network causes the data server station or the sink node to transmit back $NACK$ to sensor node. The transmitting power (P^S_{TX}) of the data station depends on the fuel type from which the station derives its electrical power, can be either coal or gas. Thus value of X can be either 870 or 370 [47]. (P^S_{TX}) depends on the type of technology used. If we assume that the sink node data station runs on the Long Term Evolution (LTE) network and uses the static micro cell topology with radius 100m. Then from [111] and [47], the carbon footprint generated by sink node is

$$\begin{aligned} F^S_{CO_2} &= P^S_{TX} \cdot (E_{T,h_i} + 1) \cdot 8.64 \cdot 10^{-3} \cdot X[KgCO_2/Year] \\ P^S_{TX} &= \left(\frac{P^D_{TX}}{\mu_{PA}} C_{TX,static} + P_{SP,static} \right) (1 + C_{PS}) \end{aligned} \tag{2.36}$$

Where, the notations are described in Table 2.4. Apart from the sink node, the battery is also responsible for generation of carbon footprint. Typical AA batteries used in sensors have a end of life carbon emission of 4.3 $KgCO_2$ per 30 batteries[112]. Thus, the carbon footprint $[KgCO_2/Year]$ generated by number of batteries used is directly proportional to the total batteries used in a year (B^{year}_u) and is given as

$$F^B_{CO_2} = B^{year}_u \left(\frac{4.3}{30} \right) [KgCO_2/Year], \quad B^{year}_u = \frac{365}{T_{network}} \tag{2.37}$$

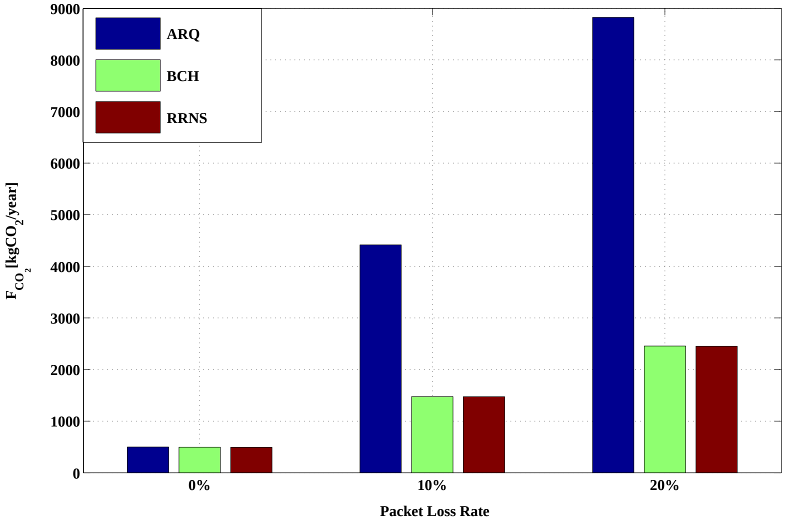


Figure 2.11: Plot of packet loss rate versus carbon footprint

Table 2.4: LTE micro base station based sink node power model parameters

Parameter	Description	Value
P_{TX}^{D}	Power consumed by sink node base station server	2 W
μ_{PA}	Power Amplifier efficiency	20%
$C_{TX,static}$	Static transmitted power	0.8
$P_{SP,static}$	Static signal processing power	15 W
C_{PS}	Power supply loss	0.11

The total carbon footprint (F_{CO_2}) is therefore the sum of carbon footprints in (2.36) and (2.37). To show the effectiveness of using ECC, WEH & WUR, we plot F_{CO_2} for different packet loss rate of $(0, 10, 20)$. We take X=370, the fuel for production of electricity as gas. The $T_{network}$ for different schemes ARQ, RRNS and BCH are taken from Fig. 2.10a at P_i=1mW. Fig. 2.11 shows the carbon footprint at different schemes. It can be seen that as the packet loss rate increases, the carbon footprint is tremendously reduced for RRNS and BCH. It is ∼2.5 times lesser kgCO_2 per year at 10% packet loss and $\sim$4 times lesser kgCO_2 per year at 20% packet loss. So, as the channel goes bad, the carbon emissions for normal scheme like ARQ increases tremendously, whereas incorporation ECC and harvesting the network becomes more greener.

Chapter 3

Energy-efficient and Distributed Data-Aware Routing and Clustering Protocol

3.1 Introduction

In this chapter, we investigate a cross-layer approach that will provide interaction between different layers in terms of energy efficient transmissions w.r.t data-awareness, energy harvesting and varied data-demand topology. The main pitfalls of the algorithms delineated in Chapter 1-Section 1.3 w.r.t energy consumption and network lifetime are, energy consumed in cluster head (CH) selection at each round, assuming nodes in always ON state [113], and limited battery capacity of energy constrained sensors [114]. Thus it is required to come up with a protocol specifically for IoT systems. Hence, we have proposed a distributed data-aware energy-efficient clustering protocol for IoT (DAEECI) which includes data awareness, RFID based CH selection and RF energy harvesting using a Power Management Unit(PMU). The rest of the Chapter is organized as follows. In Section 3.2, we describe IoT network model. Section 3.3 describes our DAEECI protocol. Section 3.4 analyzes our simulation results.

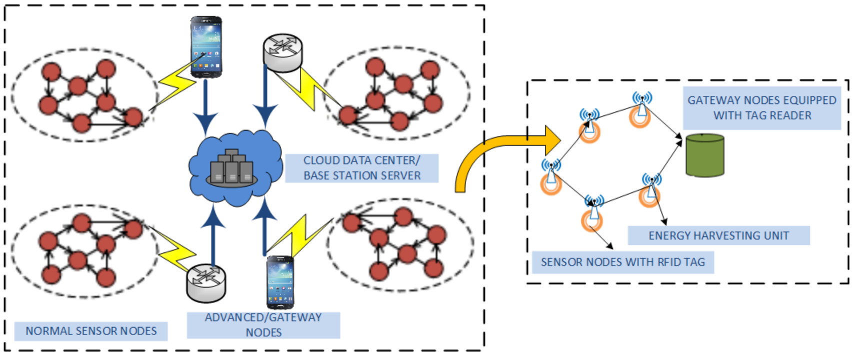


Figure 3.1: Data-aware RFID tag based IoT architecture.

3.2 IoT Network Model: Cluster Head Selection and Energy Cost Formulation

The IoT system taken here is depicted in Fig. 3.1. The network is a random distribution of N_{tot} sensor nodes in a square area of side X meters and gateway nodes K used for data aggregation and routing to BS. The nodes are differentiated based on their initial energy as advanced and normal sensor nodes. Advanced nodes have a times more energy than normal nodes and are also known as gateway nodes (K), as they route data to the base station. Thus the total nodes in the system are $(N_{tot} + K)$. Each cluster has one gateway node based on minimum distance, as their CH. Let E_B be the initial battery energy of the normal node. Let K be the number of distributed clusters that service all nodes and have one gateway node per cluster for data routing to base station. All the cluster heads send the aggregated data from sensor nodes they service to BS server. The BS server is user driven based on data request from different user generated applications.

Let $E_{tot-cls}$ is the total energy of the clusters given as

$$E_{tot-cls} = N_{tot} * E_B + K * E_B * (1+a) \tag{3.1}$$

3.2.1 Active RFID Tag Based Cluster Head Allocation

The cluster head selection is one of the major drawbacks of current clustering algorithms. In LEACH [50] and DEEC [53] algorithm, cluster head selection is divided into rounds, where each node randomly decides whether to become a cluster head based on a threshold $T_i(s)$ computed by apriori decided probability p_i.

$$T(s_i) = \begin{cases} \frac{p_i}{1-p_i\cdot\left(r\ mod\left(\frac{1}{p_i}\right)\right)} & ,if\ S_i \in G \\ 0 & Else \end{cases} \tag{3.2}$$

where, r is the current round number, and G is the set of nodes that have not been cluster-heads in the last n_i rounds $(p_i = \frac{1}{n_i})$. Let the energy dissipated in a round (E_{round}) is adopted from the radio model in [53] as

$$E_{round} = L\begin{pmatrix} (N_{tot}+K)(E_{rx}+E_{tx})+N_{tot}E_{DA} \\ +K\varepsilon_{amp}d^4_{toBS}+N_{tot}\varepsilon_{fs}d^2_{toCH} \end{pmatrix} \tag{3.3}$$

where, E_{DA} is the data aggregation cost expended in CH, d_{toBS} is the average distance between CH to BS, d_{toCH} is the average distance between cluster members to CH, L is the number of bits to be transmitted, ε_{amp} is the energy consumption of transmitter amplifier circuit, E_{tx} is the transmitted energy consumed per bit and E_{rx} is the received energy per bit, ε_{fs} is the free space parameter. From (3), it can be inferred that $L*(N_{tot}+K)*(E_{tx}+E_{rx})$ and $L*N_{tot}*\varepsilon_{fs}*d^2_{toBS}$ are the energy consumed for CH selection and routing data from nodes to CH, respectively.

Therefore, to save the energy consumed in CH selection, we propose to incorporate active RFID tags coupled to member nodes and a tag reader at the gateway node. The conceptual topology is depicted in the expanded view of the WSN in Fig. 3.1. RFID is an emerging automatic identification technology in which information is carried by radio waves. RFIDs are classified as passive, semi-passive, or active [96]. Passive RFID tags function without a battery, has almost infinite lifetime but can operate in the range of only couple of $centimeters$. Whereas, an active RFID [115] can be read at distances of 100 m or more, greatly improving the utility of the device, but it is battery powered and has shorter life. The use of active tags with sensor nodes and a tag reader at the gateway will eliminate the need of choosing the CH till the gateway nodes are exhausted of their energy. Nodes collect data from the environment and send them to the RFID reader which in turn sends it to the BS. From the BS data are sent to the cloud in order to provide it to the user through the services initiated by the cloud. With the evolution of tags like CC2650 SensorTag[1] which operate with 2.4GHz transmission and supporting technologies such as Bluetooth, ZigBee and IPv6, it is feasible to incorporate the model for IoT WSN systems. Using our proposed method, as the tag reader reads the sensed data from the tags, computation for routing data to the CH is not required. The energy consumed for CH selection becomes $L*(N_{tot}*E_{rx}+K*(E_{tx}+E_{rx}))$. This happens till all the gateway nodes die in which case the routing follows energy consumption in (3) again.

[1] Available[online]:http://www.ti.com/lit/ug/tidu862/tidu862.pdf

3.2.2 Data Aware Processing

Sensors in IoT systems are not always active. There are two types of data request from users, one is periodic monitoring type of application such as warehouses and industrial control and another is on demand processing such as home survielience, temperature control, smoke and water detectors. Thus data awareness of sensors is critical to its longetivity. Sensors that service users periodically have to be in *active* state all the time whereas the sensors sending data sporadically can be kept in *sleeping* state for most of the time. They can be woken up from sleep by asynchronous triggering on their pins when a certain threshold is crossed. An efficient approach to address this is $duty-cycling$, in which the receiver on-demand switches between active and sleeping states. Among the different categories of $duty-cycling$, namely *synchronous*, $pseudo-asynchronous$ and pure *asynchronous*, latter provides the most efficient solution in terms of energy consumption [43]. In the *asynchronous* approach, the sensor device is in deep sleep mode and only wakes up when signalled by the BS or its neighbouring devices through an interrupt command generated by a low-power wake-up radio (WUR). Let the transmitted energy consumption of sleeping nodes is only α percent of E_{tx}, where $\zeta \leq \alpha \leq 1$, ζ is a small number close to 0. Let there be n_s number of sleeping nodes in the system. Therefore, the E_{round} is as follows

$$E_{round} = L \begin{pmatrix} (N_{tot} + K)(E_{rx} + \alpha E_{tx}) + N_{tot} E_{DA} \\ + K \varepsilon_{amp} d_{toBS}^4 + N_{tot} \varepsilon_{fs} d_{toCH}^2 \end{pmatrix} \tag{3.4}$$

When α=1, all the nodes are awake and transmitting data read by the tag reader. But when the data demand is low, the α value is small providing tremendous energy saving in the system.

3.2.3 RF Energy Harvesting

Energy harvesting is a promising remedy to cope with the energy challenge. The recent technology trend in energy harvesting provides a fundamental method to prolong battery longevity of sensor devices [116]. In RF energy harvesting (EH) circuit, the antenna receives the transmitted radio waves and converts the received RF energy into a stable direct current (DC) energy source to supply the sensor device. Energy harvesting depends on the distance from the harvesting source. If the EH circuit is deployed on the sensor devices with a power management unit, it can harvest RF energy from the transmitted electromagnetic waves of the transmitter circuit of its own as well as nearby nodes, gateway nodes and BS [116][43]. In practice, the conversion from the received RF power to the usable DC supply comes with a certain amount of power loss in the matching circuit and in the internal circuitry of the power converter. The power conversion efficiency (η) of the converter is the ratio of the generated usable DC output power to the input RF power. State-of-the-art RF-to-DC converters (also known as rectifiers) can achieve high η values, up to 70% or more [116]. η is an indication of the amount of harvested energy that is available for the sensor device. Here, we assume that the energy harvested by the nodes vary randomly between $0<\beta\leq1$ of total harvested energy $E_H(t)$. $E_H(t)$ is the maximum harvested energy and is taken as η times the battery energy per unit time t. At short range, it is possible to harvest a tiny amount of energy from a typical WiFi gateway router transmitting at a power level of 50 to 100 mW. The RF energy which reaches the sensor node is efficiency η multiplied by the energy harvest factor β and is approximately 0 to 5% of the total transmitted power of an antenna for a distance in the range of tens of meters [117]. This amount of power is best used for devices with low-power consumption and long or frequent charge cycles. Typically, devices that operate for weeks, months, or years on a single set of batteries are good candidates for being wirelessly recharged by RF energy. In some applications simply augmenting the battery life or offsetting the sleep current of a microcontroller is enough to justify adding RF-based wireless power and energy harvesting technology. [117]

3.2.4 Power Management Unit

Power management unit (PMU) is an integral part of any energy harvesting system. PMU is in charge of controlling the storage of the harvested energy. It also manages the distribution of the available energy among different consumers in an effort to maximize the lifetime of the device while maintaining a high quality of service (QoS). We extend the architecture of the PMU proposed in [118] to enable effective cooperation with the EH unit. The architecture proposed, is an event triggered/asynchronous scheme based on the signal generated by a wake-up radio [2]. The PMU architecture also detects/pre-empts the failure of a node in the event of energy deficiency.

The detailed block diagram of the PMU for the EH sensor device is shown in Fig. 3.2. The PMU starts its operation by a trigger signal generated by the WUR unit of WEH unit $(INTERRUPT)$. The PMU first activates the main transceiver through $(ON/\overline{OFF})$ and then sends a wake up signal $(WAKE\ UP)$ to the sensing unit to start its operation. The sensing unit toggles the $STOP/\overline{RUN}$ to high, signifying the PMU that it is in running mode. The REQ signal indicates the amount of energy required by the sensing unit. The signals BAT and SE indicate the amount of energy left in the battery device and the EH unit storage element respectively. Accordingly, the PMU activates switches SW_1 through signal $SENSE$ to fulfill the power requirements of the sensing unit. The sensor unit is in charge of sensing, data processing via a microprocessor (µp)

[2] Section 2.2

and finally transmitting them to a low-power transceiver based on Bluetooth, WiFi, IEEE 802.15.4, Zigbee, etc. The sensor devices require a minimum power of P_{Dmin} to operate in sensing mode. When the energy in the battery device goes below a certain threshold $P_{TH} < 1.5P_{Dmin}$, the PMU sends a *RECHARGE* command to the storage element by activating switch SW_2 of WEH unit to charge the battery. When the energy level of the device remains $1.1P_{Dmin}$, the device sends out of service (OUS) command to the sink node, signaling that it goes out of the service till it recharges itself again to more than $1.5\ P_{Dmin}$. The sink node in turn sends a stop all service (*SAS*) signal to the device. The sink node/gateway puts the device out of the sensing service loop but keeps transmitting RF energy for harvesting. As the device is ready for service again, it sends a *READY* signal to the sink node which in turn gives resume all services (*RAS*) signal to the device.

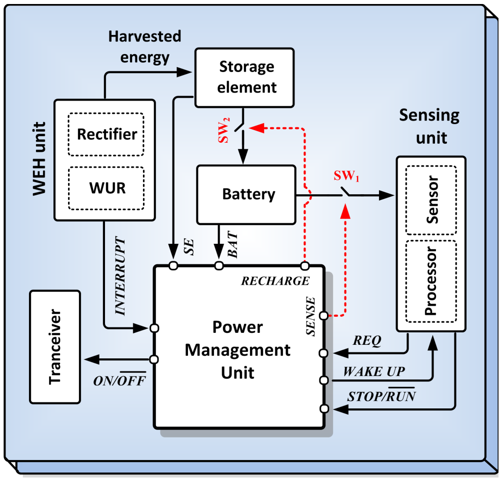


Figure 3.2: Proposed power management unit.

3.3 Data Aware Energy Efficient Distributed Clustering Protocol for IoT

In this section, we present the detail of our Data aware energy efficient distributed clustering protocol for IoT (DAEECI) protocol. DAEECI uses similar function of initial $(E_{tot-cls})$ and residual energy $(E_i(r))$ level as in [53] of the nodes to select the cluster-heads at each round. To avoid that each node needs to know the global knowledge of the networks, it estimates the ideal value of the network life-time to compute the reference energy $(\bar{E}(r))$ consumed by a node in a round. Our DAEECI divides the problem into different user cases based on data awareness (i.e. either α is 1 for periodic data sensing or $0 \leq \alpha < 1$ for sparse data sensing) and percentage of gateway nodes present in the IoT system (K is high or low). The normal nodes are assumed to have their dedicated RF energy harvesting circuit. The algorithm is summarized as in **Algorithm 1**.

3.4 Results and Analysis

In this section we provide performance evaluation of our DAEECI algorithm. We define a network area of $100 * 100\ m^2$. The simulation parameters are provided in Table 3.1. The performance metrics taken in the simulations are *number of Alive nodes*, *Residual energy of nodes* and *Packets sent to BS*. We used Matlab for evaluating our algorithm with other known protocols. In our scenario, we have evaluated the system with four different cases based on α and K for 10000 rounds. For all the cases, we assume that the advanced nodes (gateway nodes) have $a = 3$ times the more energy than the sensor nodes. The cases are as follows:

Case 1 : $a = 3$, $N_{tot} = 100$, $K = 30$, $0.8 \leq \alpha \leq 1$, noE_h. Here, the data demand on sensor nodes is high with no energy harvesting present.

Case 2 : $a = 3$, $N_{tot} = 100$, $K = 30$, $0.8 \leq \alpha \leq 1$, E_h. Here, the data demand on sensor

Algorithm 1: Data aware energy efficient distributed clustering protocol

```
1 **Initialize** :
2 Uniformly distributed region X*X.
3 $N_{tot}$, $K$, $E_{DA}$, $E_{tx}$, $E_{rx}$, $\varepsilon_{fs}$, $\varepsilon_{amp}$, $E_h(t)$, $L$.
4 $d_{toCH}=\frac{X}{\sqrt{2*K*\pi}}$, $d_{toBS}=0.765*\frac{X}{2}$.
5 **Start** :
6 The average energy of $r^{th}$ round is given as

      $\overline{E}\left(r\right)=\frac{1}{\left(N_{tot}+K\right)}E_{tot-cls}\left(1-\frac{r}{R}\right)$    (3.5)

  where, $R$ denotes the total rounds and is defined as

      $R=\frac{E_{tot-cls}}{E_{round}}$    (3.6)

  If nodes have different amounts of energy, $p_i$ of the nodes with more energy
  should be larger than $p_{opt}$ (optimum probability of choosing a cluster head).
7
      $p_i=\begin{cases}\frac{(1+a)p_{opt}E_i(r)}{\overline{E}(r)}, \sum\limits_{K}E_K\left(r\right)>0\\ \frac{p_{opt}E_i(r)}{\overline{E}(r)}, \sum\limits_{K}E_K\left(r\right)\leq 0\end{cases}$    (3.7)

  The energy dissipated in a round $E_{round}$, incorporating total cluster energy
  $\sum\limits_{K}E_K\left(r\right)$, data awareness factor $\alpha$ and RF energy harvesting factor $\eta$ is given as
8 $\longrightarrow$***for*** $\sum\limits_{K}E_K\left(r\right)>0$

      $E_{round}=L\left(\begin{array}{l}N_{tot}E_{rx}+K\left(E_{rx}+\alpha E_{tx}\right)+\\ N_{tot}E_{DA}+K\varepsilon_{amp}d_{toBS}^4\end{array}\right)-N_{tot}\beta E_H(t)$    (3.8)

  $\longrightarrow$***for*** $\sum\limits_{K}E_K\left(r\right)\leq 0$

      $E_{round}=L\left(\begin{array}{l}N_{tot}\left(E_{rx}+\alpha E_{tx}\right)\\ +K\left(E_{rx}+\alpha E_{tx}\right)\\ +N_{tot}E_{DA}+K\varepsilon_{amp}d_{toBS}^4\\ +N_{tot}\varepsilon_{fs}d_{toCH}^2\end{array}\right)-N_{tot}\beta E_H(t)$    (3.9)

  Thus we can find the lifetime of network $R$ by putting (1), (8) and (9) in (6).
9 **End**
```

Table 3.1: IoT simulation parameters

Parameters	**Value**
Network Size	100x100 m^2
Sensor nodes N_{tot} in each Cluster	100
Initial battery energy of nodes E_B	0.5 J
Packet Size L	4000 bits
E_{tx} and E_{rx}	50 nJ/bit
ε_{fs}	10 nJ/bit/m^2
ε_{amp}	0.0013 pJ/bit/m^4
E_{DA}	5 nJ/bit/signal
p_{opt}	0.1
α and β	$rand(0,1)$
η	0.4

nodes is high with energy harvesting present.

Case 3 : $a = 3$, $N_{tot} = 100$, $K = 30$, $0.2 \leq \alpha \leq 0.4$, E_h. Here, the data demand on sensor nodes is low with energy harvesting present.

Case 4 : $a = 3$, $N_{tot} = 100$, $K = 50$, $0.8 \leq \alpha \leq 1$, E_h. Here, the data demand on sensor nodes is high with energy harvesting present. Moreover, there are higher number of gateway nodes present compared to previous three cases. Fig. 3.3 represents the

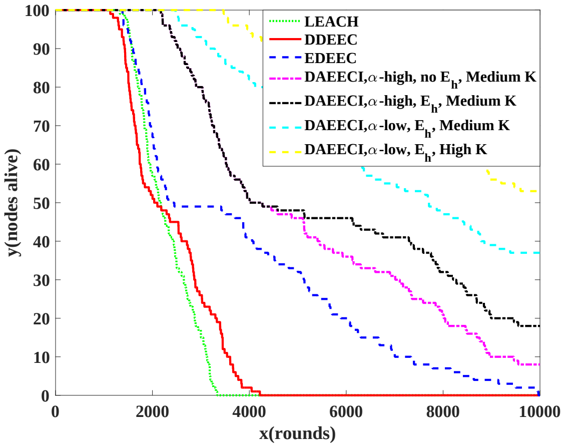


Figure 3.3: Number of alive nodes in an IoT system versus number of rounds.

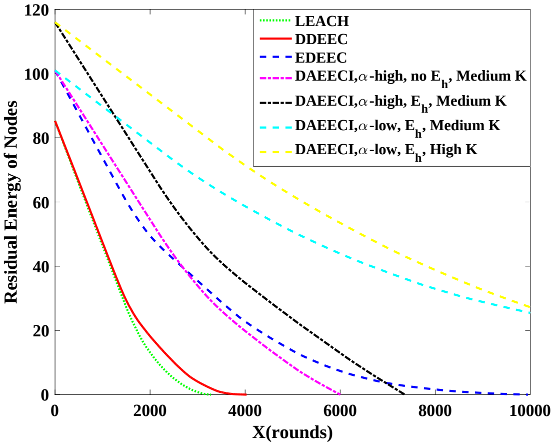


Figure 3.4: Total residual energy of nodes in the IoT architecture.

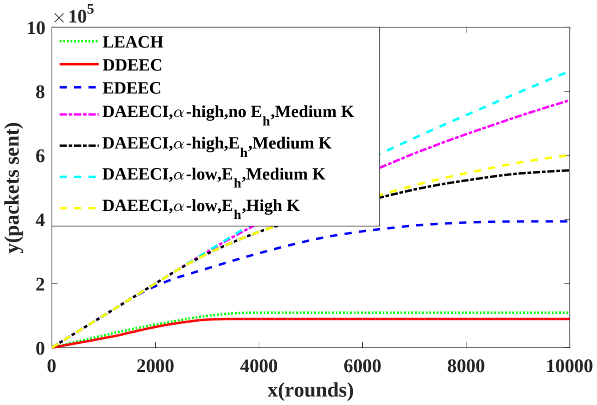


Figure 3.5: Total packets delivered to the base station server from nodes .

number of nodes alive during the lifetime of the network. It clearly shows that by introducing RFID based cluster selection and data aware processing, the lifetime improves significantly of the IoT network. LEACH and DDEEC perform poorly as all its nodes are dead by the end of 4000 rounds. Our DAEECI algorithms performance without energy harvesting is comparable to the EDEEC algorithm. With the introduction of E_H, our method outperforms the EDEEC method as around 20% nodes are still alive at the end of 10000 rounds. It can also be inferred that the low data demand of the sensors in case of sparse sensor data requirement almost boosts up the lifetime of the system by

100%.

Fig. 3.4 represents the sum of residual energy of all the nodes in the network. The DAEECI algorithm incorporating RFID tags and data awareness again allows nodes to have higher residual energy compared to the LEACH, DDEED and EDEEC methods. The EDEEC and higher data demand systems DAEECI almost perform similarly. Fig. 3.5 represents the packets sent to the BS from the cluster heads. The notable thing to infer is that low data demand reduces the amount of packet sent to the BS, whereas irrespective of the high data demand (high α), our algorithm still delivers more packets to the BS than other state-of-the-art methods.

Chapter 4

Energy-Efficient, PUF-Based Security Design for Internet-of-Things (IoT) Infrastructure

4.1 Introduction

As IoT devices are deployed in unmonitored, unsecure environments, secure IoT systems are needed, based on security algorithms, whose hardware implementation provides a balance between security and energy efficiency, in order to also support communication among large number of IoT nodes. Embedded security implementation of a physically unclonable function (PUF) is described in this chapter. A PUF models a (partly) physical system S that can be challenged with randomly generated challenges $c \in C$, upon which it reacts with corresponding responses $r \in R_C$. Furthermore, in contrast with conventional digital architectures, the PUF-based approaches intertwine cryptography and sensor properties, making the attack to such systems more challenging.

Metrics like *uniqueness*, *randomness*, and *bit-aliasing* [119][120] have been used to evaluate PUF performance. They are described below.

Uniqueness: Given two PUFs (*i* and *j*) of the same optical sensor type, each having an *l*-bit response, let r_i and r_j define their *responses* to a given *challenge c*. The mean uniqueness among a group of *p* PUFs is

$$Uniqueness = \frac{2}{p\left(p-1\right)}\sum_{i=1}^{p-1}\sum_{j=i+1}^{p}\frac{HD\left(r_i,r_j\right)}{l}\times 100\% \tag{4.1}$$

where HD is the hamming distance from different instances of PUF chips of the same sensors and *p* is the number of PUFs. Ideally, this value is around 50%.

Randomness: This is measured by the probability of obtaining a $'0'$ or $'1'$ in the PUF response to a challenge. Ideally, it should be 50%, for a PUF response to be considered as unbiased. It is obtained by computing the b^{th} bit ($'0'|'1'$) of the *l*-bit response of the p^{th} PUF.

$$Randomness = \frac{1}{l}\sum_{b=1}^{l} r_p \times 100\% \tag{4.2}$$

Bit-aliasing: Due to changes in ambient operating conditions, like temperature and power supply voltage, the response to a challenge may be slightly varying. To compute this, the mean of flipped bits among responses is found. Generally, it is best to calculate the worst-case scenarios at the boundary conditions of operating parameters. Ideally, the error should be 0%, but in actual measurements this should be as small as possible.

4.1.1 Security Requirements

IoT has various applications in military, e-health, banking etc. Therefore, security and privacy issues are becoming major concerns in the operation of IoT. Attacks on IoT may include eavesdropping, Denial of Service (DoS), and Man-in-Middle [16]. DoS happens when unauthorized access to the system occurs. Eavesdropping is an attack on confidentiality, where intruders may listen to the communication between sender and receiver. Adversaries who get hold of the key may appear as genuine senders. This type of attack is known as Man-in-Middle attack and may occur when the key can be predicted easily, thus helping the adversary to break into the system. Various parameters are used to measure the robustness, reliability, and integrity of a IoT system. As our design uses a sensor PUF, we will first define metrics related to the robustness of PUF implementation against adversaries [15]. Then, we will define metrics related to the security of an IoT system secure [16]. Let $F : C \rightarrow R : F(C) = R$, $c \in C, r \in R_C$ be a function that maps the challenge/response pairs of a PUF system. Next, we discuss a set of possible attacks that can be attempted against a PUF.

Frequency Prediction Attack (Also known as modeling attack): In this attack, the adversary collects previous output values and tries to make a probability distribution model to predict the future outputs O_i as $P(O_i = 0/1)$ [121]. The randomness property of the PUF has to be satisfied to resist this type of attacks.

Replay Attack: In this attack, the adversary tries to predict the output by studying the outputs that have similar inputs. If the hamming distance between subsequent input output pairs form a polynomial distribution, as defined in the uniqueness PUF property, generally the associated cipher would resist this attack [121].

Cloning Attack: In this type of attack, the adversary tries to clone the original PUF to replicate the challenge/response behavior, as in the original PUF. So, if F is transformed to F' with a very high probability, but $F(R_C) \neq F(R_{C'})$, then the PUF is resistive from such type of attacks.

Side-Channel Attack: A PUF may be attacked passively by using side-channel information, such as power consumption or electromagnetic radiation emanated from a chip containing a PUF. Generally, this type of attacks changes the physical properties of the PUF.

Apart from successfully resisting the attacks on the PUF circuits, the IoT system also needs to provide successful protection from cyber attacks on the internet. Requirements for implementing security in IoT-based applications [122] include:

Device Authentication: When the device is plugged into the network, it should authenticate itself prior to receiving or transmitting data. Just as user authentication allows a user to access a network based on user name and password, machine authentication allows a device to access a network based on a similar set of credentials stored in a secure gateway server. Once the device is recognized as authentic, the data transfer happens.

Confidentiality and Privacy: Latest technologies can be used to gain access to the message sent from the source to the destination. Therefore, it needs to be hidden from the adversaries and an end-to-end secrecy of the data must be maintained.

Data Integrity: In addition to confidentiality and privacy, integrity is also an important security factor during the transmission of data in IoT. An adversary can insert some malicious code or data into the system to corrupt it. The altered data may reach the destination node and prove fatal to safety-critical IoT systems, like e-health and banking. Therefore, an integrity mechanism is crucial in protecting the original data from external attacks.

Access Control: Access control ensures that the intruder has as minimal access to other parts of the system as possible. It is important to authenticate the device at regular intervals to stop an intruder from gaining access to the system. Sensors which are not authenticated are excluded from the system network.

In a previous paper[123], we proposed a PUF-based cryptographic system that is based on optical sensors used in e-health systems, such as heart rate monitors and pulse oximeters [124], using photodiodes. In this Chapter, we analyze the intricate details of the internal circuitry and have built the prototype of the system. A generic cryptographic system is proposed for IoT applications, as infrared optical sensors find applications in various fields, like defense, e-health, banking, and home automation[125]. The design we propose is different from all designs mentioned in the introduction as it does not exploit digital variations [72–74]. Instead, our approach leads to Strong PUF with integrated control logic to further consolidate the security of the system.

The rest of the Chapter is organized as follows. In Section 4.2, we describe the proposed method and algorithms. Section 4.3 presents a prototype PUF circuit design and the effects of noise constraints and energy consumption in reaching an optimal design point. In Section 4.4, we analyze the simulation and measurement results.

4.2 Proposed Security Approach and Protocol

Among the biggest challenges in the design and implementation of a PUF-based systems are:

1. Finding a physical property of the device, whose variations are difficult to predict.
2. Designing large cycles of random-like binary challenges to authenticate the system, so that the authentication process cannot be easily predicted in a short time frame.

3. Encrypting the system through PUF-based digital signature generation, and verifying only through public key information.

4. Requiring minimal circuitry changes in the existing system hardware.

Note that we are using here the optical sensor as a proof-of-concept. The technique can be also applied to other sensors with random-like physical properties. The physical property that we have chosen is the dark current of the photodiode and the large cycles of binary pseudo-random challenge/response pairs (i.e., input-output pairs to and from the target sensing system) generated by quadratic residue property to validate the approach.

The dark current in silicon-based photodiodes depends on the doping concentration of carriers as well as changes in temperature. For a given temperature and operating conditions, the dark current varies due to inherent variation in doping concentration. No two photodidodes can have exactly the same dark current. We have measured and plotted dark current variations for different silicon-based (Si-based) photodiodes at room temperature and operating at wavelength λ = 940 nm. Fig. 4.1 shows the measured value of dark currents in nA (nano-amperes) versus the reverse voltage of photodiodes, varying from 0 to 25 Volts. Our region of measurement spans from 0 V upto the diodes' breakdown voltage. The measurements are shown for photodiodes of the same manufacturer as well as those of different vendors (two from Vishay, two from Everlight, and one from Fairchild). The measurement procedure is explained in detail in the results section.

As the IoT devices are commonly resource-constrained, the computational resources of gateway nodes (cloud server) as mentioned in previous section about IoT architecture are utilized. After the authentication of the device the encryption of the data using

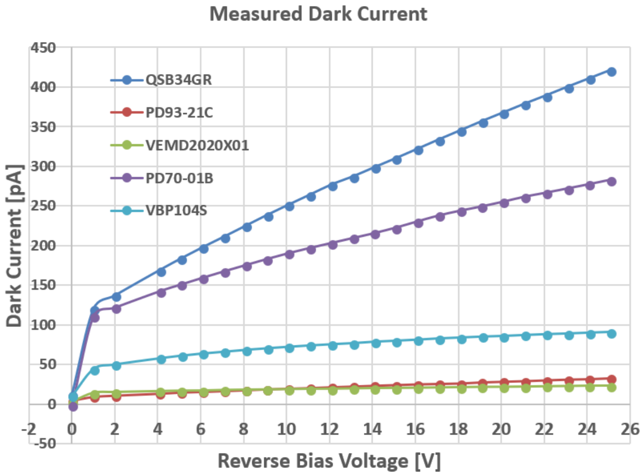


Figure 4.1: The dark current vs. reverse voltage of different silicon PIN photodiodes.

digital signatures follows.

4.2.1 Quadratic Residue based Device Authentication

As the dark current of each photodiode is uniquely varying, we use a quadratic residue based scheme to propose a device authentication protocol. Let a and N be positive integers, with $N \neq 0$. We note the following definition [126].

Definition 1. *Given an integer number $a \in \mathbb{Z}$ and a natural number $n \in \mathbb{N}$ that are relatively prime, then a is called the **quadratic residue** (QR) modulo n, if the congruency $x^2 \equiv a \bmod n$ has a solution, that is, a is a perfect square modulo n.*

In general, the quadratic residues follow a residue cycle starting with an initial seed S_0, which is also a QR modulo n itself. To illustrate this concept, we provide an example in Fig. 4.2 by computing the QRs *mod* 319 (note that in this example, 319 = 29 × 11, that is, we have $p = 29$ and $q = 11$). If we take initial seed S_0 as 16 or 146 which are QRs, i.e., S_0^2 *mod* 319, we achieve the cycles shown in Fig. 4.2.

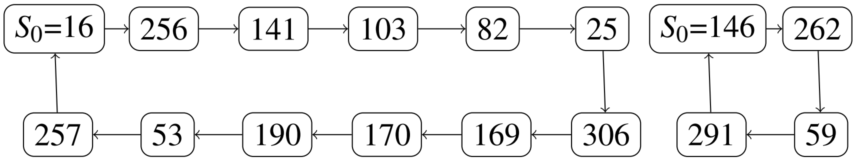


Figure 4.2: Quadratic residue cycles with seeds $S_0 = 16$ & $S_0 = 146$

Algorithm 2: Sensor PUF authentication protocol

challenge/response Pair Generation

(1) The cloud server generates two large prime numbers p and q, and initial seeds S_i∈QR mod $[p * q(= n)]$, $i \in 0,1,2,...,k$. The value of k is determined by the iterations needed to validate the system as decided by the authenticating party.

(2) The server then fills up a mapping table starting from S_0 as shown in Fig. 4.3. After the first seed cycle is complete, it completes the table S_1 as in **step 1** and starts filling the rest of the table. It continues generating seeds till the table is completed for all seeds from S_0 to S_k.

(3) The server randomly chooses values from the mapping table to send to the sensor node and forms a response voltage output pair corresponding to the sent values, using its pre-measured (voltage) values $(n_v(table))$ of dark currents of the photodiode (or in general, any other PUF variable) of the circuit.

Key Generation

(1) Let g < n be a randomly chosen generator of the multiplicative group of integers modulo n (Z_n^*).

(2) Let H be a collision-resistant hash function.

(3) The sensor node's voltage $(n_v(measured))$ w.r.t. dark current is measured corresponding to the QR value sent from the cloud server and hash function of an XOR operation with its ID and the data is performed to generate the public key as P_{key}=H($n_v(measured) \oplus ID \oplus Data$).

(4) The public key P_{key} is then sent back to the cloud through a wireless channel.

Authenticating and Pairing

(1) Upon receiving the P_{key}, the cloud decodes the message using the challenge/response pair table $\widehat{Data}$=H$^{-1}\{P_{key}\} \oplus ID \oplus n_v(table)$ by comparing the values of $n_v(measured)$ with its own values $n_v(table)$. If a satisfying level of confidence is found in the correlation between challenge/response pairs, it sends acknowledgment to the sensor node.

(2) Upon receiving the acknowledgment, the device is authenticated and the pairing is formed. The process is repeated after every defined time interval to re-enforce the integrity of the device.

It can be seen that the two seeds form a residue cycle of lengths 12 and 4, respectively. Note that these two cycles are disjoint, that is, the intersection of the two sets of residue cycles is a null set. This is true in general for any two residue cycles. Similarly, other QR seeds can be randomly chosen and the residue cycles can be formed that would be difficult to predict because of the random nature of the choice [127]. In our approach, since we are using $n = p \times q$, where p and q are odd prime numbers, to determine whether a is a quadratic residue modulo n, one has to know how we have factorized n in terms of its odd primes p and q and then find the solution of the congruence x^2 *mod n*. We will randomly change p and q and thus due to the difficulty of finding p and q, it is computationally time consuming to find x satisfying $x^2 \equiv a \ mod \ n$ [128] [129][130].

The authentication process consists of three different stages. The first stage is the challenge number generation based on QR at the cloud server and sending it to the sensor node using a secure transmission channel. Second stage is the key generation at the sensor end and transmitting it back to the cloud server. The final stage involves decoding of the key at the server and sending back the acknowledgment for pairing. **Algorithm 2** explains the three stages in detail.

4.2.2 IoT PUF Security Encryption through Digital Signatures

We will describe the QR based PUF security variant of the ElGamal digital signature protocol [131] to do encryption of the data. An adversary that can introduce malicious data may cause the system to respond inappropriately. The receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in IoT applications. As many IoT devices are sensors broadcasting observations, cryptographic digital sig-

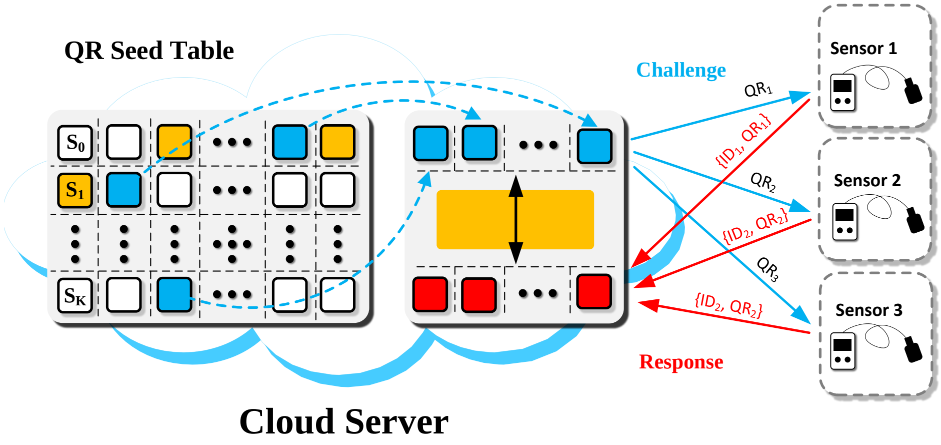


Figure 4.3: Proposed sensor PUF authentication protocol architecture.

natures ensure the integrity of the device's data stream. **Algorithm 3** describes the signature generation process in detail.

4.3 Energy-Efficient Circuit Design

Fig. 4.4a shows the simplified circuit diagram of the sensor node, involved in measurement of dark current for a given challenge value generated by the cloud. Fig. 4.4b shows the details of current-to-voltage conversion circuitry. The sensor node consists of mainly three parts : an IoT sensor processor, a photodiode, and a trans-impedance amplifier (TIA). When the challenge value is received by a processor, the digital value is converted to its corresponding analog voltage (reverse bias of the photodiode) by a digital-to-analog converter (DAC). Then, the dark current generated by the photodiode is converted to voltage by the TIA circuit, which consists of low-offset/low-leakage OpAmp with a gain resistor RF connecting the input and output of the OpAmp. The dark current (typically in the range of 100pA to 1nA) flows through this resistor, creating the voltage (in the range of 1mV to 100mV) at the output of the TIA, which is then amplified by a simple non-inverting low-offset OpAmp, and the amplified voltage

Algorithm 3: PUF-based Digital Signatures

System parameters

(1) The cloud server generates two large prime numbers p and q, and initial seeds $a \in$QR mod $[p * q (= n)]$.

(2) Let g $<$ n be a randomly chosen generator of the multiplicative group of integers modulo n (Z_n^*).

(3) Let H be a collision-resistant hash function.

Key Generation

(1) The server fills up a mapping table starting from a_0 as shown in Fig. 4.3. After the first seed cycle is complete, it completes the table a_1 and starts filling the rest of the table. It continues generating seeds till the table is completed for all seeds from a_0 to a_k.

(2) Generate the private key X_A. The server randomly chooses values from the mapping table to send to the sensor node and forms a response voltage output pair corresponding to the sent values, using its pre-measured (voltage) values ($X_A = n_v(table)$) of dark currents of the photodiode (or in general, any other PUF variable) of the circuit.

(3) Generate the public key Y_A as g^{X_A} mod n.

(4) Thus the sender has the set of keys $\{X_A, Y_A\}$.

Signature generation

(1) Message m is $ID \oplus Data$.

(2) Choose a random a such that 1<a<p-1 and gcd($a, p-1$) = 1.

(3) Compute $r = g^k(mod\ n)$. Compute $s = (H(m) - X_A.r)a^{-1}(mod\ n-1)$.

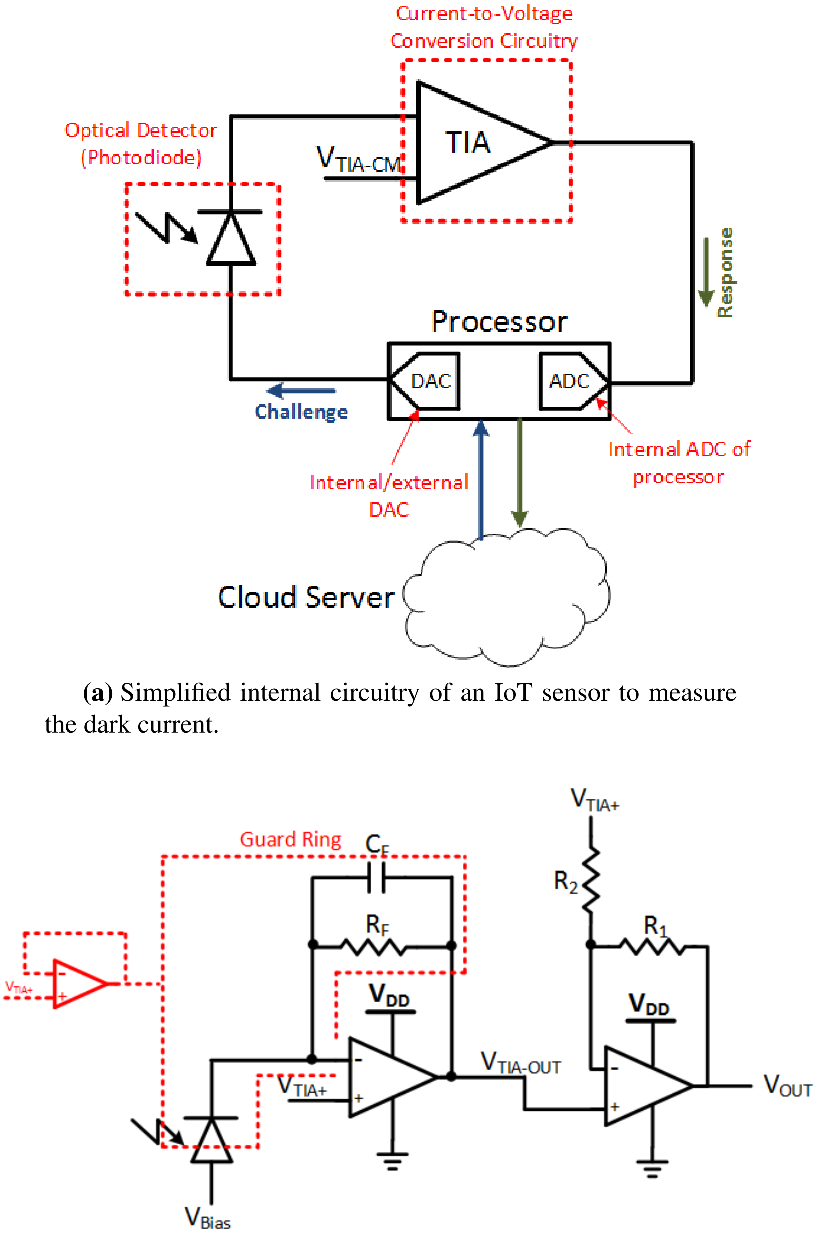
(4) If s=0, start over again. Then the pair (r, s) is the digital signature of m. The signer repeats these steps for every signature.

Verification

(1) Look Up public key Y_A for device d.

(2) Verify $g^m = Y_A^r * r^s(mod\ n)$

is converted by an analog-to-digital converter (ADC) to digital values, which the processor uses to convert to a key that is then sent to the cloud server. The DAC of the circuit can be either external components or integrated parts of the processor.



(a) Simplified internal circuitry of an IoT sensor to measure the dark current.

(b) Current-to-voltage conversion circuit with TIA.

Figure 4.4: Circuit to measure the dark current

One of main challenges of using dark current in a portable sensor node is that the magnitude of the dark current is in the order of pA to nA, and any measurement attempt of such tiny current requires careful attention to the effect of noise on the measurement result. It requires an accurate measurement method with limited energy budget. In our prototype, the current is first converted to voltage by low-noise/high-gain TIA which is amplified by a simple non-inverting voltage amplifier before being measured by ADC. Depending on the level of output voltage from TIA, this voltage amplifier can be also omitted from the design, but in this prototype version we have included it for measurement. In IoT applications like the ones proposed here, the energy budget of the sensor node is limited, and the amount of energy consumption is mainly determined by the minimum amount of time required for the circuit to process the challenge voltage received from the processor of the sensor node. The speed bottleneck of the sensor node is on the bandwidth of the TIA circuit, and the trade off between the bandwidth and noise relationship of TIA are studied through measurements described in the following sections.

4.3.1 PUF Prototype Circuitry Design with Consideration of Leakage Current

As the range of dark current of photodiode is in the order of pA to nA, special design consideration is required in order to prevent leakage current from interfering with accurate measurements of such small amounts of current. Several factors could contribute leakage current in the design, and one of main factors that can have direct impact on our measurement is the leakage current through the inverting input of the OpAmp used in TIA. When the impedance of the input of OpAmp is not large enough, a significant fraction of the dark current can leak through the OpAmp instead of flowing through the gain resistor of TIA, degrading the measurement accuracy. For our initial measurement, we chose the LMV793 OpAmp from Texas Instruments[132], which is low-noise/low-leakage and CMOS-based. The LMV793 has input bias current of 100fA at 5V V_{dd}, V_{cm}=2V at 25^{o}C, which is much smaller than the typical range of dark current of photodidoes. Another contributor of leakage current is the material used in the PCB. The solder mask used in the PCB generally helps to reduce moisture infiltration on to the PCB material, but too much area of the solder mask could build up surface charge, affecting measurement accuracy. Therefore, the solder mark was removed near the sensitive region of our circuit (near the photodiode and the input of TIA). The dust and moisture accumulated between the inverting input of TIA and low-impedance supply trace on the PCB could also induce leakage current flow. This leakage between traces could get worse when the voltage difference between adjacent traces is large. In order to address this issue, we implemented a guard ring, whose potential is driven by the same voltage applied to the inverting input of TIA. This guard ring surrounds the trace connected to the inverting input of TIA to remove potential difference. Fig. 4.5 shows the PUF prototype layout of the circuit used to measure the dark current of the photodiode, amplify it and derive the desired voltage in the measurement range of *millivolts*. The figure shows two different versions of circuit without and with a guard ring to minimize leakage current.

4.3.2 Circuit Design Optimization through Noise Analysis

Due to the small magnitude of the dark current from photodiodes, it is important to investigate the effects of noise on measurements. Fig. 4.6 shows the noise model of the TIA part of the circuit. R$_D$ is the output impedance of photodiodes and C$_{IN}$ is the sum of capacitances of the photodiode and the input of the OpAmp. R$_F$ is the feedback gain

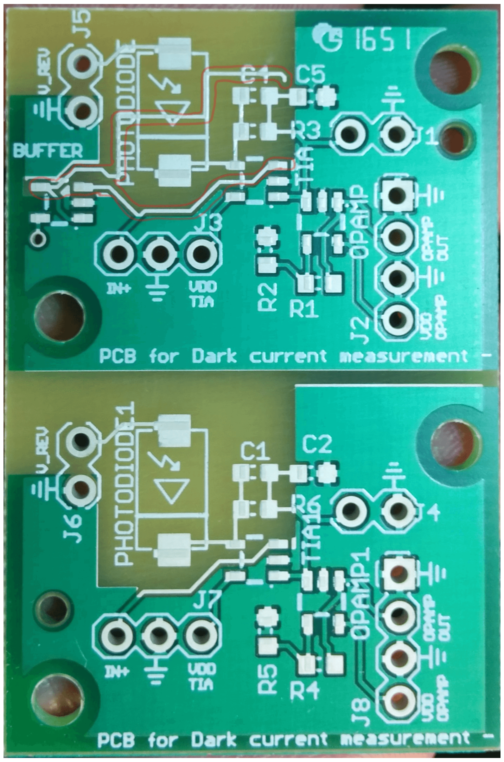


Figure 4.5: The PUF prototype circuit for measuring dark current from a photodiode. (Top: with a guard ring around the input of TIA to minimize the leakage current, Bottom: without a guard ring).

resistor and C$_F$ is the compensation capacitor of TIA. The compensation capacitor (C$_F$) is required in the TIA to create a zero to stabilize the circuit since without the compensation capacitor the circuit is essentially a differentiator, which is inherently unstable. Since the feedback factor (β) of the TIA is defined as V$_{IN}$/V$_{OUT}$, β can be expressed as below:

$$\beta = \frac{V_{IN}}{V_{OUT}} = \left(\frac{1 + sR_F C_F}{1 + \frac{R_F}{R_D} + sR_F(C_{IN} + C_F)} \right) \tag{4.3}$$

The zero and pole frequency from $\frac{1}{\beta}$ with the feedback capacitor are

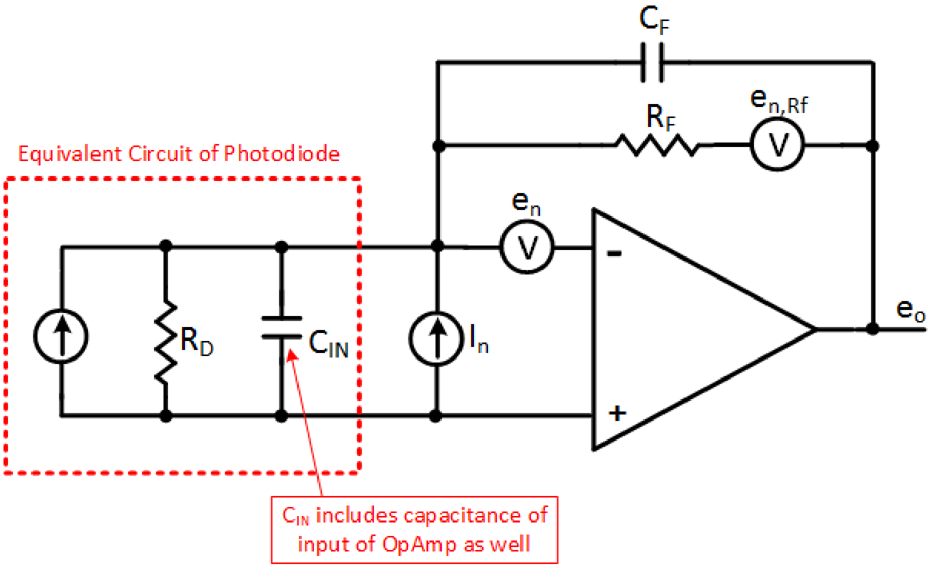


Figure 4.6: Noise model of TIA circuit with a photodiode.

$$f_Z = \frac{1}{2\pi R_F(C_{IN}+C_F)} \qquad (4.4)$$

$$f_P = \frac{1}{2\pi R_F C_F}$$

In order to investigate the magnitude of the voltage noise spectral density appearing at the TIA output (e$_o$), we need to consider both the feedback factor β of the TIA and the noise spectral density of the OpAmp itself (e$_n$). The input referred voltage spectral density of OpAmp (e$_n$) is scaled by a factor of $1/\beta$ to become the voltage spectral density at the output of TIA (e$_o$). The voltage spectral density profile of the OpAmp (e$_n$) can be obtained from the datasheet of the component [132], and the total output noise due to e$_n$ can be calculated by integrating the square of the output noise density over the entire frequency and taking the square-root of the value.

$$E_{o,rms} = \sqrt{\int_{-\infty}^{\infty} e_o^2(f)df} = \sqrt{\int_{-\infty}^{\infty} \frac{1}{\beta^2(f)} e_n^2(f)df} \qquad (4.5)$$

Since the magnitude of the dark current is quite small (in the order of hundreds of pA to a few nA), the TIA needs to have very large V/I gain, which is defined by the feedback resistor. However, as R$_F$ becomes comparable to the output impedance of the photodiode (R$_D$), some of the dark current would leak through R$_D$. Therefore, we chose 10MOhm for R$_F$, considering the typical value of 100MOhm of shunt resistance R$_D$ of the photodiode for initial calculation in this section [133]. The compensation capacitor C$_F$ was set to be 10pF to filter out the high frequency noise and to make the TIA stable. The value of input capacitance C$_{IN}$ was set to 15 pF considering typical capacitance of photodiodes, and the output impedance of the photodiode R$_D$ was chosen to 100MOhm. The zero and pole frequency of TIA are calculated as $f_Z = 700Hz$ and $f_P = 1592Hz$. Using the datasheet of LMV793 [132], we calculate the corner frequency (f_c), where the transition from 1/f flicker noise to white noise occurs, as $f_c = 340.2Hz$. Now, we can proceed to calculate the voltage noise of the TIA circuit.

For $f < f_c$, the rms-noise in this frequency region becomes

$$E_{o,rms,1} = \sqrt{\int_{f_o}^{f_c} \left(\frac{1}{\beta}\right)^2 e_n^2(f)df} = 0.347\mu V_{rms} \tag{4.6}$$

For $f_c < f < f_z$, both $1/\beta$ and e$_n$ are constant, and the rms-noise in this region becomes

$$E_{o,rms,2} = \sqrt{\int_{f_c}^{f_z} \left(\frac{1}{\beta}\right)^2 e_n^2 df} = 0.125\mu V_{rms} \tag{4.7}$$

For $f_z < f < f_p$, the rms noise is

$$E_{o,rms,3} = \sqrt{\int_{f_z}^{f_p} \left(\frac{1}{\beta(f)}\right)^2 e_n^2 df} = 0.330\mu V_{rms} \tag{4.8}$$

Finally, for $f_p < f$, the noise spectral density is

$$E_{o,rms,4} = \sqrt{\int_{f_p}^{f_\infty} \left(\frac{1}{\beta(f)}\right)^2 e_n^2 df} = 111.536\mu V_{rms} \tag{4.9}$$

The voltage noise density at the output of TIA due to the current noise of the OpAmp is equal to the input referred current noise of OpAmp multiplied by the impedance of feedback resistor and capacitor. Therefore, when a very large gain resistor is used, it is important to include the contribution from the current noise of the OpAmp for complete noise analysis. The rms output noise due to the current noise is

$$E_{o,rms} = \sqrt{\int_{-\infty}^{\infty} e_{ni}^2 df} = \sqrt{\int_{-\infty}^{\infty} i_n^2 \times \left(R_F || \frac{1}{sC_F}\right)^2 df} \tag{4.10}$$

From the datasheet of LMV793, we assumed that the corner frequency (f_i) where the current noise starts increasing is $30kHz$ in this calculation. For $f < f_p$ region, both i$_n$ and R$_F$ are constant, and the rms-noise from current noise source becomes

$$E_{o,rms,5} = \sqrt{\int_{f_o}^{f_p} i_n^2 R_F^2 df} = 3.99\mu V_{rms} \tag{4.11}$$

For $f_p < f < f_i$ and $f_i < f$, the rms-noise becomes

$$\begin{aligned} E_{o,rms,6} &= 3.88\mu V_{rms} \\ E_{o,rms,7} &= 39.44\mu V_{rms} \end{aligned} \tag{4.12}$$

The thermal noise of the feedback resistor also needs to be considered for complete noise calculation of TIA. The noise of feedback resistor R$_F$ at the room temperature can be calculated as

$$E_{o,rms,R_F} = \sqrt{4kTR_F\left(\frac{\pi}{2}\frac{1}{2\pi R_F C_F}\right)} = \sqrt{kT\left(\frac{1}{C_F}\right)} \tag{4.13}$$

$$E_{o,rms,R_F} = 20.28\mu V_{rms}$$

Note that the rms-thermal noise of the R$_F$ appearing at the output of TIA does not depend on the value of resistor any more. This is because as R$_F$ increases the bandwidth of TIA decreases at the same rate as the increase in thermal noise. Therefore, the value of R$_F$ doesn't have any impact on the thermal noise contribution. However, the signal is amplified by the gain of TIA, which is equal to R$_F$. Thus, it is important to maximize R$_F$ to obtain the best SNR ratio. The contribution due to OpAmp's noise is a little bit less intuitive. One might think that as the bandwidth of TIA decreases by increasing R$_F$, the output noise due to the OpAmp should be reduced since the high frequency noise would not appear at the output of TIA. However, the calculation shows that this is not the case. Also, the current noise also increases slightly since Z$_F$ increases by (4.10). Despite this increase in OpAmp noise, however, the amount of added noise is not significant compared to the amount of amplification on the signal achieved by increasing R$_F$. Therefore, it is still valid to say that using a largest possible R$_F$ maximizes SNR. Finally, the total rms output noise of TIA can be calculated by adding squared values of rms noise from different sources of noise, and taking a square-root of the final value.

$$E_{o,rms,Total} = \sqrt{\left(\sum_{i=1}^{7} (E_{o,rms,i})^2\right) + (E_{o,rms,R_F})^2} \tag{4.14}$$

$$E_{o,rms,Total} = 120.16\mu V_{rms}$$

If the maximum range of dark current from a photodiode is 200pA, the maximum output voltage swing appearing at the TIA output with the gain of 10MOhm is

$$\begin{aligned} V_{\max -pp,TIA_{out}} &= \left\{200pA \times \left(\frac{R_D}{R_F+R_D}\right)\right\} \times 10M\Omega \\ &= 1.82mV_{pp} \end{aligned} \tag{4.15}$$

Therefore, we find the dynamic range of the TIA from (4.14) and (4.15)

$$DyR = \frac{V_{\max -pp,TIA_{out}}}{V_{noise,rms,TIA_{out}}} = \frac{1820\mu V_{pp}}{120.16\mu V_{rms}} = 15.15 \tag{4.16}$$

4.3.3 Circuit Design Optimization

Since the key generation is done by measuring the dark current of the photodiode using a TIA circuit, the role of the sensor node processor is minimized to a few tasks – (a) receive challenge/ response from cloud server, (b) convert digital challenge values to analog bias voltage to the photodiode, (c) convert received analog voltage from TIA to digital and encrypt it into a key using **Algorithm 2**, and (d) send the response back to cloud server. The speed of processing these tasks is much faster than the speed bottleneck of the TIA circuit. Since other computation effort required by the processor is not significant compared to the amount of time TIA needs to process challenge voltages, the energy consumed by the sensor node is estimated to be inverse-proportional to the bandwidth of TIA. As a result, the total energy required for the sensor node depends on three major factors -(a) the time required for TIA to convert dark current to corresponding voltage response for each challenge, (b) the number of challenges required for one authentication by the proposed protocol and (c) the energy consumed by the components, such as the OpAmp required for dark current measurement. Since only the processor part of the sensor node needs to be powered when no challenge/response is received from the cloud server, the energy consumed by the other part of the sensor node, including the TIA circuitry, during idle time, is assumed to be zero. In short, the energy saving of the sensor node can be achieved by maximizing the speed of TIA circuitry, minimizing the number of challenges required by the security algorithm, and choosing power-efficient components for dark current measurement.

As shown earlier, the bandwidth of the TIA depends on the feedback capacitance (C$_F$) and the gain (R$_F$) of TIA. The speed of the TIA, however, is closely related to the noise at the TIA output. In general, as the bandwidth increases, the maximum allowable speed of varying challenge voltages increases, reducing the amount of computation time, but the TIA with large bandwidth also allows the high frequency noise to appear at the output, degrading the SNR and the dynamic range (DyR) of the TIA. From the pole frequency we obtained in the previous section, the minimum time required for the TIA to process each challenge voltage can be calculated as

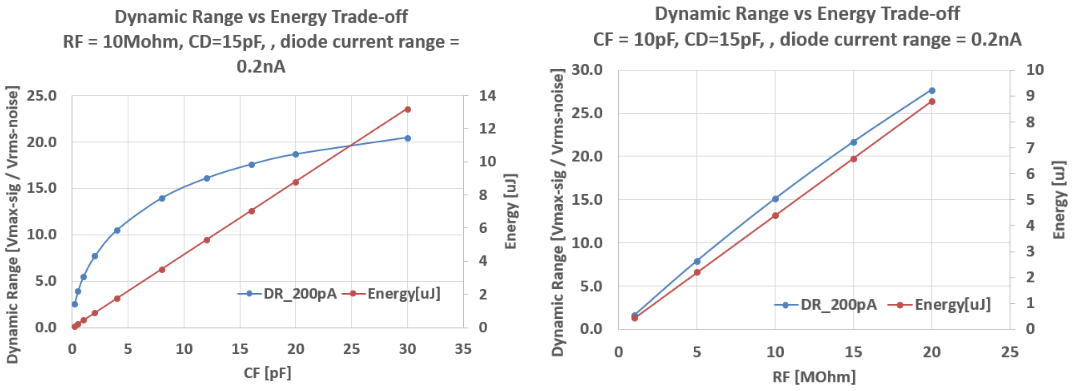
$$t_p = \frac{1}{f_p} = \frac{1}{1592Hz} = 628.3\mu s \tag{4.17}$$

Therefore, the energy required to process each challenge voltage by the TIA is the power consumed by the TIA multiplied by t_p. From the datasheet of LMV793, the power consumption for the chosen OpAmp is 7mW with 5V supply voltage [132]. Therefore, the estimated energy is calculated as

$$E_{bit,TIA} = t_p \times P_{TIA} = 628.3\mu s \times 7mW = 4.40\mu J \tag{4.18}$$

One of the options for further reducing the energy consumption of the TIA is to increase the bandwidth of TIA by either decreasing the gain (R$_F$) or decreasing the compensation capacitance (C$_F$). However, larger bandwidth inevitably increases the noise floor due to high frequency noise of the OpAmp that starts appearing at the output of TIA, degrading the dynamic range of the TIA. Fig. 4.7a and Fig. 4.7b show the trade-off between energy consumption and dynamic range of TIA with LMV793, for different values of R$_F$ and C$_F$. The maximum range of dark current was assumed to be 200pA, and dynamic range was calculated by taking the ratio of the estimated output voltage to the output voltage noise in rms as defined in (4.16). As C$_F$ increases, the output signal voltage remains the same but the overall noise decrease, improving DyR. As R$_F$ increases, the noise floor stays almost the same while the output signal voltage increases; improving DyR. However, for both cases, the reduced bandwidth decreases the speed of TIA and worsens the energy consumption.

Another option for reducing the energy consumption is to choose more power-efficient OpAmp for TIA. The LMV793 we used for earlier energy estimation consumes 7mW which is not very power efficient. Choosing the OpAmp for battery-powered applications could significantly reduce the energy consumption. To improve the energy savings, we used OpAmp **LMP2231** that is designed for battery-powered applications which draws only 50uW of power from 5V supply [134]. The noise calculation for LMP2231 is redone and the energy/noise trade-off is shown in Fig. 4.8.



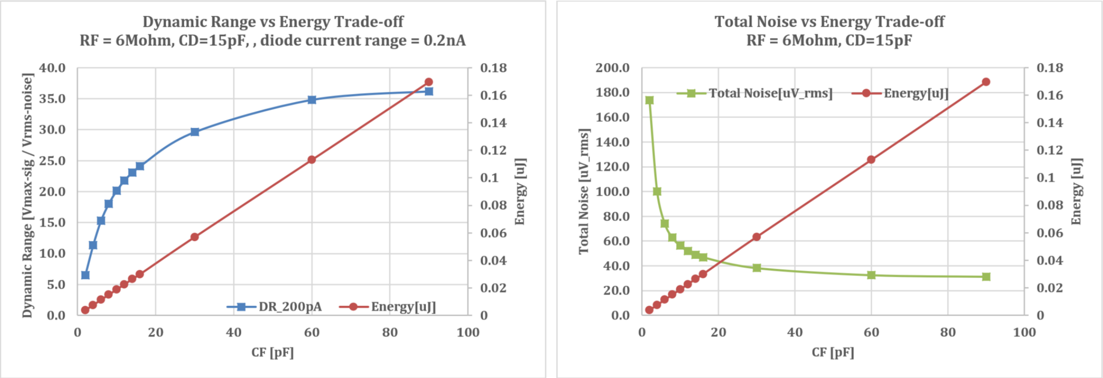
(a) Dynamic range vs. energy for various C$_F$ values for TIA LMV793.

(b) Dynamic range vs. energy trade-off for various R$_F$ values for TIA LMV793.

Figure 4.7: Plots for different C$_F$ values with R$_F$ = 10MOhm for TIA LMV793.

Compared to LMV793, the energy consumption is significantly reduced down to an order of tens of nanoJoules. For example, with R$_F$=6MOhm and C$_F$=8pF, a dynamic range of 18.0 can be achieved with energy consumption of 0.0151 uJ. It is noticeable that as C$_F$ increases, the energy consumption increases linearly, while the rate of increase in dynamic range eventually slows down. Fig. 4.8 shows the magnitude of total TIA noise for different C$_F$ values. Since the gain is fixed to 6MOhm, DyR in Fig. 4.8a and total noise in Fig. 4.8b are inverse-proportional to each other.

Fig. 4.9 shows the trade-offs between dynamic range and energy consumption as the value of R$_F$ changes from 4 to 100 MOhm. As R$_F$ increases, energy consumption of TIA increases linearly, but the slope of dynamic range slightly decreases as more current starts flowing through R$_D$ instead of R$_F$. Fig. 4.9b shows that the amount of total noise is relatively constant for different R$_F$ values, and Fig. 4.9c shows the source of noise. As mentioned earlier, changing the value of R$_F$ did not affect the thermal noise appearing at the output of TIA since the rate of thermal noise increase is the same as the rate of bandwidth decrease of TIA, canceling each other. The noise contributed by



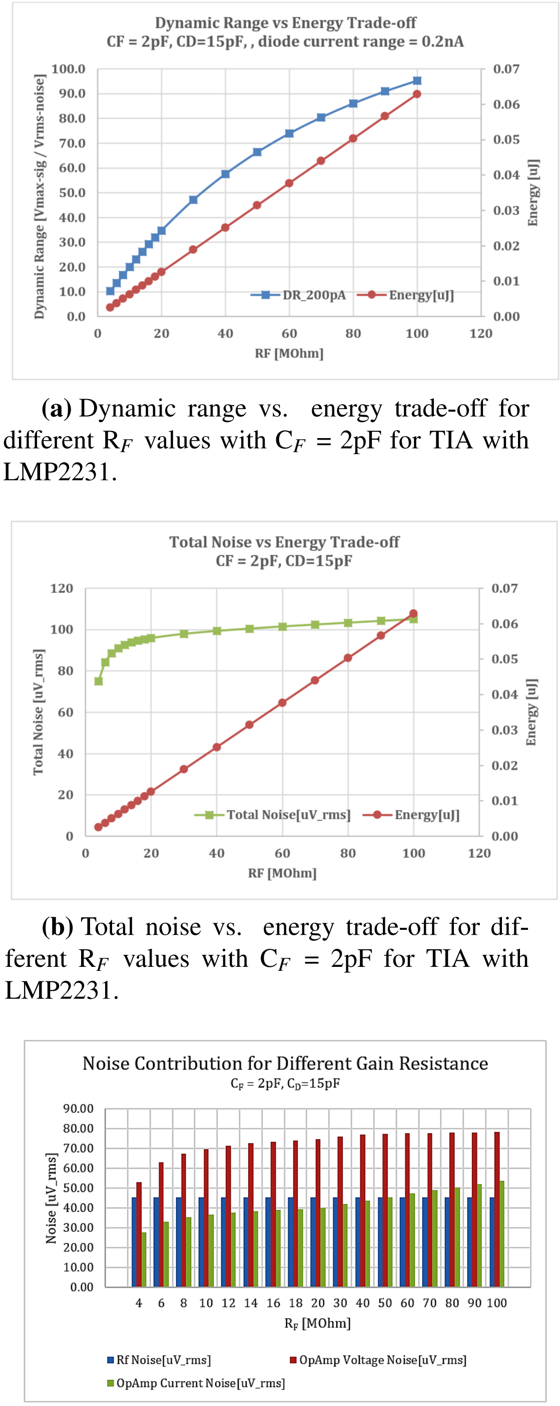
(a) Dynamic range vs. energy trade-off for various C_F values for TIA LMP2231.

(b) Total noise vs. energy trade-off for various C_F values for TIA LMP2231.

Figure 4.8: Plots for different C_F values with R_F = 6MOhm for TIA LMP2231.

the OpAmp slightly increases as R_F increases. The above results show that changing the values of R_F and C_F affects the amount of energy consumption linearly. However, changing R_F has more drastic impact on the dynamic range than changing C_F, as the value of R_F and C_F become larger. Therefore, it is better to increase the dynamic range of TIA by increasing R_F, and decrease the energy consumption by lowering C_F. Note that as R_F approaches the output impedance of photodiode, a fraction of dark current could start leaking through the internal resistance of the photodiode. However, this may not be an issue in implementing the proposed idea in terms of true dark current measurement since the purpose of measuring dark current is to identify a unique photodiode for security purpose, and the output impedance of individual photodiodes can be pre-measured and stored in the cloud along with the pre-measured dark-current profile required for key verification. Therefore, the variance of output impedance between photodiodes can be compensated in the cloud during the authentication process, adding an extra layer of complexity and making the system more secure.

Fig. 4.10a and Fig. 4.10b show the trade-off between dynamic range and energy

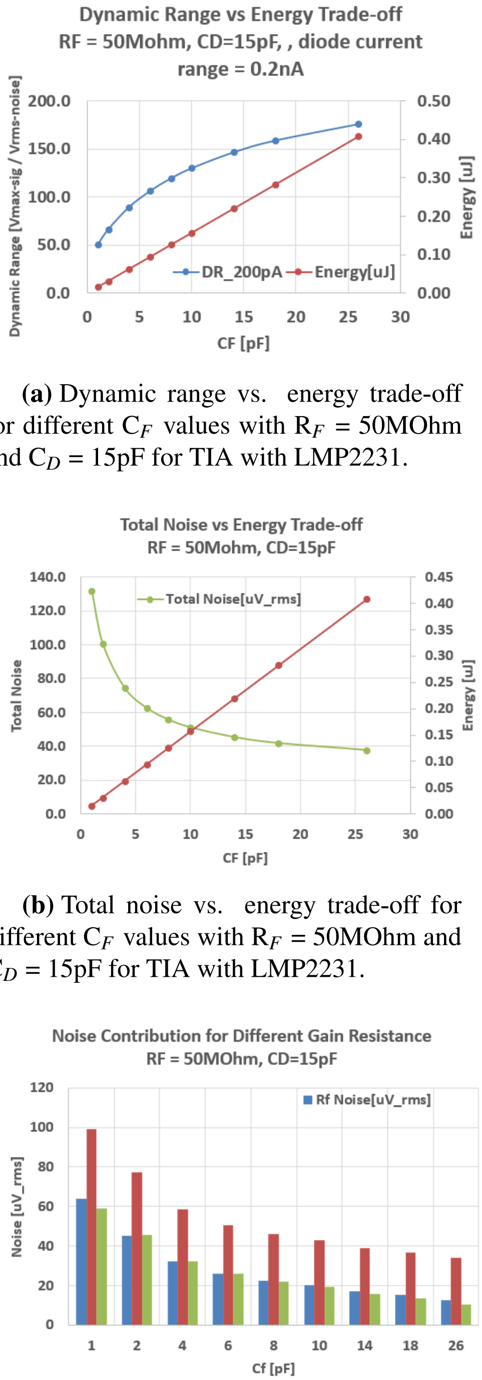


(a) Dynamic range vs. energy trade-off for different R$_F$ values with C$_F$ = 2pF for TIA with LMP2231.

(b) Total noise vs. energy trade-off for different R$_F$ values with C$_F$ = 2pF for TIA with LMP2231.

(c) Noise contribution for different R$_F$ values with C$_F$ = 2pF for TIA with LMP2231.

Figure 4.9: Plots for different R$_F$ values with C$_F$ = 2pF for TIA with LMP2231.



(a) Dynamic range vs. energy trade-off for different C$_F$ values with R$_F$ = 50MOhm and C$_D$ = 15pF for TIA with LMP2231.

(b) Total noise vs. energy trade-off for different C$_F$ values with R$_F$ = 50MOhm and C$_D$ = 15pF for TIA with LMP2231.

(c) Noise contribution for different C$_F$ values with R$_F$ = 50MOhm and C$_D$ = 15pF for TIA with LMP2231.

Figure 4.10: Plots for various C$_F$ values with R$_F$ = 50MOhm for TIA with LMP2231.

consumption for larger gain values of R$_F$ =50MOhm. The results show that a dynamic range of 119.6 can be achieved with smaller energy consumption of 0.126uJ with R$_F$ =50MOhm and C$_F$ = 8pF. It clearly indicates that increasing R$_F$ gives better energy saving for the same dynamic range, as long as the leakage current through the internal shunt resistance of the photodiode can be compensated accurately. Fig. 4.10c shows the contribution to the total noise for different C$_F$ values. As C$_F$ increases, both the thermal noise of R$_F$ resistor and OpAmp noise decrease. The decrease in thermal noise comes from the decreased pole frequency by (4.13), and the decrease in OpAmp noise comes from decreased noise gain $1/\beta$ at the high frequency region by (4.3).

The compensation capacitance values used in all Figures in this section are at least 10 times greater than the minimum capacitance required for guaranteeing stability of the TIA. The above results suggest when configuring the TIA for IoT sensor nodes choosing R$_F$ = 50MOhm and C$_F$= 10pF. This leads to a dynamic range of 130.3 (7bits) with energy consumption of 0.157uJ.

4.4 Results and Analysis

4.4.1 Output Measurements of the PUF Prototype Circuit

Fig. 4.11 shows the TIA circuit with OpAmps having offset at their inputs. The current from the photodiode and the output voltage of TIA can be expressed as

$$I_D = \frac{V_{TIA\_OUT} - V^*_{TIA+}}{R_F}$$
$$V_{TIA\_OUT} = I_D R_F + V^*_{TIA+} \tag{4.19}$$

where V$^*{}_{TIA}$ is the voltage appearing at the “–“ input of the first OpAmp when the

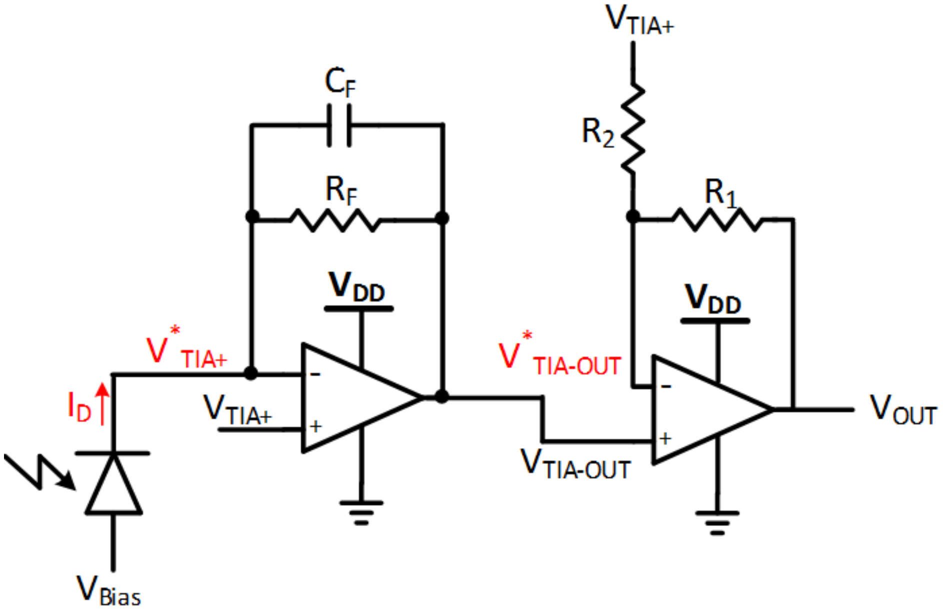


Figure 4.11: TIA circuit with input offset of the OpAmp.

output voltage is zero, and it can be expressed as a sum of V$_{TIA+}$ and the input offset voltage of the OpAmp as

$$V^*_{TIA+} = V_{TIA+} + V_{offset\_opamp1} \tag{4.20}$$

The voltage output of a non-inverting amplifier can be written as

$$V_{OUT} = G(V^*_{TIA\_OUT} - V_{TIA+}) + V_{TIA+} \tag{4.21}$$

where the gain of non-inverting amplifier (G) is $1+\frac{R_1}{R_2}$. The voltage at the “-“ input of the second OpAmp when the output voltage is zero is described as

$$V^*_{TIA\_OUT} = V_{TIA\_OUT} + V_{offset\_opamp2} \tag{4.22}$$

where V_{offset_opamp2} is the input offset voltage of the second OpAmp. Then, the voltage at the output of the second OpAmp can be written as

$$\begin{aligned} V_{OUT} &= G\left(V_{TIA\_OUT} + V_{offset\_opamp2} - V_{TIA+}\right) \\ &+V_{TIA+} \\ &= G\left(I_D R_F + V^{*}_{TIA+} + V_{offset\_opamp2} - V_{TIA+}\right) \\ &+V_{TIA+} \\ &= G\left(I_D R_F + V_{offset\_opamp1} + V_{offset\_opamp2}\right) + V_{TIA+} \end{aligned} \tag{4.23}$$

Then, the current can be re-written as

$$I_D = \frac{V_{OUT} - V_{TIA+}}{R_F G} - \frac{V_{offset\_opamp1} + V_{offset\_opamp2}}{R_F} \tag{4.24}$$

The input offset voltage of the OpAmp comes from the mismatch between two inputs of OpAmp due to manufacturing variation, and it is constant for a given device when the common-mode voltage is constant at a fixed temperature. Therefore, we can expect that the real value of dark current might differ from the measured one by the constant value due to the input offset voltage of OpAmp. Fig. 4.12 shows the measured dark current of various surface-mount photodiode devices with LMV2231 OpAmp with a TIA gain of 50MOhm at 24 Celsius. As the reverse bias voltage applied to the photodiode increases, the amount of dark current also increases. Some photodiodes, such as Vishay and Everlight, appear to have less than 20pA of dark current variation when the reverse bias voltage changes from 5 to 25V. However, this could be also due to the dark current leaked through the internal shunt resistor of photodiodes, which could happen when the shunt impedance of photodiode is comparable to the gain resistor value (50MOhm). The dark current measurement can be affected by two main factors: input offset voltage of the two opamps in our circuit, and tolerance of gain resistance. The

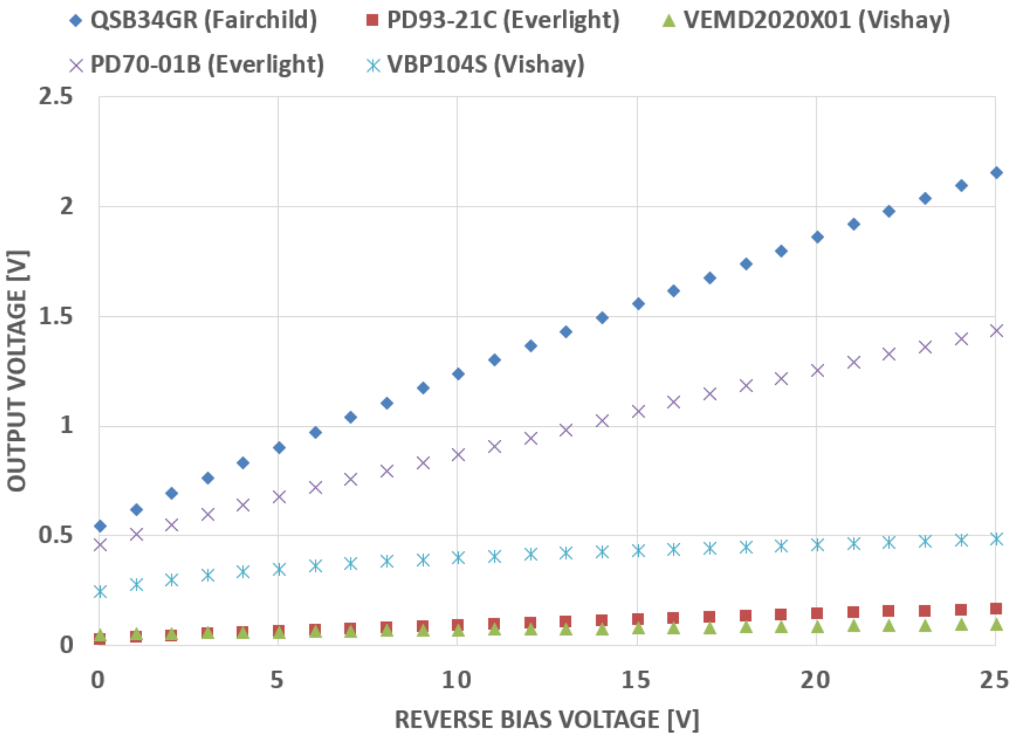
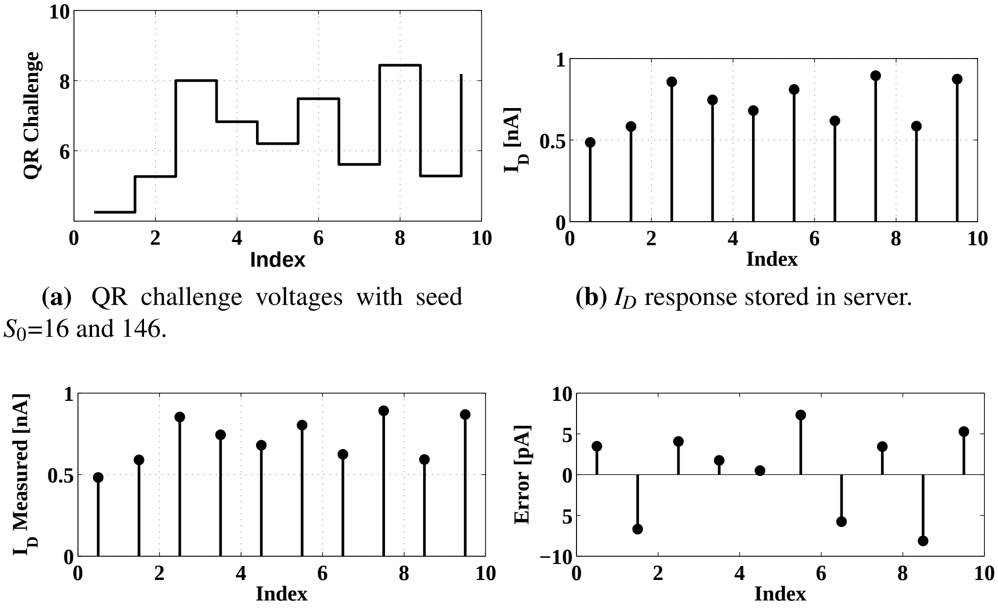


Figure 4.12: TIA amplified output voltage (response) vs. reverse voltage (challenge) of different silicon PIN photodiodes.

input offset voltage of an opamp is caused by mismatch of differential input transistors created during manufacturing process. Although the range of offset values can be found from the datasheet of the opamp vendors, the exact value is not known. Also, the gain resistor has its own tolerance. As shown in (4.24), the exact amount of dark current can be shifted from the true value based on these factors. Through the experiments, the resistance of a resistor is found to be a constant here and the input offset voltage is also constant at a fixed input voltage level; therefore, the difference between the measured and true dark current value is constant. Since knowing the exact dark current value is not important to identify between different sensor nodes as long as pre-measured dark current profile matches with the ones from a sensor node, these variation from



(a) QR challenge voltages with seed S_0=16 and 146.

(b) I_D response stored in server.

(c) I_D measured from Fig. 4.

(d) Error between stored I_D & measured I_D.

Figure 4.13: Measured and stored values of dark currents (I_D) in Everlight silicon photodiode.

manufacturing process does not play a negative roles for our security system.

Table 4.1: Amplified voltage response for different challenge voltages between 0 to 5V with respect to various silicon photodiodes.

Reverse Bias Voltage (V)	QSB34GR (mV) (Fairchild)	PD93-21C (mV) (Everlight)	VEMD2020X01 (mV) (Vishay)	PD70-01B (mV) (Everlight)	VBP104S (mV) (Vishay)
0.01	547	32	53	462	250
1	625	41	57	511	281
2	699	49	60	557	305
3	770	56	62	602	324
4	839	62	64	643	340
5	908	68	66	684	354

In Fig. 4.12, we have plotted the output voltage measurements using (4.23) with respect to the reverse bias voltage for the photodiode dark currents shown in Fig. 4.1. The measurements shown in Fig. 4.12 are for an ambient room temperature of 25^{o}C and an operating voltage range of 0 to 25V. The TIA amplified voltages are the measured responses to each challenge in the form of reverse voltage generated as in **Algorithm 2**.

Measurements in Fig. 4.12 are used in testing the IoT-PUF circuit in the lab environment before deployment. Where not possible to maintain laboratory voltage range, the proposed circuit also works well in the low voltage range on 0 to 5V. Table 4.1 depicts the TIA amplified voltage response for different challenge voltages between 0 to 5V with various silicon photodiodes taken in this Chapter as samples for validation. As can be interpreted from the table that with a 12-bit ADC, the resolution can be as small as 1.22 milli-Volts. Hence all the photodiodes with amplified voltage w.r.t their dark currents are in the range much higher than the ADC resolution. Further, the photodiodes are distinguishable even with an error in measurement accuracy of 1%-2% for very low values as in the VEMD2020X01 and PD93-21C photodiodes and ≈20 times more accurate for other photodiodes.

Fig. 4.13 depicts the measured and stored values of dark current (I_D) of an Everlight silicon photodiode. The measured value is the response to the corresponding challenge to the IoT sensor. The plot in Fig. 4.13a shows the QR voltage challenge generated by the server with two different seeds and sent to the sensor. Fig. 4.13b shows the value of (I_D) stored in the serve as a response to the corresponding challenge, which is then compared to the measured I_D, i.e., the response from sensor in Fig. 4.13c. The error,shown in Fig. 4.13d, is small and the correlation between the two current values is $\sim$ 0.9996. This means that using **Algorithm 2** the device can be authenticated.

4.4.2 Security Characteristics

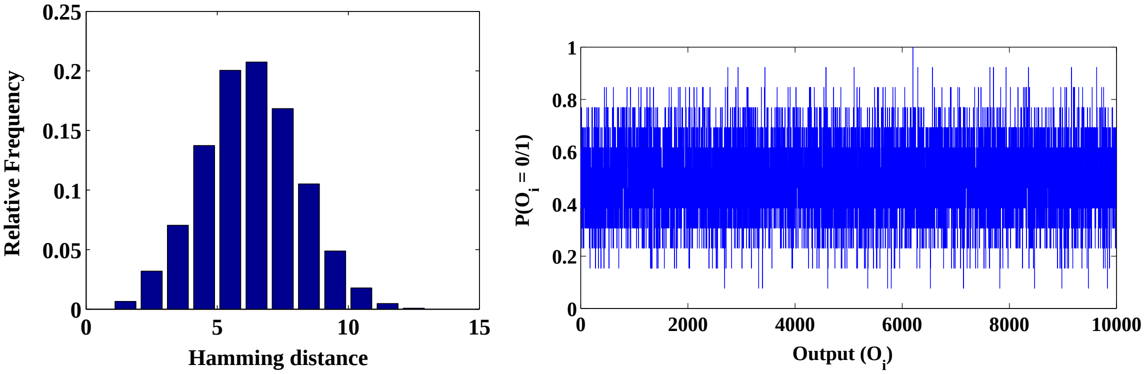
Earlier, we presented various PUF-IoT security metrics. Here, we will evaluate how our proposed algorithm and design satisfy the key metrics of a secure system from our measurements and algorithmic simulations. First, we will analyze our design for PUF-targeted attacks on the system.

Frequency Prediction Attack : We challenged the circuit with 10000 challenges and measured the response O_i of the system. From Fig. 4.14a, it can be inferred that the probability of O_i being a particular value is always around 0.5, which makes the randomness parameter to be $\approx 50\%$. Therefore, our method is resilient to this kind of attack.

Replay Attack : In this attack, the adversary tries to predict the output by studying the outputs that have similar inputs. In the proposed design, the randomness of input-output in the sensor PUF is enhanced by using a QR challenge/response pair generator. From Fig. 4.14b, it is evident that the proposed method generates a polynomial distribution with respect to the input-output hamming distance, i.e., the distance between the output vectors by changing one bit of input vectors in every iteration, for two different PUFs, i and j. This shows resiliently to this type of attack.

Cloning Attack : As the cipher generator knows the *ID* issued to the sensor, as well as the measured values of challenge/response pairs, it is difficult for the attacker to authenticate its own PUF. Further, as the mapping is a PUF function, it is impossible to exactly replicate the physical variations of the system.

Side-Channel Attack : This type of attack changes the physical properties of the original PUF. Once the inherent PUF properties are changed, challenge c will not generate the same response r_c as before. Rather, it will generate $r_c^{'}$. So, the adversary will not be able to validate its system. Once that will fail, the system will remove access for the affected IoT node. The node will be flagged as malicious and will not be able to send



(**a**) Input-output hamming distance distribution.

(**b**) probability of output $O_i = 1$.

Figure 4.14: Optical IoT sensor PUF's resilience towards various adversary attacks.

any further data.

Device authentication is performed using **Algorithm 2**. Only when successful pairing is done and access is granted to the a particular IoT node, the data transfer happens. Depending on the vulnerability of the network, authentication and pairing are done at regular intervals to maintain data integrity and authorized access to the system. This makes the system robust to DoS type of attacks. Also a bit-aliasing error is observed for various optical sensors. The error is the worst-case error, at boundary temperature conditions. We have taken a temperature range of 5^oC-40^oC for our measurements, although a larger range is possible as per the datasheet. The worst-case error is found to be 5.39% and the best case is 0.8%. To ensure integrity in the system, a public key is generated using the private key generated by the challenge/response pair of the IoT-PUF circuit. As shown in **Algorithm 3**, the encryption algorithm resist any eavesdropping attacks on the system.

4.4.3 Threat Analysis

Security threat to the PUF-based IoT system is through the user, manufacturer and external adversary. All the threats posed by external adversaries are explained in the previous section with the corresponding various types of attacks on the system. In this section, we will explain our system's defense to the other two threats.

Malicious user : It is the owner of the IoT device with potential to perform attacks to learn the secrets to gain access to restricted functionality. By uncovering the flaws in the system the malicious user tries to sell secrets to third parties, or even attack similar systems. Our proposed system will not be able to stop such an user to model some systems, but as our dark current property is unique it can stop the malicious user from modeling the system altogether. Although such a threat can be initially successful, but it will not give long term results for the user.

Bad Manufacturer : Is the producer of the device with the ability to exploit the technology to gain information about the users, or other IoT devices. Such a manufacturer can deliberately introduce security holes in its design to be exploited in the future for accessing the user's data and exposing it to third parties. Again the manufacturer's attack cannot be successful on our proposed system due to its random like properties. It is impossible to change the physical properties of a photo-diode using external resources. By doing so the diode will be corrupted and is unusable for the PUF circuit. Thus making this threat ineffective.

External threat : External adversary does not have access to the physical device. The secure cloud used in our authentication protocol if intercepted by the external adversary, can only give them access to the public key. The public key in turn is generated from the private key derived by PUF variations of our proposed system. Hence, this can give adversary initial success. But, without knowing the actual voltage used to generate the dark current, it is impossible for the adversary to decode the message. And such an interception will alert the receiving server system, which will in turn block the malicious node. Thus, the adversary would have to start again. In the worst case scenario, the nodes may become unusable by the system, but still the message will remain safe from being decoded.

4.4.4 Energy Consumption

Energy is a central concern in the deployment of IoT nodes having limited battery size and computational resources. Here, we investigate and compare the energy cost of various cryptographic protocols with our IoT PUF, from a computation at energy point of view. The energy consumption is linearly proportional to the processing time as described in (4.18) . The design proposed in this Chapter, uses R$_F$ = 50MOhm and C$_F$= 10pF with a dynamic range of 130.3 (7 bits), having energy consumption of 0.157uJ. Depending on the length of the encryption bits, the energy consumption can be computed from the TIA measured data. Our Op-Amp draws only 50uW of power from a 5V supply voltage. PUFs provide lightweight hardware fingerprints just like hash functions and can be used alternatively for authentication of the device [135]. Some of the hash functions found in the literature are MD5 (Message Digest 5)[136], SHA-1 (Secure Hash Algorithm 1)[137], and HMAC (Hash Message Authentication Code)[138]. MD5 is a cryptographic hash function to derive the authentication token, also called white list. SHA-1 is a 160-bit hash function, which resembles the MD5 algorithm. This was designed by the US National Security Agency (NSA) to be part of the Digital

Signature Algorithm. The standard for implementing hash-based authentication is the HMAC as in FIPS (Federal Information Processing Standards) [138]. HMAC is used in combination with an approved cryptographic hash function and needs a secret key for the calculation and the verification of the MACs. In Table 4.2, we of show the energy consumption the hash functions. MD5 and SHA-1 are lightweight hash functions and consume less energy as compared to HMAC. HMAC is a keyed function, for bit ranges of 0 to 128 bits, and the energy consumption fluctuates by a very minute amount. SHA1 has more steps of computation than MD5, hence it consumes more energy than MD5. All the values are shown per Byte of data. Our design consumes 0.1794 uJ/Byte, the least of all other hashing functions.

Table 4.2: Energy cost of various hash functions compared to our design

S.No.	Hashing Method	Energy Consumption (uJ/Byte)
1	Our IoT PUF	0.18
2	MD5	0.59
3	SHA-1	0.76
4	HMAC	1.16

Table 4.3: Energy cost of various asymmetric encryption algorithms as implemented in different sensor motes

Algorithm	MICAz mote		TelosB mote	
	Cycles	Energy	Cycles	Energy
ECC-160 [139]	15.6 M	55 mJ	14.0 M	17 mJ
Our IoT PUF 128-bit	**4640**	**16 μJ**	**3480**	**4 μJ**
RSA-1024 [139]	108.1 M	378 mJ	60.4 M	73 mJ
Our IoT PUF 1024-bit	**5.9 M**	**21 mJ**	**4.4 M**	**5 mJ**

Algorithm 3, uses an asymmetric approach to encrypt our IoT-PUF system. This secures the system from intruders and provides resistance to malicious attacks. It also provides confidentiality, privacy, and integrity to the IoT node. Rivest-Shamir-Adleman

(RSA) and Elliptic Curve Cryptography (ECC) are two lightweight secure asymmetric algorithms for IoT[139–142]. Both work by generating public and private keys. Public keys are published openly, whereas private keys are made secure. ECC has faster computation times and bit-shifting operations instead of multiplications, to save energy for low power devices. In Table 4.3, we have compared our method with ECC and RSA in terms of energy cost, and number of computation cycles, using tiny sensors, such as the MICAz and TelosB. Note that the computation energy values are taken from [139]. It can be inferred from the table that the proposed method consumes less energy as compared to other public cryptographic algorithms. This is due to the fact that our private and public keys are generated by PUF functions rather than complex multiplications as in RSA and ECC. Further, the decryption is done at the receiving end in a cloud server, thus relieving the low power IoT devices of computation burdens.

Chapter 5

Energy Management in Smart Cities: Peak Demand Reduction and Energy Savings

5.1 Introduction

Smart cities in brief can be defined as a city which uses information and communication technologies (ICT) such as smart sensors, cognitive learning, and context awareness to make lives more comfortable, efficient, and sustainable [2]. Cities today face multifarious challenges, including environmental sustainability, low carbon solutions and providing better services to their citizens. Given these trends, it is critical to understand how ICT can help make future cities more sustainable. As microcosms of the smart cities, smart and green buildings and homes stand to benefit the most from connecting people, process, data, and things. The Internet of Things (IoT) is a key enabler for smart cities, in which sensing devices and actuators are major components along with communication and network devices. Management of smart homes often requires analyzing IoT data from the interconnected networked devices to optimize efficiency, comfort, safety, and to make decisions faster and more precise [143].

The significant efficiency gains from home automation can make cities sustainable in terms of resources. Importantly, the IoT ambitions and scope are designed to respond to the need for real-time, context-specific information intelligence and analytics to address specific local imperatives [144]. Further, realization of smart, energy-efficient and green home infrastructure would allow the development of 'livable' interconnected communities, which will form the backbone of a futuristic green city architecture [145]. Hence, energy management in smart homes is a key aspect of building efficient smart cities [146]. Energy management consists of demand side management (dsm), peak load reduction and reducing carbon emissions[147]. In an industrialized country, residential and commercial loads in urban centers consume a significant amount of electrical energy. As per the survey report [148] nearly $39\% - 40\%$ of the total energy consumption in Canada is consumed by the residential and commercial complexes. It is evident from various load surveys that the demand of electricity in these residences is highly variable and changes throughout the day. Therefore, finding suitable strategies for efficient management of home energy demand and to help reduce the energy consumption during peak period will make the communities' more energy efficient. The Canada Green Building Council is working towards finding ways of making buildings greener and community sustainable[1]. Therefore, the need for energy efficient buildings is growing rapidly.

The power systems require equilibrium between electricity generation and demand [149]. Power system operators dispatch generating units primarily based on operating

[1] [Online] Available : http://www.cagbc.org

cost or market bid price. In order to meet the increased demand during peak period, more resources are often required to increase the generation capacity. Since addition of resources to meet the peak demand is an expensive investment, distribution system planners and utility engineers very often consider the reduction in peak load as a feasible solution to the problem. However, peak load reduction is mostly valuable for utilities and most popular only in a purely market-driven energy management environment. Under these circumstances, Demand Response (DR) [150] and [151] offers an opportunity for consumers to play a significant role in the operation of the electric grid by reducing or shifting their electricity consumption during peak periods in response to time-based rates or other forms of financial incentives. In most of the cases, DR is a voluntary program that compensates the consumers. There are many modern methods that reduce the peak load and load at peak time which is referred as Demand Side Management (DSM) [152]. Current market framework and lack of experience and understanding of the nature of demand response are the most common challenges in DSM nowadays [152].

Newer technologies like energy management using smart meters are now becoming popular in places like Ontario, Canada where few utilities have introduced energy tariff based on the Time-Of-Use (TOU) model in which a consumer pays differently for the energy consumption at the different time of the day. This has been possible due to the implementation of smart meters which track the energy usage in a home on an hourly basis [153] and then consumption information is bundled into multiple TOU price brackets. However, all these processes mostly help the local distribution company and in order to take advantages of the TOU, each household has to adopt a change in the use of the appliances which may cause significant discomfort to the consumers. In this scenario home appliance scheduling with electrical energy services for residential consumers is useful.

In this Chapter, a home energy management system named as Home Energy Management as a Service (HEMaaS) is proposed which provides intelligent decisions, is interactive with the environment, scalable and user friendly. Wi-Fi connected smart sensors with centralised decision-making mechanism can identify peak load conditions and employ the automatic switching to divert or reduce power demand during peak period, thereby reducing the energy consumption. Therefore, by implementing monitoring and controlling sections of the HEMaaS platform using web services, one may achieve the agility, flexibility, scalability, and other features required for a feasible and affordable HEMaaS platform.

We have based our experimental findings on a typical Canadian residential apartment IoE system to investigate the effectiveness of the proposed home energy management service. The main objective of HEMaaS is to shift and curtail household appliance usages so the peak demand and total energy consumption can be reduced. A new neural network based reinforcement learning algorithm has been proposed in this Chapter to achieve the objectives. The classical Q-learning problem of the reinforcement learning has been formulated as a neural fitted supervised learning problem here and is named Neural Fitted Q-based Home Energy Management (*NFQbHEM*) algorithm. We design a node-red framework based user interface for controlling home appliance action based on *NFQbHEM* algorithm. The reward matrix incorporates user convenience parameters for state- action transition and includes user preference, power cost savings, robustness measure and user input preferences to initialize the algorithm.

Rest of the Chapter is organized as follows: Section 5.2 describes the HEMaaS platform and its architecture. Section 5.3 formulates the home energy management problem as a markov problem and its possible solution strategy is described using various modelling parameters. The *NFQbHEM* algorithm is explained in Section 5.4. The experimental results are shown in Section 5.5 for different cases.

5.2 Home Energy Management as a Service

Home energy management is a service platform for the users to efficiently perform demand side management and control. It consists of home appliances connected through a grid of interconnected network of devices with preference given to the user convenience. The platform may be used for different types of community houses (condo and town homes) to manage their energy consumption. The systems may be categorized into hardware and software architectures.

5.2.1 The Hardware Architecture

A typical home consists of various appliances. These appliances establish a connection with the user and provide them with the monitoring and controlling capabilities. They are to be monitored and controlled locally or remotely by a HEMaaS platform using a Sonoff wireless switch [2]. Most of the common home devices fall within the (current, voltage) range of Sonoff currently commercially available in the market.

The architectural diagram is shown in Figure 5.1. It consists of a Main Command and Control Unit (MCCU), Sonoff wireless switch, Smart meter, Gateway router and a Community Cloud Management panel (CCM). The MCCU is the main intelligence of the network which is responsible for triggering grid signals based on the output of the machine learning algorithms. It also has an input port which monitors for user input signals and accordingly provides user input to the controller. Sonoff Switch receives

[2] The Sonoff is a device that is to be put in series with the power lines allowing it to turn any device on and off remotely. Its voltage range is 90-250V and it can handle a max current of 10A.[Online] Available : https://www.itead.cc/sonoff-pow.html.

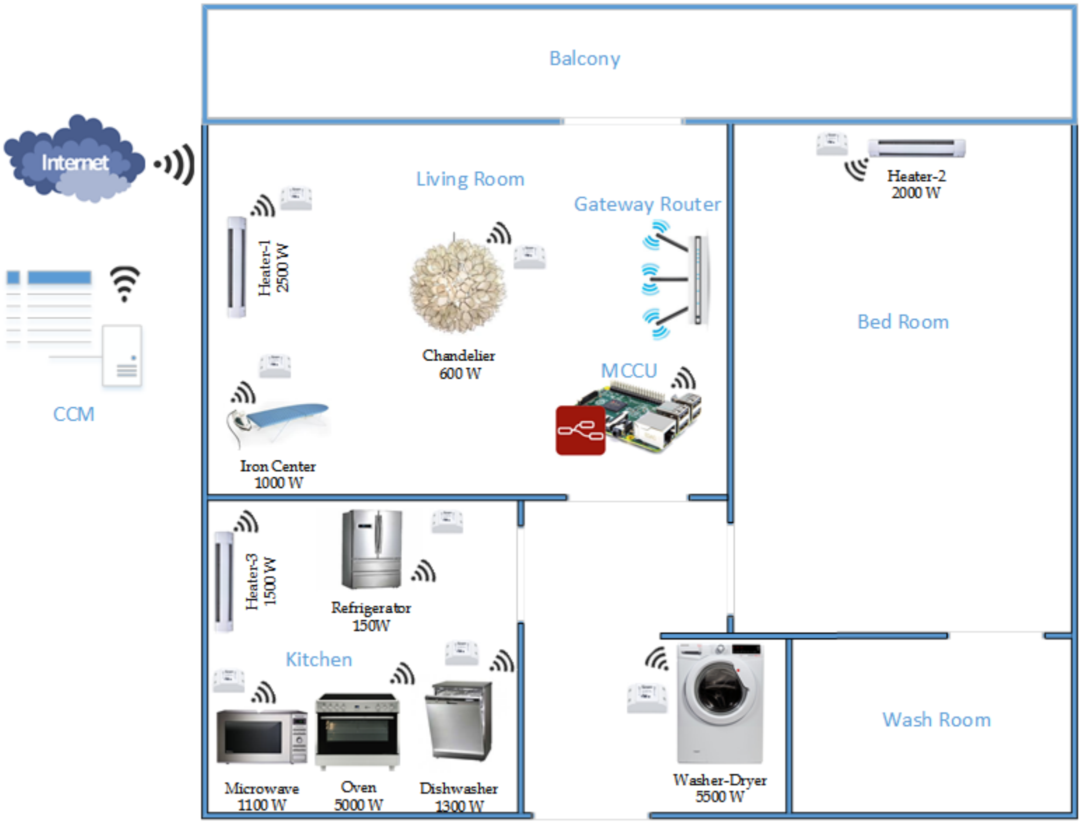


Figure 5.1: HEMaaS hardware architecture of a typical Canadian condo

the trigger at its input port from the MCCU and turns the appliance Off/On accordingly. Smart meter provides power consumption data to the power station for overall efficient community energy management. Gateway router translates the MCCU messages using network address translation (NAT) in order to translate from a private network address (like 192.168.x.x, 10.0.x.x) to a public facing one. The smart meter and CCM are outside of gateway router and are separated by a secured firewall. CCM is monitored by the city power substation. The substation according to its generation and distribution has a set amount of available power for the community to use. CCM receives input from the substation and sends those commands to the each home's MCCU which in term updates its power management strategy.

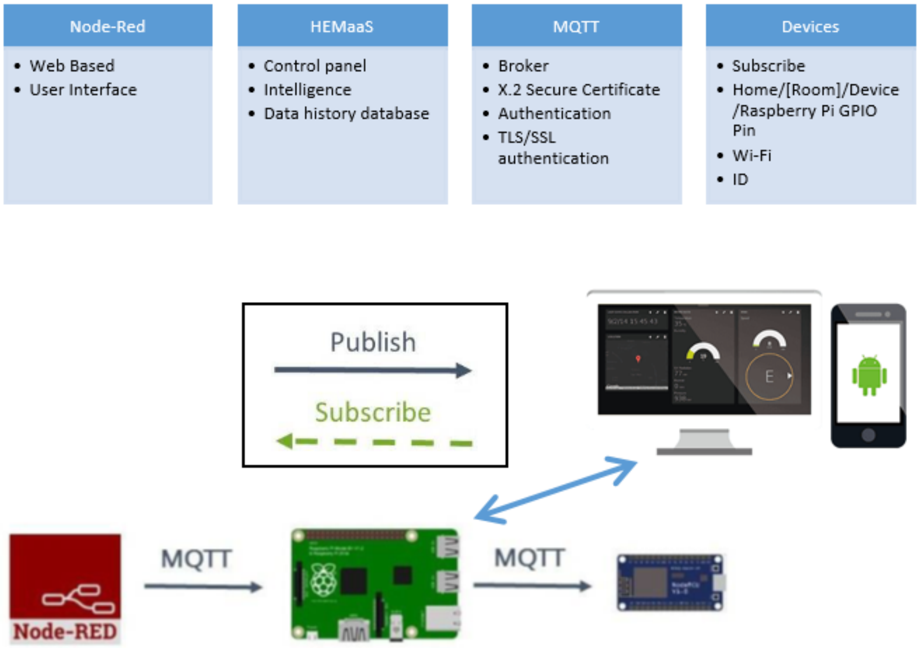


Figure 5.2: Software architecture and communication framework of HEMaaS platform

5.2.2 The Software Architecture and Communication Interface

The HEM MCCU needs to process the $NFQbHEM$ algorithm integrating historical data as well as the user input preferences. Thus a decision needs to be formed quickly. Moreover, the state-action pair and user preferences change rapidly throughout the day and HEMaaS platform needs to provide service in a timely manner. Therefore, here a Linux-based fast microcontroller has been used, namely Raspberry Pi3[3]. Raspberry Pi3 runs the $NFQbHEM$ algorithm using python programming language and plots the charts with its matplot library. Figure 5.2 shows the software architecture and communication framework of HEMaaS platform. The web-based node-red programming model have been choosen to implement the controlling structure of the HEMaaS platform. It is easy to implement with a flow and is easily explandable if more appliances

[3] [Online] Available : https://www.raspberrypi.org/products/raspberry-pi-3-model-b/.

join the network. The user input is modelled inside the flow with a switch. User input manually can cause either a delay in the operation of the appliance or it will reset its temperature. These settings can also be changed via the smart MCCU algorithmic decision. A lightweight, low-power and secure protocol has been used in the Chapter to communicate between home appliances and the MCCU over Wi-Fi. The protocol is called Message Queue Telemetry Transport (MQTT) [154] and it is optimized for high-latency or unreliable networks. MQTT provides three level security for the data over the network. It uses a broker to publish messages to clients who subscribe to a particular topic. Topic are in the form of a hierarchy of devices in the home [Home/(Room)/(Device)/RaspberryPi GPIO Pin]. Mosquitto[4] broker has been used in this architecture. Broker performs authentication via username and password, client ID and X.2 certification to validate the clients in the HEM network. Thus intrusion can be prevented. A dashboard user interface (UI) for desktop and mobile have been designed to give users ample interaction opportunities. The design of the UI is described in detail in the result section.

5.3 HEM as a Markov Decision Process and Its Solution

We formulate our HEM problem as a set of discrete states, where each state represents a binary formulation of the power levels of home appliances. The MCCU issues command to switch these power states. We model the power states as a Markov Decision Process (MDP) and derive its solution using reinforcement learning (RL) based Neural Fitted Q-Iteration (NFQI) algorithm. The reason for choosing RL with neural network function classifier is based on the type of system being modeled and its behavior. As

[4] [Online] Available : https://mosquitto.org/.

per [155] and [156], the machine learning algorithms are divided into unsupervised and supervised learning. For unlabeled data algorithms like k-means, gaussian mixture models are applied to the data. However, as we have historical data [148] to be used for our modeling, these algorithms will not be the best suited for our scenario. For labeled data training and fitting, algorithms like regression, decision trees, support vector machines, naive Bayes classifier and neural networks are used. As the HEMaaS system has user interaction and feedback from wireless access point of the appliances, only using supervised learning algorithms to fit the data for maximum accuracy/minimizing cost will be time and resource consuming. The algorithm has to interact with the environment and objects, learn from their feedback and should update its goals accordingly. Thus reinforcement learning (RL) [157], which starts from a particular state, learns from the environment and update its goals is the best suited for our application. As the algorithm will pass through multiple states in order to reach its optimum goal, a supervised classifier can be used in conjunction with the RL algorithm. Neural network is slow, but classifies accurately in comparison to other supervised learning methods [158]. Hence it is chosen as the modeler for our system.

MDP [159] is a set of discrete time stochastic control process where outcomes are obtained with a combination of partly random events and partly by a decision making process. At each time step, the MDP is modeled as a sequence of finite states $s_i \in S$, the agent action $a_i \in A$ that are evaluated based on a random process to lead the agent to another state. For each action performed, the agent receives an award R. As in [159], MDP is formulated as a set of four-tuple $<S,A,P,R>$, where P is the state transition probability when agent moves from state $(s(t) \rightarrow s(t+1)) \in S$. From the current state $s_i(t) \in S$ to state $s_j(t) \in S$ in response to action $a \in A$, the transition probability is $P(s_i,a,s_j)$ and an award $R(s_i,a)$ is received. Let s_k denote the state of the system just before the k^{th} transition. In an infinite horizon problem ($s \to 1...\infty$), maximum average discounted reward received is found using the action executed at each state using a reward policy $\pi(s)$. RL [157] is a machine learning approach that solves the MDP problem. It learns the policy online with real-time interaction with the dynamic environment and adjusts the policy accordingly. After a certain set-up time, the optimal policy can positively be found.

Q-learning is an online algorithm that performs reinforcement learning [160]. The algorithm calculates the quality of a state-action pair which is denoted by Q and is initialized to zero at the beginning of the learning phase. At each step of environment interaction, the agent observes the environment and decides on an action to change state based on the current state of the system. The new state gives the agent a reward which indicates the value of the state transition. The agent keeps a value function $Q^{\pi}(s(t),a(t))$ according to an action performed which maximizes the long-term rewards. The Q-factor update equation with discounted reward is as follows

$$\begin{aligned}&Q^{t+1}(s(t+1),a(t)) = Q^{t}(s(t),a(t)) + \alpha(s(t),a(t))[R(t)+\\&\gamma \cdot MAX\left(Q^{t}(s(t+1),a(t))\right) - Q^{t}(s(t),a(t))]\end{aligned} \tag{5.1}$$

Where, $\alpha(s(t),a(t))$ is the learning rate ($0<\alpha<1$) and γ is the discount factor within the range 0 and 1. If γ is close to 0, the agent chooses immediate rewards, else it will choose to explore and aim for long-term rewards. In [160] it is proved that the learning rate α is a function of k, where k is the number of state transitions. It satisfies the condition as

$$\alpha^{k} = \frac{A}{B+k} \tag{5.2}$$

Where, A and B need to be found out using simulations.

Online learning methods like Q-learning are good from a conceptual point of view and are very successful when applied to problems with small, discrete state spaces. But for more realistic systems, the ‘exploration overhead’, stochastic approximation inefficiencies and stability issues cause the system to get stuck in sub-optimal policies. Updating the Q-value of state-action pair $(s(t), a(t))$ in time step t this may influence the values $(s(t-1), a(t))$ for all $a \in A$ of a preceding state s_{t-1}. However, this change will not back-propagate immediately to all the involved preceding states. Batch Reinforcement Learning (BRL) typically address all three issues and come up with specific solutions. It performs efficient use of collected historical data and yield better policies [161]. It consists of three phases, which are exploration, learning and application. Exploration has an important impact on the quality of the policies that can be learned. The distribution of transitions in the provided batch must resemble the ‘true’ transition probabilities of the system in order to allow the derivation of good policies. For achieving this, training of samples is done from the system itself, by simply interacting with it. When samples cover the state spaces closed to the goal state, policy achieved will be closed to the optimal policy and convergence would be faster. NFQI algorithm is one of the popular algorithms described in [162]. Given a set of transition samples over $(s(t), a(t), R(t), s(t+1))$ and an initial Q-value $\overline{q}^{0}_{s,a} = 0$, derive an initial approximation Q^0 with $Q^0 = \overline{q}^{0}_{s,a}$. Update the value of $\overline{q}^{k}_{s,a}$ at each iteration. Define a training set T^k and convert the update problem into a supervised neural network based learning problem. Finally, find the resulting function approximator $\hat{Q}^i$ using the pattern trained using set T^k. At the end, a greedy policy is used to define the policy $\pi(s)$.

$$\pi(s) = \underset{a \in A}{argmax}\ Q(s, a) \tag{5.3}$$

5.3.1 State-Action Modelling of Appliances

The software architecture of the homes in communities shown in Section 5.2.2 describes a typical condo home architecture with living room, bedroom, kitchen and washroom. Each of the sections have various common home appliances having varied peak load power rating as in Table 5.1 as taken from [163]. The states $s(t)$ defined in the **Algorithm 4** are different combinations of power levels derived from the peak power rating of the appliances. Apart from refrigerator all other appliances can be turned *On/Off* in a smart home as the refrigerator needs to continuously run throughout the day and should not be stopped. Usage pattern of all other appliances vary throughout the day and can be controlled through the MCCU. Therefore, in total there are 10 appliances and a $2^n - 1$ transition states depicting various combination of power levels ($n = 9$) which results in 511 states. Lets depict each appliance in ascending order of their peak power level from Table I with level 'p_l'. Thus *Lighting* will be symbolized by p_1 and *WasherDryer* by p_9. The power values are coded as binary states i.e. 0 represents the *Off* state and 1 represents *On* state. For example, 001001010 means $Microwave$, $Heater - 2(Bedroom)$ and *Stove* are in *On* state and rest all are in *Off* condition. The total power consumed at that instant t is 7600 $Watts$ if every *On* appliance is operating at peak load.

Table 5.1: Maximum load rating of home appliances

Appliances	**Peak Power Rating [Watts]**
Heater - 1 (Living Room)	2500
Heater - 2 (Bedroom)	2000
Heater - 3 (Kitchen)	1500
Iron Center	1000
Microwave	1100
Dishwasher	1300
Lighting	600
Stove	5000
Washer Dryer	5500
Refrigerator	150

There are four different actions that can be performed based on the states. Turning the appliance *Off*, turning it *On*, pausing the operation and postponing the operation. For the case of simplicity, turning the appliance *Off* is considered as an required action. Also pausing and postponing the operation of the appliance can be selected for the symbolic *Off* state through the MCCU control based on the situation. The representation remains the same but power level changes. Moreover, we also define User Input Preferences (UIP) as a user input control which changes the decision of the MCCU controller algorithm as desired by the user at a certain time interval. After the scheduling task is over, the control is shifted back to MCCU algorithm. Agent can move from one state to another state after performing an action. The user inconvenience is modeled in the reward matrix and the goal of the strategy is to minimize the user inconvenience.

5.3.2 User Convenience and Reward Matrix

In this section, user convenience $UC(t)$ is modeled at a time instant t and the goal is to maximize the $UC(t)$. The reward values for turning off an appliance is based on the user inconvenience. The parameters taken to model $UC(t)$ are user preference $(P_a(t))$ of the appliances, power consumption energy cost saving $(C_a(t))$, and robustness $(S_a(t))$. Maximum inconvenience is caused by turning off an user preffered appliance at a given time. The time slot is discretized for every 15 minutes regarding the preferences and is divided into four times of the day i.e. Morning(MR), Afternoon(AF), Evening(EV) and Night(NT). Table 5.2 depicts the $(P_a(t))$ values of the appliances for different times of the day and the preferences are set according to a typical winter usage in Canada.

Table 5.2: User preference of appliances (P_a)

Appliances	**Morning(MR)**	**Afternoon(AF)**	**Evening(EV)**	**Night(NT)**
Heater - 1 (Living Room)	1	0.3	1	0.3
Heater - 2 (Bedroom)	1	0.3	0.4	1
Heater - 3 (Kitchen)	0.6	0.3	0.7	0.1
Iron Center	0.6	0.1	0.1	0.1
Microwave	1	0.1	0.8	0.1
Dishwasher	0.5	1	0.3	0.7
Lighting	0.4	0.1	0.7	0.1
Stove	0.7	0.1	1	0.1
Washer Dryer	0.6	0.6	0.3	0.5

User inconvenience $UIC(t)$ due to turning off an appliance with preference represented by Table 5.2 will become

$$UIC(t) = C_1 \cdot P_a(t) \tag{5.4}$$

C_1 is a constant and is set to 1 to give user preference maximum importance while choosing the agent action. As appliances are turned off, energy savings in terms of the cost is achieved. So turning *Off* the maximum power consuming appliance at a given time t will give the maximum convenience to the users in terms of cost savings.

Rest all appliances' energy cost is normalized w.r.t the maximum power load of the maximum power consuming appliance at t. User inconvenience $UIC(t)$ due to turning off an appliance is also dependent on the cost saving $(C_a(t))$.

$$UIC(t) = C_2 \cdot (1 - C_a(t)) \tag{5.5}$$

The more the cost saving, lesser the user inconvenience. But cost cannot be saved sacrifising preference comfort for users. Hence, constant C_2 will have lower contribution to the $UIC(t)$. We take C_2 as 0.5 here for our case. Emergency $(E_a(t))$ gives users options for choosing to start an appliance regardless of the time of the day, power consumed and preference control. When the user choose to run an appliance, it becomes a don't care condition in the state for that instant t. Hence the number of state-action pair for the reward matrix decreases. The appliance power is substracted fom the goal usage power.

Section 5.2.2 describes how MQTT handles broker security with Password Authentication, Client ID Authentication, SSL/TLS Certification and firewalls. Robustness of a system shows how it is immune to security threats and fault tolerant. Less robust system also creates inconvenience to the users. Robustness of the system is modelled behaviouraly has been categorized as {Good, Medium and Bad}. For each behaviour of the system a constant C_3 value have been assigned to the $UIC(t)$ function as

$$\begin{gathered} UIC(t) = C_3 \cdot S_a(t) \\ C_3 = \begin{cases} 0.2, Good \\ 0.3, Medium \\ 0.5, Bad \end{cases} \end{gathered} \tag{5.6}$$

The user experiences more inconvenience for a *Bad* system as compared to a *Good* system in terms of their robustness measure. User convenience $UC(t)$ is calculated from (5.4), (5.5) and (5.6) as

$$UC(t) = 1 - \left\{ \frac{C_1 P_a(t) + C_2 (1 - C_a(t)) + C_3 S_a(t)}{3} \right\} \tag{5.7}$$

Algorithm 4: Reward Matrix (R) Computation Algorithm

```
Initialize: $n, R(s,a) = Zeros(2^n - 1)$
Initialize: Threshold Power (Th)
Load      : Actual power consumption curve
while $(s,a)\ != (2^n - 1)$ do
    $R(s,a) \leftarrow -1$;   ($State\ Transition\ Not\ possible$)
    if cumulative power $\leq$ Th (Goal State) then
        $R(s,a) \leftarrow 0$;   ($Turning\ Off\ an\ Appliance$)
        $R(s,a) \leftarrow 1$;   ($transition\ to\ the\ same\ state$)
    else
        $R(s,a) \leftarrow 0$;   ($transition\ to\ the\ same\ state$)
        $R(s,a) \leftarrow UC(t)$;   ($Otherwise$)
    end
end
```

Reward matrix (R) is based on the user convenience values for each appliance using **Algorithm 4**. Size of the reward matrix depends on the number of appliances and the number of power levels the house agent can occupy. The size of the reward matrix for this problem is 255×255. Power level zero is not taken into consideration as it is impossible for the power to reduce to zero level in a home throughout the day. **Algorithm 4** depicts the steps to formulate the reward matrix and is true for any number of state

Algorithm 5: Reward Matrix (R) Computation Algorithm

```
{
    function UC($C_1,C_2,C_3,P_a,C_a,S_a$)
        if Goal reached without turning Off appliance then
            $UC(t) \leftarrow 1$
        end
        if Goal reached after turning Off appliance then
            $UC(t) \leftarrow 1 - UIC(t)$
        end
        if Goal not reached after turning Off appliance then
            $UC(t) \leftarrow 1 - UIC(t) - 0.2$
        end
        if Goal reached but resulting power level $\leq 0.6 \cdot Th$ then
            $UC(t) \leftarrow 1 - UIC(t) - 0.1$
        end
        $UC(t) \leftarrow 0$

        return $UC(t)$
}
```

transitions. According to required threshold power (Th) to be achieved, reward matrix $R(s,a)$ is computed as per **Algorithm 4**. Th is the goal state where the optimization of power stops. **Algorithm 5** depicts the process to compute the user convenience. The goal state may be reached with or without turning off an appliance. According to the power level where the goal state is reached, user convenience value is penalized. The most penalty is for goal state not being reached even after turning off an appliance. The penalties are 0.1 at goal state power less than or at 60% of threshold power and 0.2 for goal not being reached even after turning off an appliance.

5.4 Neural Fitted Q-based Home Energy Management

The proposed Neural Fitted Q-based Home Energy Management (*NFQbHEM*) algorithm is described in this section. The algorithm is based on RL based NFQI method as in Section 5.3. The algorithm works in three phases: exploration, training and application. In the exploration phase, NFQbHEM captures the historical demand data based on different seasons [163]. Winter month data has been chosen in our application. The algorithm is defined in **Algorithm 6** and the steps are listed as follows,

Algorithm 6: NFQbHEM Algorithm

```
Input   : Define $Q^0 = \overline{q}^0_{s,a} = 0$, $s_k = Th$
Output  : $\pi(s)$
$ITER \leftarrow 200$
$T^k \leftarrow empty\ set$
$\theta \leftarrow randomweight$
while ($||Q(s+1,a) - Q(s,a)|| < 10^{-4}$) do
    $\overline{q}^i_{s,a} = r(t) + \gamma \cdot MAX\ \overline{Q}^{i-1}(s(t+1),a(t))$ ;
    for 1:ITER do
        $T^k \leftarrow T^{k-1} \cup (s,a;\overline{q}^{i+1}_{s,a})$;
        $\delta \leftarrow \hat{Q}(s(t+1),a(t)) - \overline{Q}^i(s(t+1),a(t))$;
        $\phi_k(s,a) \leftarrow exp^{-\frac{||s-\overline{s}_k||^2}{2*\sigma_k^2}}$ ;
        $\theta \leftarrow \theta + \alpha\delta\phi(s,a)$;
    end
    $P(s,a) \leftarrow \frac{e^{ExplorationCount} \cdot age \cdot Q(s,a)}{\Sigma(e^{ExplorationCount} \cdot age \cdot Q(s,a))}$
end
return $\pi(s)$
```

Exploration Phase:

Step 0 (Inputs): Set the Q-factors to some arbitrary values (e.g. 0).

Step 1 : For each state s, the set of admissible actions, a is defined, and an action $a \in A$ is chosen randomly and applied. After applying $a(t)$ in $s(t)$, the next state $s(t+1)$ is reached and the immediate reward $r(t)$ from **Algorithm 4** is calculated.

Step 2 : The set of $(s(t),a(t),R(t),s(t+1))$ is inserted from the environment as a new sample F. Repeating the process, sufficient samples are found to train the algorithm.

Training Phase:

Step 1 : The training initializes $Q^0 = \overline{q}^0_{s,a} = 0$, and tries to find a function approximator $\hat{Q}^i$.

Step 2 : Similar to the Q-update process, append a corresponding pattern set T^k to the set $(s, a; \overline{q}^{i+1}_{s,a})$.

Step 3 : As our historical data is a curve fitting problem, Radial Basis Function Neural Network (RBFNN) [164] is chosen to approximate the function $Q(s, a)$.

Step 4 : The feature function ϕ : S x A maps each state-action pair to a vector of feature values.

Step 5 : θ is the weight vector specifying the contribution of each feature across all state-action pairs. The weight is updated at each iteration. The training is done for 200 iterations in our case.

Execution Phase:

Step 1 : Current data determine the state of the system.

Step 2 : A greedy policy is used to find the policy $\pi(s)$ as in (5.3).

Step 3 : Later in learning with more episodes, exploitation makes more sense because, with experience, the agent can be more confident about what it knows.

Step 4 : Stopping criterian with absolute error
$||Q(s+1, a) - Q(s, a)|| < 10^{-4}$.

5.5 Experimental Results

This section describes the results of HEMaaS platform with the *NFQbHEM* algorithm to control 10 appliances in a sample condo home in a smart community. The sample condo home is a one bedroom condo with 10 appliances connected wirelessly to the MCCU. Power measurements have been taken consistently for a month and *NFQbHEM* algorithm have been applied to the measured load. Due to the experimental nature of the setup and results, the results have been presented in the context of the sample condo home. Comparison with other architectures in literature have not been drawn as the method described here is unique to the setup and it would be unfair to compare algorithms with different setup. Due to hardware complexity, it is very hard to implement other algorithms for the setup explained in this Chapter. As explained in the software architecture and communication interface in Section 5.2.2, the MCCU consists of a Raspberry-Pi3 deploying a node-red platform. MQTT (Mosquitto) is used as the broker between the MCCU publisher and subscribing home appliances. Custom python code with the *NFQbHEM* algorithm deployed on it runs on the Raspberry-Pi3 to control the home appliances' *Delay/Pause/On/Off* operation via sonoff wi-fi switches through a MQTT gateway. The node-red dashboard interface designed in this Chapter offers an easy and convenient user interface (UI) for a homeowner to interact with the HEMaaS system. Figure 5.3 and Figure 5.4 illustrates our user interface (UI) flow design and dashboard control respectively. The UI shows the node-RED flow of the different appliances as connected to the MCCU. Each appliance is controlled through a GPIO pin and follows the Home/(Room)/(Device)/Pin hierarchy. The proposed UI also offers several visualization features to a user. They can have access to real-time and historical appliance usage information with graphs via the sonoff accumulated data information of real time power usage. User Input preferences (UIP) can be set via the dashboard. The different options which are available include setting a temperature for Heater-1, Heater-2, Heater-3 and washer-dryer, rescheduling washer-dryer operation and starting necessary appliances immediately bypassing the automated control for a particular duration. The UI is also accessible from anywhere in the world via the smartphone app. If for any reason there is a communication failure, the local settings of the appliances will take precedence.

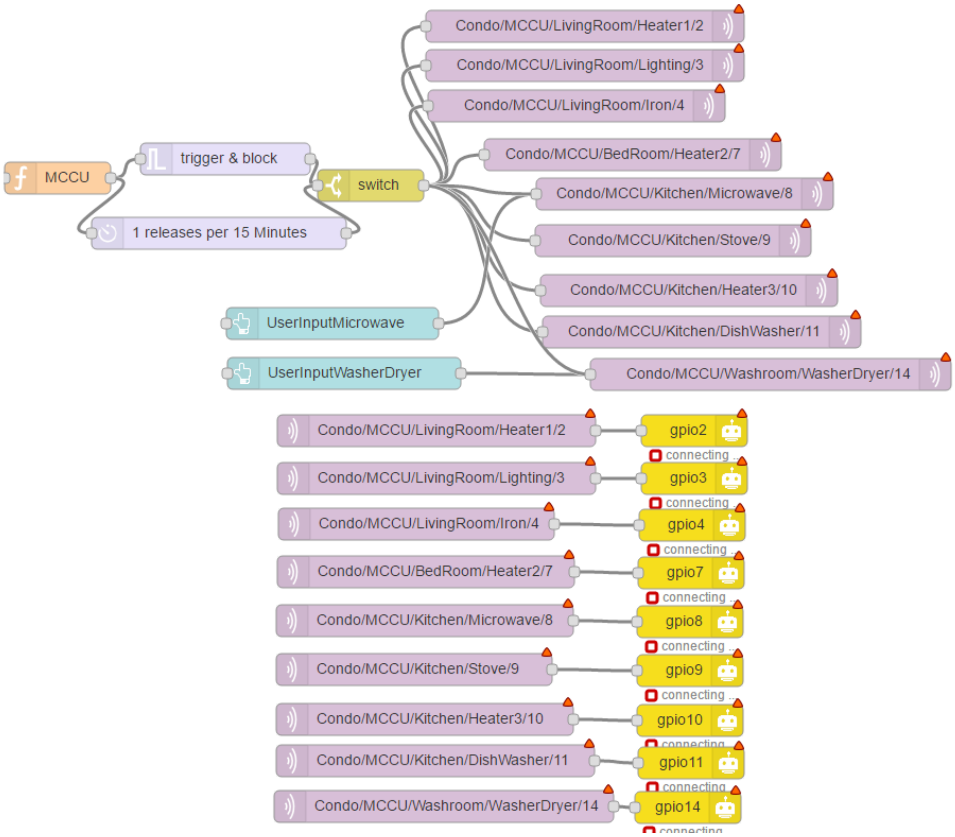

MCCU
trigger & block
1 releases per 15 Minutes
switch
UserInputMicrowave
UserInputWasherDryer
Condo/MCCU/LivingRoom/Heater1/2
Condo/MCCU/LivingRoom/Lighting/3
Condo/MCCU/LivingRoom/Iron/4
Condo/MCCU/BedRoom/Heater2/7
Condo/MCCU/Kitchen/Microwave/8
Condo/MCCU/Kitchen/Stove/9
Condo/MCCU/Kitchen/Heater3/10
Condo/MCCU/Kitchen/DishWasher/11
Condo/MCCU/Washroom/WasherDryer/14
Condo/MCCU/LivingRoom/Heater1/2
gpio2
connecting ...
Condo/MCCU/LivingRoom/Lighting/3
gpio3
connecting ...
Condo/MCCU/LivingRoom/Iron/4
gpio4
connecting ...
Condo/MCCU/BedRoom/Heater2/7
gpio7
connecting ...
Condo/MCCU/Kitchen/Microwave/8
gpio8
connecting ...
Condo/MCCU/Kitchen/Stove/9
gpio9
connecting ...
Condo/MCCU/Kitchen/Heater3/10
gpio10
connecting ...
Condo/MCCU/Kitchen/DishWasher/11
gpio11
connecting ...
Condo/MCCU/Washroom/WasherDryer/14
gpio14
connecting

Figure 5.3: User interface design.

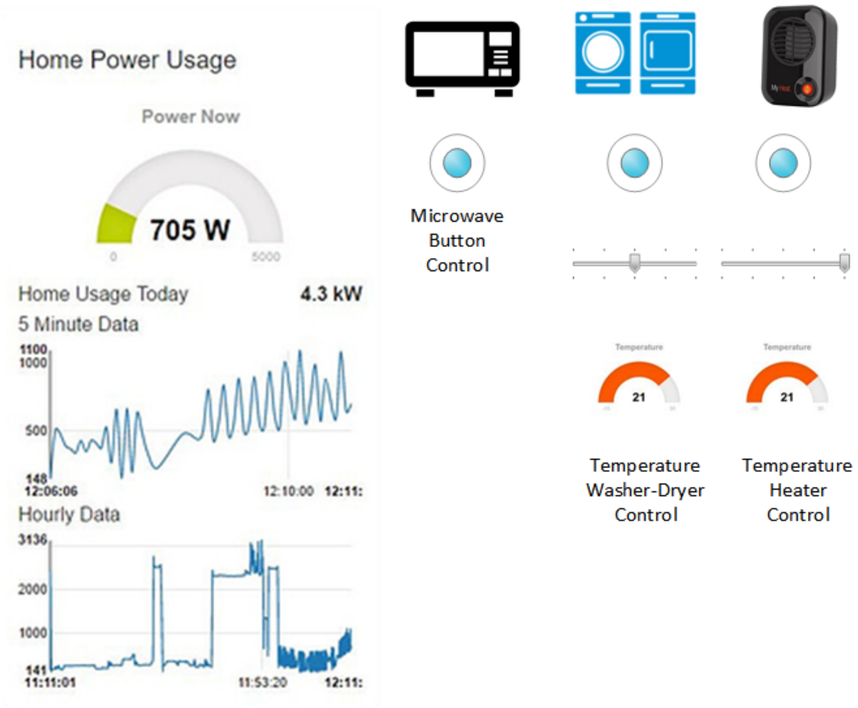


Figure 5.4: HEM interface.

Matplot library of python gives us the tool to analyse the power demand data for different cases. Two different cases have been discussed here for analyzing and plotting our results.

Case I : A sample day's total power consumption data is compared with different peak power reduction of $5\%, 10\%, 15\%$ and 20% of the total peak demand. The user convenience is also shown as a comparison.

Case II : The user convenience in terms of random (Good, medium and bad) behavior of the system is analyzed in this case.

For the **Case I** above, the energy in KWh savings and reduction in carbon-footprint for a community consisting of 85 condos of our typical architecture as in Section 5.2.1 is also plotted.

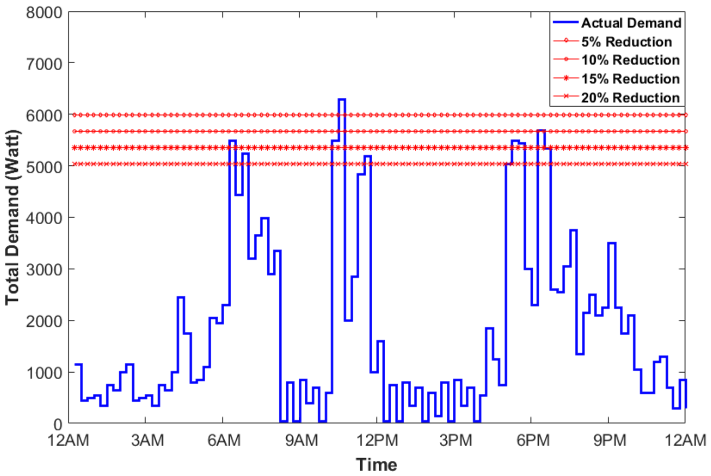


Figure 5.5: Plot of the total demand versus time during a typical Canadian winter month in Ontario

5.5.1 Case I

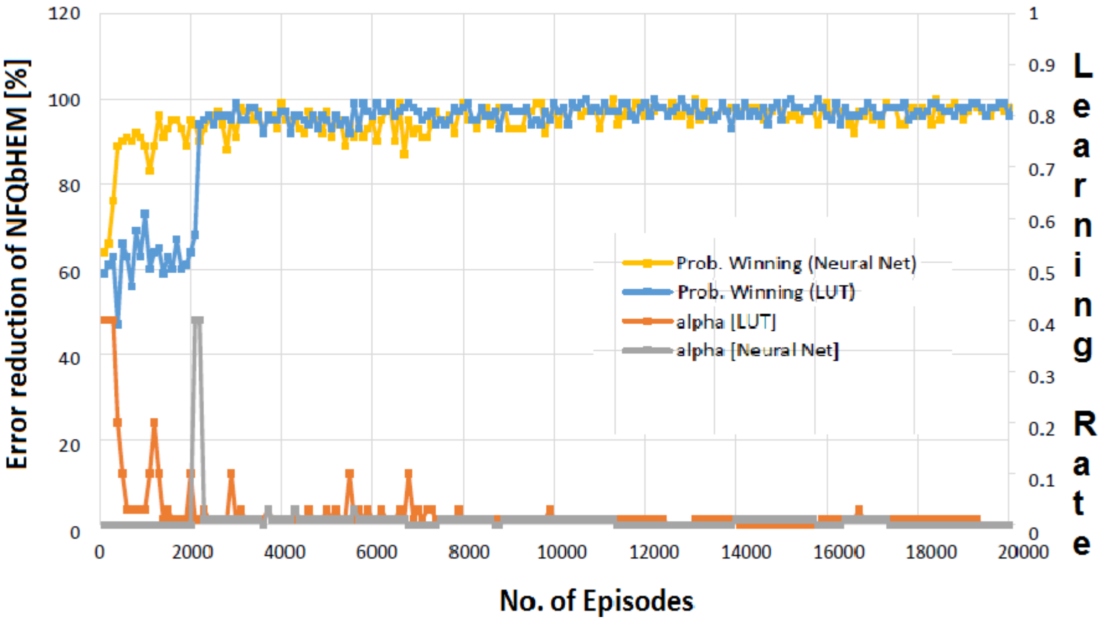


Figure 5.6: Plot of sample episodic run *NFQbHEM* learning process

In this section, the actual power consumption plot is generated using 10 smart appliances. The plot in Figure 5.5 shows the peak demand in watts versus time of the day. The interval of time duration is 15 minutes. Starting with initial $Q(s,a)$, the HEMaaS platform has to learn to find the optimal path when peak demand power during a certain interval exceeds the available power. The available power is taken as a percentage reduction of the peak power. $5\%, 10\%, 15\%$ and 20% are taken as the peak reduction percentages to test and validate our methodology. **Algorithm 6** has been initialized with starting parameters of learning $\alpha = 0.5$, discount $\gamma = 0.8$, A and B as 90 and 100 respectively. The center state $\bar{s}_k$ is taken as the median power consumed at a particular interval. The peak power is 6300 watts and **Algorithm 4** depicts the reward matrix initial computation. The total energy consumption historical data of a typical condo has been taken from national resources canada [165] for a typical winter month in Canadian ontario province. The feature function ϕ is derived from approximating the curve of the historical data and is used to train the weight vector θ. When the total power consumption is greater than the peak power power reduction, it selects actions (randomly) and moves from current state to a new state, receives reward and then it starts issuing control signals $(Delay/Pause/On/Off)$ to other appliances until one of the goal states is reached.

Figure 5.6 depicts the learning process of the *NFQbHEM* algorithm. The graph is plotted between number of episodes algorithm running for look-up table based Q-learning and the neural network Q-learning based *NFQbHEM* algorithm. The proposed algorithm learns faster and reaches a stable value in only about 570 episodes as compared to look-up only based Q-learning. The algorithm is stopped at 570 episodes as the error achieved is 10^{-5}. Thus neural network modeler helps the Q-learning achieve its goal state faster. Figure 5.7 shows the total demand versus time for different peak reduction percentages. Once the optimal policy is found, the MCCU will execute the sequence of rules (turning off appliances, rescheduling their timing of operation and temperature control one by one) until the goal state with maximum user convenience is reached. At the optimal policy, MCCU determines when the power goes above the desired reduction, it modifies its power as in Figure 5.7. Table 5.3 shows the appropriate actions taken by the MCCU unit at varied time intervals for different appliances.

Table 5.3: Actions taken by MCCU

Time	**Required Load Reduction**	**Required Action**
5% Reduction Threshold		
10:15-10:30 am	400 W	Turn off the Heater-1 and Heater-3
10% Reduction Threshold		
10:15-10:30 am	650 W	Turn off the Heater-1, Heater-2 and Heater-3
6:00-6:15 pm	600 W	Reduce the temp. setting of Heater-1
15% Reduction Threshold		
6:00-6:15 am	500 W	Reduce the temp. setting of Heater-1 and Heater-2
10:00-10:15 am	1500 W	The temperature setting of the washer-dryer may be changed to reduce the power demand or washer-dryer operation may be rescheduled to another time.
10:15-10:30 am	1500 W	The temperature setting of the washer-dryer may be changed to reduce the power demand or washer-dryer operation may be rescheduled to another time.
5:00-5:15 pm	250 W	Turn off the Heater-1
5:15-5:30 pm	300 W	Turn off the Heater-2
6:00-6:15 pm	600 W	Reduce the temp. setting of Heater-1

Time	Required Load Reduction	Required Action
20% Reduction Threshold		
6:00-6:15 am	500 W	Reduce the temp. setting of Heater-1 and Heter-2
6:30-6:45 am	500 W	Turn off the Heater-2
10:00-10:15 am	1500 W	The temperature setting of the washer-dryer may be changed to reduce the power demand or washer-dryer operation may be rescheduled to another time.
10:15-10:30 am	1500 W	The temperature setting of the washer-dryer may be changed to reduce the power demand or washer-dryer operation may be rescheduled to another time.
11:15-11:30 am	150 W	Refrigerator Turned Off
4:45-5:00 pm	150 W	Turn off the Refrigerator
5:15-5:30 pm	500 W	Turn off the Heater-3
5:30-5:45 pm	800 W	Turn off the Heater-2 and Heater-3
6:00-6:30 pm	600 W	Reduce the temp. setting of Heater-1

The user convenience (UC), is shown in Figure 5.8 for the four peak reduction threshold values. It can be inferred from the figures that the UC decreases with the increase in the threshold for power saving. Some of the peak load consumption which lies during the afternoon and evening time slots are affected severely. One suggestion of improvement in the user convenience could be having a variable thresholds for the *NFQbHEM* algorithm. Therefore the times of day having maximum user utility power consumption, the available power threshold can be increased and can be compensated with a lower available power threshold during other Off peak times while maintaining the overall average power threshold at the same level. If the user convenience level can be maintained more than 70% for most times of the day, then the HEMaaS system can

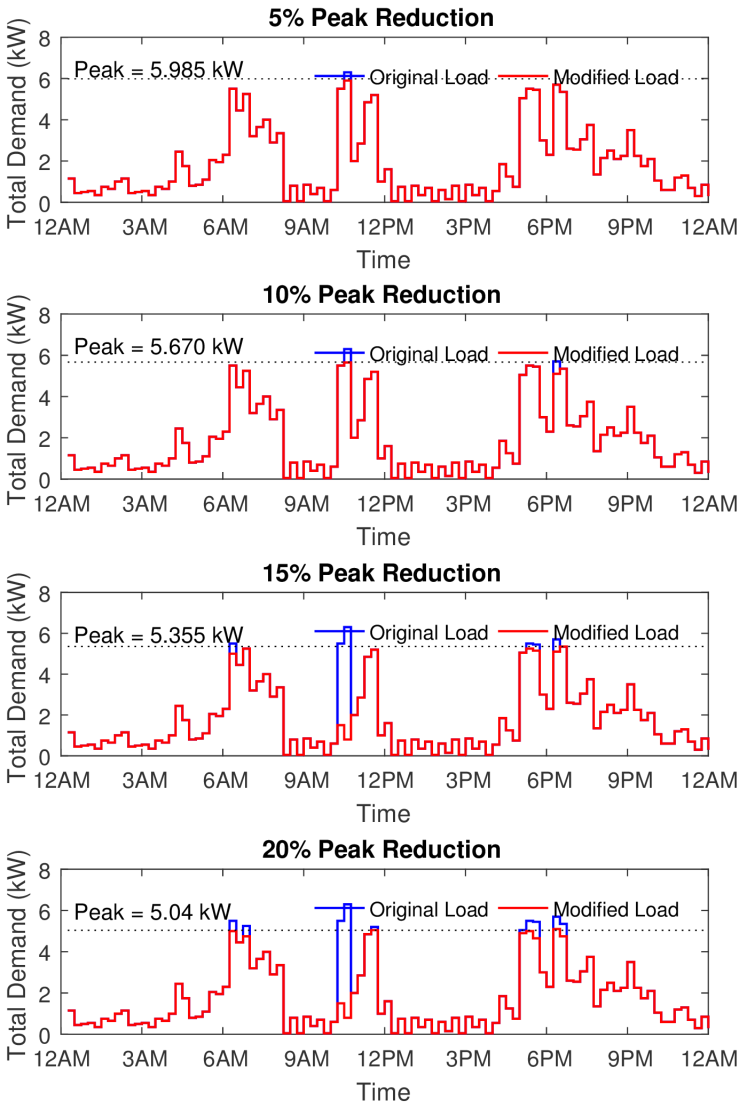


Figure 5.7: Plot of the total demand versus time for different peak reduction percentages

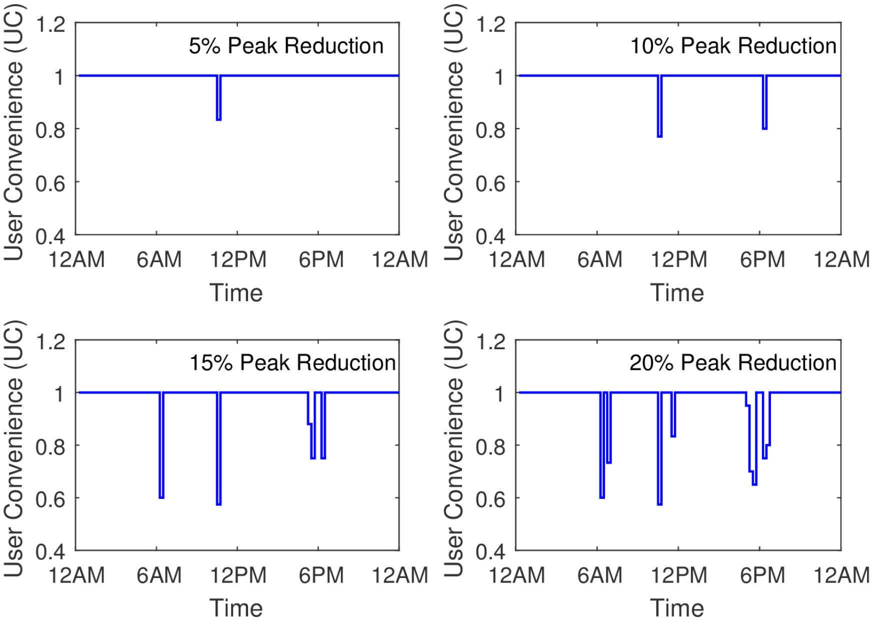


Figure 5.8: Plot of the user convenience (uc) versus time

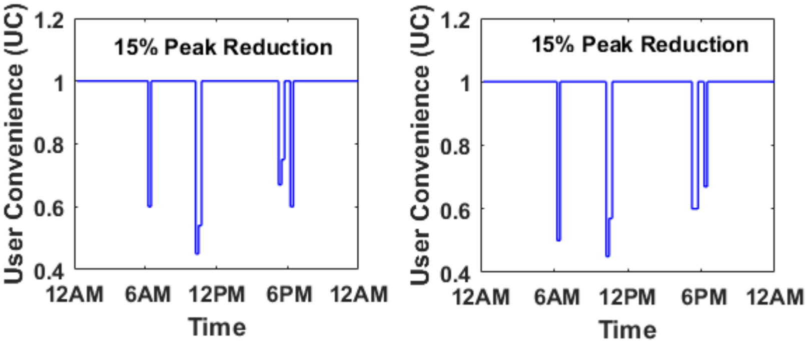


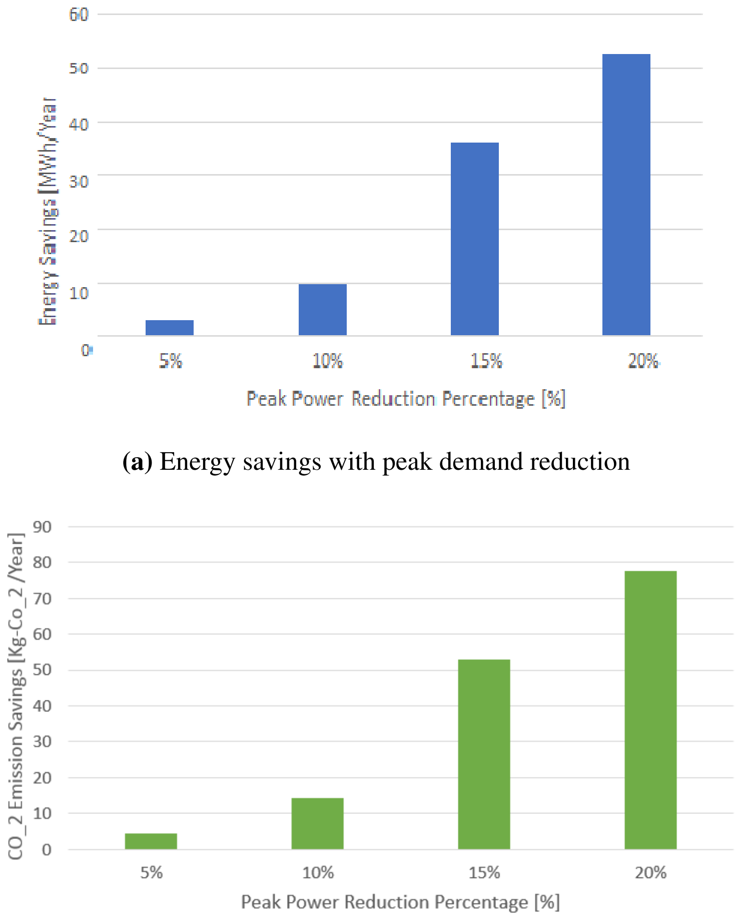
Figure 5.9: Plot of the user convenience (uc) versus time for (20% Good, 60% Medium and 20% Bad) and (10% Good, 40% Medium and 50% Bad) robustness measure.

be successful in delivering a coherent and inter-operable platform.

In this section, the behavioral modeling of the system is considered in terms its robustness. Robustness measure evaluates a systems quality in terms of security and fault tolerance. To simulate this behavior in the system, the $UC(t)$ from (5.6) has been chosen with randomly assigning measure of robustness C_3 at different time intervals. The power level of peak reduction at 15% is taken as the threshold. Figure 5.9 depicts the UC w.r.t the time of the day and is compared for two different situations. The first situation has (20% Good, 60% Medium and 20% Bad) robustness measure and the second situation has (10% Good, 40% Medium and 50% Bad) robustness measure respectively. The user convenience is severely affected for both cases specifically in the second situation, due to presence of more faulty/malicious channel. Thus security and fault tolerance is shown to have significant effect to the users. Once the UC goes below 50%, the system is considered as a very poorly managed system where users are forced to save energy sacrificing their comfort, which is highly undesirable.

5.5.2 Case II

The carbon intensity per KWh (CIPK) is a fundamental measure of a sustainable society. The lesser the CIPK, the better the society in terms of its environment and livability index. The energy savings that are obtained from results in Section 5.5.1 can be seen as potential price saving for the community as well as a means of reducing the CO_2 gas emissions. As Canada is progressing towards a sustainable green building infrastructure, it is a healthy sacrifice to have some inconvenience to achieve the greater benefit of having a greener environment in terms of achieving lesser carbon emissions. From [165], the Ontario province's CIPK is obtained as 125 $gr-CO_2$ per KWh. Using the CIPK, the energy savings and carbon emission savings have been computed for a community consisting of 85 condos. Figure 5.10 shows the energy savings in Mega-Watt-hour (MWh) per year. It also shows the carbon-footprint savings in $Kg - CO_2$ per year. The improvement is nearly 14 times from 5% to 15% peak power reduction, which is quite substantial.



(a) Energy savings with peak demand reduction

(b) Plot of carbon-footprint reduction

Figure 5.10: Comparison of peak reduction energy savings and carbon-footprint reductions

Chapter 6

Conclusions and Future Work

6.1 Summary and Conclusions

In this thesis, the major challenges of energy efficient implementation of architectures and technologies with respect to an IoE network have been discussed and different solutions to solve these problems have been critically evaluated. In Chapter 1, we have discussed the layered architecture of IoE systems and showed how physical layer, monitoring and security layers are linked to each other. Our thesis tackles the issue of energy-efficient implementation in these layers. In Section 1.2, we categorize the problem of energy-efficiency based on hardware design, wireless energy harvesting, energy saving policies, data transmission, management and control, and carbon-footprint generation for IoE networks. We have proposed solutions to the issues mentioned in Section 1.2 through Chapter 2-5. In Chapter 2 and Chapter 3, issues related node battery related issues are discussed and solutions were found out to increase the network lifetime through wireless energy harvesting, data transmission , error correction coding and data awareness. In summary the major take aways of the work in this thesis are as follows:

- The major contribution of the work in Chapter 2 is to provide a solution for data-utility lifetime trade-off problem by incorporating a detailed energy model combining various strategies of maximum network utilization and network lifetime increase by error correction, proper duty cycling and wireless battery energy replenishment. We provide user the flexibilty of choosing their system trade-off parameters by showing sumulation results for varied cases. This caters to a broad application scenario for the IoE systems having wireless sensing objects.
- Continuing our objective of saving energy, in Chapter 3, we have applied our energy model solution from Chapter 2 to save energy through data awareness in an event driven IoE system as compared to a traditional WSN system. Our first goal is to apply the energy saving problem with respect to a IoE system and then use the diversified nature of the IoE systems to solve the problem and save battery energy and increase network lifetime.
- Our major contribution in the Chapter 4, is the design of a low energy, resource limited PUF prototype current amplification circuit that mitigates the key attacks aimed at the system such as man in middle, cloning, and modelling attacks. Replicating and authenticating the system for the intruder is specifically blocked by our proposed solution. The results are verified by measurements and simulations. This provides the solution for an energy-efficient security design.
- After proposing, testing, validating and implementing energy-efficient design for individual layers and blocks in Fig. 1.2 through Chapter 2 to Chapter 3, in Chapter 5 we have implemented the algorithmic models in to smart homes as micro-

cosms of smart cities based on IoE systems (which has a system level implementation and application). This implementation deals with the policy-based issues that have an impact throughout the system architecture. Through measurements, we validated our energy and data awareness model incorporating security for a typical IoE application scenario. This gives the users of this work flexibility in choosing their system. It also shows the merits and demerits of applying each criteria of energy-efficient models of Chapter 2-4 to their overall convenience and system's QoS.

Specifically in Chapter 2, Wireless energy harvesting is investigated as a remedy to prolong the lifetime of sensor nodes and enable maintenance-free operation. Wake-up radio scheme is incorporated as an efficient solution to address the idle listening energy dissipation of sensor nodes. RRNS Error control coding is proposed to improve the reliability of the transmission and reduce re-transmission, hence, reducing energy consumption. A utility-lifetime maximization problem incorporating WEH, WUR and ECC schemes is formulated and solved using distributed dual subgradient algorithm based on Lagrange multiplier method. Simulation results verify the effectiveness of the proposed schemes in reducing the energy consumption and accordingly, carbon footprint of wireless sensor nodes, providing the means for a greener wireless sensor network.

In Chapter 3, we propose a Data aware energy efficient distributed clustering protocol for IoT (DAEECI) by saving CH selection energy using active RFID tags, cutting processing energy by incorporating data awareness factor in the system and improving lifetime by inculcating RF energy harvesting. We propose a PMU architecture that accommodates a battery charging scheme using the harvested energy through a WEH unit. We formulate energy consumption models in each round data is sent from sensor nodes to BS through gateway nodes. Our simulation depict substantial improvement in lifetime of network and data delivery to the BS.

The hardware-based related energy efficiency issues are dealt in Chapter 4. These issues are discussed in terms of security layer implementation of an IoE system. The energy-efficient security hardware design is an important part of the IoE system which can't be neglected. A hardware based energy-efficient PUF current amplication prototype have been developed and tested. Specifically, in Chapter4, we have proposed an IoT sensor PUF-based security design that exploits variations of physical sensor characteristics (e.g., dark current, is presented in this work) and challenge/response pair generation using the quadratic residue property. We have proposed algorithms for device authentication and encryption by using the PUF challenge/response outputs. Our analysis shows that there is strong relationship between the energy consumption of the sensor node and the dynamic range of the TransImpedance Amplifier (TIA) circuit, which is determined by signal strength and noise at the output of TIA. Thus, one of possible design choices for configuring the PUF circuit is to use RF = 50MOhm and CF= 10pF to get a dynamic range of 130.3 (7bits) with energy consumption of 0.157 J. Through simulations and measurements, we have shown that design is better in terms of energy and costs requirements than other state-of-the-art security algorithms. Moreover, it provides a two-fold secure data transfer and is resilient towards various attacks. This method can be extended to other IoT sensors, if suitable physically varying and unclonable circuit properties are chosen.

Energy management in smart cities is an indispensable challenge to address due to rapid urbanization. In Chapter 5, we first present an overview of energy management in smart homes to build a green and sustainable smart city, and then present a unifying framework for IoT in building green smart homes. To achieve our goal, a neural network based Q-learning algorithm is proposed to reduce the peak load demand of a typical Canadian home while minimizing the user inconvenience and enhancing the robustness of the system. The user convenience level for 5% and 10% load reduction is maintained at and above 80%. Whereas other levels of peak power reduction causes more discomfort for the users. While Canada Green Building Council is working towards finding ways of making buildings greener and community sustainable, a novel method has been applied for finding suitable strategies for efficient management of home energy demand and reducing the energy consumption during peak period in a typical Canadian condo. In a purely market-driven energy management environment, peak-reduction is mostly valuable for utilities. In order to make the demand side management more user friendly and consumer centric, a reward matrix based self-learning algorithm has been applied. The energy savings and carbon-footprint reduction is also shown to be quite significant. In future, it has been planned to incorporate real time scheduling into the system to schedule and pause appliance operation. Moreover, it is also proposed to design a system that learns from feedback smart sensors in the environment to ease the MCCU decision making and reduce user input, yet still maintaining a high enough user convenience.

6.2 Future Work

The approaches presented in this thesis are not exhaustive. In this section, we propose some possible research directions that can be followed from this thesis.

6.2.1 Highly Efficient, Low-cost, and Small-Form-Factor Wireless Energy Harvesting System

The key challenge in successful large-scale deployment of sensor devices in an IoE infrastructure is to minimize their impact on users and the environment. Non-intrusive devices need to be small, be fabricated and deployed at very low cost, and are expected to operate in a selfsufficient manner for a long time. A WEH unit as an integral part of such devices must comply with such cost and size requirements. Efficiency is another crucial factor for a WEH system. High efficiency becomes increasingly relevant considering that the transmitted power by the dedicated source is usually limited due to health issues and interference constraints. Commercial RF harvesting systems currently existing in the market enable single-band RF harvesting at sub-milliwatt power levels with efficiencies as high as 50 percent. However, extensive studies are still being carried out to improve the performance of WEH systems at the circuit and system levels. Energy beamforming [166], high gain antennas, and multi-band harvesting are among the other hot topics in the context of WEH systems for IoE.

6.2.2 Channel Statistics for IoE Systems

The scenarios and their respective analysis in our thesis in chapter 2 and Chapter 3 assume the channel as static and time invariant. Practically, channel characteristics vary depending on the environment in which the number of interferers and the number of paths available from source device to sink. Harvested energy depends on the distance between sink and sensor node. In the presence of fading or multipath, the received energy for the purpose of harvesting and the transmitted data are adversely affected. In [167], a compressive sensing based approach is proposed to recover sparse signals from multiple spatially correlated data transmitted to a fusion center. Recently, in [168], researchers have proposed techniques to reduce the amount of packets to be retransmitted in case of faulty transmission, eventually saving energy.

6.2.3 Cross-Layer Design

Although in Chapter 3 we have used data-awareness for our design in the physical layer, the sensor device still has to operate in duty-cycled mode due to limited energy collection from the environment, and dynamically adjust duty cycles to adapt to the availability of environmental energy. Such dynamic duty cycles pose challenges for medium access control (MAC) layer protocol design in terms of synchronization, reliability, efficiency of utilizing channel resource and energy, and so on. Therefore, solutions of duty-cycling-aware middleware between MAC and physical layer power management are highly desired. Moreover, dynamic duty cycling also has nontrivial impact on the end-to-end performance of the network layer, including end-to-end delay, throughput, and so on. However, the current routing protocol design for IoT has paid very little attention to duty cycling. The problem of seamlessly integrating duty-cycle awareness into the multi-path routing scenario has been dealt with in [169] using a sleep scheduling mechanism; however, it still remains an open question.

6.2.4 Security and Privacy Concerns

In Chapter 4, we have not dealt with profiles of same manufacturer's photodiode dark currents in detail. In the future work, investigating the range of dark current profile for the large sample of the same type of photodiode can provide a useful background to determine the required range of bias voltage. Then, the existing actual dark current profile can be used to evaluate the necessity of a step-up voltage converter which can boost the typical voltage range used for a microcontroller (3.3V 5.0V) to the voltage level which is large enough for biasing a photodiode. In our prototype circuit, separate discrete components such as a TIA and an opamp were used with an external power source. However, these circuits can be more optimally designed and integrated in a single die to increase the performance of a sensor node such as lower noise and reduced power consumption. Integrating to a single chip would also increase the portability of a sensor node, which is one of key requirements for IoT application.

6.2.5 Home Energy Management

Real-time management is a challenging issue for resource constrained sensor networks. In the Chapter 5, the IoE system needs to rely on effcient service gateway to minimize the amount of data to be sent by constantly receiving the feedback data from users, and intelligent data oriented middleware design to only transmit real time information when a reward matrix is to be calculated. The modelling is done through radial-basis neural network. In future works, deep learning with boosting can be applied to faster train the data to achieve better models.

Dynamic registration, bootstrap and management will be particularly considered for a large scale deployment with devices coming in and out and changing their characteristics and functionalities. The IoE device management should be suitable to develop an open and universal ecosystem with sustainable interactions and interoperability among things.

Bibliography

[1] D. Evans, *The Internet of Everything: How More Relevant and Valuable Connections Will Change the World*. CISCO Internet Business Solutions Group (IBSG), 2012. [Online]. Available: https://www.cisco.com/c/dam/global/en_my/assets/ciscoinnovate/pdfs/IoE.pdf

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of things for smart cities,” *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, Feb 2014.

[3] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. Mccann, and K. K. Leung, “A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities,” *IEEE Wireless Communications*, vol. 20, no. 6, pp. 91–98, December 2013.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.

[5] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[6] S. Sen, J. Koo, and S. Bagchi, “Trifecta: Security, energy efficiency, and communication capacity comparison for wireless iot devices,” *IEEE Internet Computing*, vol. 22, no. 1, pp. 74–81, Jan 2018.

[7] IEEE-SA-P2413, *Standard for an Architectural Framework for the Internet of Things (IoT)*. IEEE Standards Association, 2016. [Online]. Available: http://grouper.ieee.org/groups/2413/Intro-to-IEEE-P2413.pdf

[8] A. Ahmed and E. Ahmed, “A survey on mobile edge computing,” in *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, Jan 2016, pp. 1–8.

[9] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct 2017.

[10] R. Arshad, S. Zahoor, M. A. Shah, A. Wahid, and H. Yu, "Green iot: An investigation on energy saving practices for 2020 and beyond," *IEEE Access*, vol. 5, pp. 15 667–15 681, 2017.

[11] J. Huang, Y. Meng, X. Gong, Y. Liu, and Q. Duan, "A novel deployment scheme for green internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 196–205, April 2014.

[12] R. Want, B. N. Schilit, and S. Jenson, "Enabling the internet of things," *Computer*, vol. 48, no. 1, pp. 28–35, Jan 2015.

[13] D. Bol, J. D. Vos, F. Botman, G. de Streel, S. Bernard, D. Flandre, and J. D. Legat, "Green socs for a sustainable internet-of-things," in *2013 IEEE Faible Tension Faible Consommation*, June 2013, pp. 1–4.

[14] Y. W. Lim, S. B. Daas, S. J. Hashim, R. M. Sidek, N. A. Kamsani, and F. Z. Rokhani, "Reduced hardware architecture for energy-efficient iot healthcare sensor nodes," in *2015 IEEE International Circuits and Systems Symposium (ICSyS)*, Sept 2015, pp. 90–95.

[15] M. Sain, Y. J. Kang, and H. J. Lee, "Survey on security in internet of things: State of the art and challenges," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, Feb 2017, pp. 699–704.

[16] A. M. Nia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. PP, no. 99, pp. 1–1, 2017.

[17] J. Gilbert and F. Balouchi, "Comparison of energy harvesting systems for wireless sensor networks," *International Journal of Automation and Computing*, vol. 5, no. 4, pp. 334–347, 2008.

[18] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *CoRR*, vol. abs/1406.6470, 2014. [Online]. Available: http://arxiv.org/abs/1406.6470

[19] C. Mahapatra, Z. Sheng, V. Leung, and T. Stouraitis, "A reliable and energy efficient iot data transmission scheme for smart cities based on redundant residue based error correction coding," in *Sensing, Communication, and Networking -*

Workshops (SECON Workshops), 2015 12th Annual IEEE International Conference on, June 2015, pp. 1–6.

[20] X. Peng, M. Bessho, N. Koshizuka, and K. Sakamura, "Epdl: Supporting context-based energy control policy design in iot-enabled smart buildings: Programing the physical world with epdl," in *Data Science and Data Intensive Systems (DSDIS), 2015 IEEE International Conference on*. IEEE, 2015, pp. 297–303.

[21] A. Fensel, V. Kumar, and S. D. K. Tomic, "End-user interfaces for energy-efficient semantically enabled smart homes," *Energy Efficiency*, vol. 7, no. 4, pp. 655–675, 2014.

[22] M. Moreno, B. Úbeda, A. F. Skarmeta, and M. A. Zamora, "How can we tackle energy efficiency in iot basedsmart buildings?" *Sensors*, vol. 14, no. 6, pp. 9582–9614, 2014.

[23] E. Capo-Chichi, H. Guyennet, and J.-M. Friedt, "K-rle: A new data compression algorithm for wireless sensor network," in *Sensor Technologies and Applications, 2009. SENSORCOMM '09. Third International Conference on*, June 2009, pp. 502–507.

[24] T. Schoellhammer, B. Greenstein, E. Osterweil, M. Wimbrow, and D. Estrin, "Lightweight temporal compression of microclimate datasets [wireless sensor networks]," in *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*, Nov 2004, pp. 516–524.

[25] N. Xu, S. Rangwala, K. K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin, "A wireless sensor network for structural monitoring," in *Proceedings of the 2Nd International Conference on Embedded Networked Sensor Systems*, ser. SenSys '04. New York, NY, USA: ACM, 2004, pp. 13–24. [Online]. Available: http://doi.acm.org/10.1145/1031495.1031498

[26] M. Rubin and T. Camp, "On-mote compressive sampling to reduce power consumption for wireless sensors," in *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2013 10th Annual IEEE Communications Society Conference on*, June 2013, pp. 291–299.

[27] E. Candes and M. Wakin, "An introduction to compressive sampling," *Signal Processing Magazine, IEEE*, vol. 25, no. 2, pp. 21–30, March 2008.

[28] N. Kimura and S. Latifi, "A survey on data compression in wireless sensor networks," in *Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on*, vol. 2, April 2005, pp. 8–13 Vol. 2.

[29] G. Bovet, A. Ridi, and J. Hennebert, “Machine learning with the internet of virtual things,” in *Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), 2015 International Conference on*, July 2015, pp. 1–8.

[30] *GeSi better 2030.* GeSi, 2018. [Online]. Available: http://smarter2030.gesi.org/

[31] F. P. Kelly, A. K. Maulloo, and D. K. Tan, “Rate control for communication networks: shadow prices, proportional fairness and stability,” *Journal of the Operational Research society*, pp. 237–252, 1998.

[32] R. Madan and S. Lall, “Distributed algorithms for maximum lifetime routing in wireless sensor networks,” *Wireless Communications, IEEE Transactions on*, vol. 5, no. 8, pp. 2185–2193, Aug 2006.

[33] S. Ehsan, B. Hamdaoui, and M. Guizani, “Radio and medium access contention aware routing for lifetime maximization in multichannel sensor networks,” *Wireless Communications, IEEE Transactions on*, vol. 11, no. 9, pp. 3058–3067, September 2012.

[34] J. Chen, W. Xu, S. He, Y. Sun, P. Thulasiraman, and X. Shen, “Utility-based asynchronous flow control algorithm for wireless sensor networks,” *Selected Areas in Communications, IEEE Journal on*, vol. 28, no. 7, pp. 1116–1126, Sep. 2010.

[35] S. He, J. Chen, D. Yau, and Y. Sun, “Cross-layer optimization of correlated data gathering in wireless sensor networks,” in *Sensor Mesh and Ad Hoc Communications and Networks (SECON), 2010 7th Annual IEEE Communications Society Conference on*, June 2010, pp. 1–9.

[36] D. S. Lun, M. Médard, R. Koetter, and M. Effros, “On coding for reliable communication over packet networks,” *Physical Communication*, vol. 1, no. 1, pp. 3–20, 2008.

[37] K. Yu, F. Barac, M. Gidlund, and J. Akerberg, “Adaptive forward error correction for best effort wireless sensor networks,” in *Communications (ICC), 2012 IEEE International Conference on*, June 2012, pp. 7104–7109.

[38] W. Xu, Q. Shi, X. Wei, Z. Ma, X. Zhu, and Y. Wang, “Distributed optimal rate reliability lifetime tradeoff in time varying wireless sensor networks,” *Wireless Communications, IEEE Transactions on*, vol. 13, no. 9, pp. 4836–4847, Sept 2014.

[39] J. Zou, H. Xiong, C. Li, R. Zhang, and Z. He, "Lifetime and distortion optimization with joint source/channel rate adaptation and network coding-based error control in wireless video sensor networks," *Vehicular Technology, IEEE Transactions on*, vol. 60, no. 3, pp. 1182–1194, March 2011.

[40] T. He, K.-W. Chin, and S. Soh, "On wireless power transfer and max flow in rechargeable wireless sensor networks," *IEEE Access*, vol. 4, pp. 4155–4167, 2016.

[41] M. Magno, D. Boyle, D. Brunelli, E. Popovici, and L. Benini, "Ensuring survivability of resource-intensive sensor networks through ultra-low power overlays," *Industrial Informatics, IEEE Transactions on*, vol. 10, no. 2, pp. 946–956, May 2014.

[42] R. Deng, Y. Zhang, S. He, J. Chen, and X. Shen, "Globally optimizing network utility with spatiotemporally-coupled constraint in rechargeable sensor networks," in *Global Communications Conference (GLOBECOM), 2013 IEEE*, Dec 2013, pp. 4810–4815.

[43] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. Leung, and Y. L. Guan, "Wireless energy harvesting for the internet of things," *Communications Magazine, IEEE*, vol. 53, no. 6, pp. 102–108, June 2015.

[44] Z. Mao, C. Koksal, and N. Shroff, "Near optimal power and rate control of multi-hop sensor networks with energy replenishment: Basic limitations with finite energy and data storage," *Automatic Control, IEEE Transactions on*, vol. 57, no. 4, pp. 815–829, April 2012.

[45] S. Chen, P. Sinha, N. Shroff, and C. Joo, "Finite-horizon energy allocation and routing scheme in rechargeable sensor networks," in *INFOCOM, 2011 Proceedings IEEE*, April 2011, pp. 2273–2281.

[46] A. Biason and M. Zorzi, "Joint online transmission and energy transfer policies for energy harvesting devices with finite batteries," in *European Wireless 2015; 21th European Wireless Conference; Proceedings of.* VDE, 2015, pp. 1–7.

[47] G. Koutitas, "Green network planning of single frequency networks," *Broadcasting, IEEE Transactions on*, vol. 56, no. 4, pp. 541–550, Dec 2010.

[48] M. Naeem, U. Pareek, D. C. Lee, and A. Anpalagan, "Estimation of distribution algorithm for resource allocation in green cooperative cognitive radio sensor networks," *Sensors*, vol. 13, no. 4, pp. 4884–4905, 2013.

[49] J. N. Al-Karaki and A. E. Kamal, “Routing techniques in wireless sensor networks: a survey,” *Wireless communications, IEEE*, vol. 11, no. 6, pp. 6–28, 2004.

[50] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “An application-specific protocol architecture for wireless microsensor networks,” *Wireless Communications, IEEE Transactions on*, vol. 1, no. 4, pp. 660–670, 2002.

[51] S. Lindsey and C. Raghavendra, “Pegasis: Power-efficient gathering in sensor information systems,” in *Aerospace Conference Proceedings, 2002. IEEE*, vol. 3, 2002, pp. 3–1125–3–1130 vol.3.

[52] O. Younis and S. Fahmy, “Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks,” *Mobile Computing, IEEE Transactions on*, vol. 3, no. 4, pp. 366–379, 2004.

[53] L. Qing, Q. Zhu, and M. Wang, “Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks,” *Computer communications*, vol. 29, no. 12, pp. 2230–2237, 2006.

[54] T. Qureshi, N. Javaid, M. Malik, U. Qasim, and Z. Khan, “On performance evaluation of variants of deec in wsns,” in *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on*, Nov 2012, pp. 162–169.

[55] K. Zhao and L. Ge, “A survey on the internet of things security,” in *2013 Ninth International Conference on Computational Intelligence and Security*, Dec 2013, pp. 663–667.

[56] J. Granjal, E. Monteiro, and J. S. Silva, “Security for the internet of things: A survey of existing protocols and open research issues,” *IEEE Communications Surveys Tutorials*, vol. 17, no. 3, pp. 1294–1312, thirdquarter 2015.

[57] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, 2007.

[58] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC press, 1996.

[59] C. Karlof, N. Sastry, and D. Wagner, “TinySec: a link layer security architecture for wireless sensor networks,” in *Proceedings of the 2nd international conference on Embedded networked sensor systems*. ACM, 2004, pp. 162–175.

[60] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of things,” *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[61] M. Potkonjak and V. Goudar, “Public Physical Unclonable Functions,” *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1142–1156, Aug. 2014.

[62] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial,” *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[63] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, “Emerging physical unclonable functions with nanotechnology,” *IEEE Access*, vol. 4, pp. 61–80, 2016.

[64] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, “Modeling attacks on physical unclonable functions,” in *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010, pp. 237–249.

[65] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, “Fpga intrinsic pufs and their use for ip protection,” in *CHES*, vol. 4727. Springer, 2007, pp. 63–80.

[66] S. S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen, and P. Tuyls, “Extended abstract: The butterfly puf protecting ip on every fpga,” in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, June 2008, pp. 67–70.

[67] P. Tuyls, G.-J. Schrijen, B. Škorić, J. Van Geloven, N. Verhaegh, and R. Wolters, “Read-proof hardware from protective coatings,” in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2006, pp. 369–383.

[68] J. Delvaux, D. Gu, D. Schellekens, and I. Verbauwhede, “Secure lightweight entity authentication with strong pufs: Mission impossible?” in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2014, pp. 451–475.

[69] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, “Puf modeling attacks on simulated and silicon data,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1876–1891, 2013.

[70] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, “Physical one-way functions,” *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[71] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, “Silicon physical random functions,” in *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 2002, pp. 148–160.

[72] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of the 44th annual design automation conference*. ACM, 2007, pp. 9–14.

[73] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200–1205, Oct 2005.

[74] J.-L. Zhang, G. Qu, Y.-Q. Lv, and Q. Zhou, "A survey on silicon pufs and recent advances in ring oscillator pufs," *Journal of computer science and technology*, vol. 29, no. 4, pp. 664–678, 2014.

[75] D. Choi, S. H. Seo, Y. S. Oh, and Y. Kang, "Two-factor fuzzy commitment for unmanned iot devices security," *IEEE Internet of Things Journal*, pp. 1–1, 2018.

[76] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer, "Implementation and characterization of a physical unclonable function for iot: A case study with the tero-puf," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 1, pp. 97–109, Jan 2018.

[77] D. Mukhopadhyay, "Pufs as promising tools for security in internet of things," *IEEE Design Test*, vol. 33, no. 3, pp. 103–115, June 2016.

[78] B. Zhou, W. Li, K. W. Chan, Y. Cao, Y. Kuang, X. Liu, and X. Wang, "Smart home energy management systems: Concept, configurations, and scheduling strategies," *Renewable and Sustainable Energy Reviews*, vol. 61, pp. 30–40, 2016.

[79] D. Díaz Pardo de Vera, A. Siguenza Izquierdo, J. Bernat Vercher, and L. A. Hernández Gómez, "A ubiquitous sensor network platform for integrating smart devices into the semantic sensor web," *Sensors*, vol. 14, no. 6, pp. 10 725–10 752, 2014. [Online]. Available: http://www.mdpi.com/1424-8220/14/6/10725

[80] H. Farhangi, "The path of the smart grid," *IEEE power and energy magazine*, vol. 8, no. 1, 2010.

[81] A. Kumar and G. Hancke, "An energy-efficient smart comfort sensing system based on the IEEE 1451 standard for green buildings," *IEEE Sensors Journal*, vol. 14, no. 12, pp. 4245–4252, 2014.

[82] V. R. Shen, C.-Y. Yang, and C. H. Chen, "A smart home management system with hierarchical behavior suggestion and recovery mechanism," *Computer Standards & Interfaces*, vol. 41, pp. 98–111, 2015.

[83] M. Rahman, M. Kuzlu, M. Pipattanasomporn, and S. Rahman, “Architecture of web services interface for a home energy management system,” *Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES*, pp. 1–5, 2014.

[84] Y.-T. Lee, W.-H. Hsiao, C.-M. Huang, and T. C. Seng-cho, “An integrated cloud-based smart home management system with community hierarchy,” *IEEE Transactions on Consumer Electronics*, vol. 62, no. 1, pp. 1–9, 2016.

[85] F. Ciancetta, B. D’Apice, D. Gallo, and C. Landi, “Plug-n-play smart sensor based on web service,” *IEEE Sensors Journal*, vol. 7, no. 5, pp. 882–889, 2007.

[86] C. Chen, J. Wang, Y. Heo, and S. Kishore, “Mpc-based appliance scheduling for residential building energy management controller,” *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1401–1410, 2013.

[87] S. Li, D. Zhang, A. B. Roget, and Z. O’Neill, “Integrating home energy simulation and dynamic electricity price for demand response study,” *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 779–788, 2014.

[88] Q. Wei, F. L. Lewis, G. Shi, and R. Song, “Error-tolerant iterative adaptive dynamic programming for optimal renewable home energy scheduling and battery management,” *IEEE Transactions on Industrial Electronics*, vol. 64, no. 12, pp. 9527–9537, Dec 2017.

[89] A.-H. Mohsenian-Rad, V. W. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, “Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid,” *IEEE transactions on Smart Grid*, vol. 1, no. 3, pp. 320–331, 2010.

[90] K. Dehghanpour, H. Nehrir, J. Sheppard, and N. Kelly, “Agent-based modeling of retail electrical energy markets with demand response,” *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[91] M. Magno, T. Polonelli, L. Benini, and E. Popovici, “A low cost, highly scalable wireless sensor network solution to achieve smart led light control for green buildings,” *IEEE Sensors Journal*, vol. 15, no. 5, pp. 2963–2973, 2015.

[92] D. O’Neill, M. Levorato, A. Goldsmith, and U. Mitra, “Residential demand response using reinforcement learning,” *2010 First IEEE International Conference on Smart Grid Communications*, pp. 409–414, 2010.

[93] F. Ruelens, B. J. Claessens, S. Vandael, S. Iacovella, P. Vingerhoets, and R. Belmans, “Demand response of a heterogeneous cluster of electric water heaters using batch reinforcement learning,” *2014 Power Systems Computation Conference*, pp. 1–7, 2014.

[94] K. Turitsyn, S. Backhaus, M. Ananyev, and M. Chertkov, “Smart finite state devices: A modeling framework for demand response technologies,” *2011 50th IEEE Conference on Decision and Control and European Control Conference*, pp. 7–14, 2011.

[95] E. C. Kara, M. Berges, B. Krogh, and S. Kar, “Using smart devices for system-level management and control in the smart grid: A reinforcement learning framework,” *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, pp. 85–90, 2012.

[96] G. Deak, K. Curran, and J. Condell, “A survey of active and passive indoor localisation systems,” *Computer Communications*, vol. 35, no. 16, pp. 1939–1954, 2012.

[97] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, “Wireless networks with rf energy harvesting: A contemporary survey,” *IEEE Communications Surveys Tutorials*, vol. 17, no. 2, pp. 757–789, Secondquarter 2015.

[98] S. Boyd and L. Vandenberghe, *Convex optimization.* Cambridge university press, 2004.

[99] H. How, T. Liew, E.-L. Kuan, L.-L. Yang, and L. Hanzo, “A redundant residue number system coded burst-by-burst adaptive joint-detection based cdma speech transceiver,” *Vehicular Technology, IEEE Transactions on*, vol. 55, no. 1, pp. 387–396, Jan 2006.

[100] B. Zarei, V. Muthukkumarasay, and X.-W. Wu, “A residual error control scheme in single-hop wireless sensor networks,” in *Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference on*, March 2013, pp. 197–204.

[101] M. C. Vuran and I. Akyildiz, “Error control in wireless sensor networks: A cross layer analysis,” *Networking, IEEE/ACM Transactions on*, vol. 17, no. 4, pp. 1186–1199, Aug 2009.

[102] J.-D. Sun and H. Krishna, “A coding theory approach to error control in redundant residue number systems. ii. multiple error detection and correction,” *Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on*, vol. 39, no. 1, pp. 18–34, Jan 1992.

[103] W. Jenkins and E. Altman, “Self-checking properties of residue number error checkers based on mixed radix conversion,” *Circuits and Systems, IEEE Transactions on*, vol. 35, no. 2, pp. 159–167, Feb 1988.

[104] M. Russo, P. Šolić, and M. Stella, "Probabilistic modeling of harvested GSM energy and its application in extending UHF RFID tags reading range," *Journal of Electromagnetic Waves and Applications*, vol. 27, no. 4, pp. 473–484, 2013. [Online]. Available: http://dx.doi.org/10.1080/09205071.2013.753659

[105] P. Kamalinejad, K. Keikhosravy, R. Molavi, S. Mirabbasi, and V. Leung, "Efficiency enhancement techniques and a dual-band approach in RF rectifiers for wireless power harvesting," in *IEEE International Symposium on Circuits and Systems (ISCAS),*, June 2014, pp. 2049–2052.

[106] V. Jelicic, M. Magno, D. Brunelli, V. Bilas, and L. Benini, "Analytic comparison of wake-up receivers for WSNs and benefits over the wake-on radio scheme," in *Proceedings of the 7th ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks*, ser. PM2HW2N '12. New York, NY, USA: ACM, 2012, pp. 99–106. [Online]. Available: http://doi.acm.org/10.1145/2387191.2387206

[107] V. Jelicic, M. Magno, D. Brunelli, V. Bilas, L. Benini, "Benefits of wake-up radio in energy-efficient multimodal surveillance wireless sensor network," *IEEE Sensors Journal,*, vol. 14, no. 9, pp. 3210–3220, Sept 2014.

[108] P. Kamalinejad, K. Keikhosravy, M. Magno, S. Mirabbasi, V. Leung, and L. Benini, "A high-sensitivity fully passive wake-up radio front-end for wireless sensor nodes," in *IEEE International Conference on Consumer Electronics (ICCE),*, Jan 2014, pp. 209–210.

[109] M. Bhardwaj and A. Chandrakasan, "Bounding the lifetime of sensor networks via optimal role assignments," in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 3, 2002, pp. 1587–1596 vol.3.

[110] M. A. Razzaque and S. Dobson, "Energy-efficient sensing in wireless sensor networks using compressed sensing," *Sensors*, vol. 14, no. 2, pp. 2822–2859, 2014.

[111] O. Arnold, F. Richter, G. Fettweis, and O. Blume, "Power consumption modeling of different base station types in heterogeneous cellular networks," in *Future Network and Mobile Summit, 2010*, June 2010, pp. 1–8.

[112] E. Olivetti, J. Gregory, and R. Kirchain, "Life cycle impacts of alkaline batteries with a focus on end-of-life," *Study Conducted for the National Electrical Manufacturers Association*, 2011.

[113] D. Kumar, "Performance analysis of energy efficient clustering protocols for maximising lifetime of wireless sensor networks," *Wireless Sensor Systems, IET*, vol. 4, no. 1, pp. 9–16, March 2014.

[114] J. Yu, Y. Qi, G. Wang, and X. Gu, "A cluster-based routing protocol for wireless sensor networks with nonuniform node distribution," {*AEU*} *- International Journal of Electronics and Communications*, vol. 66, no. 1, pp. 54 – 61, 2012.

[115] M. Hossain and V. Prybutok, "Consumer acceptance of rfid technology: An exploratory study," *Engineering Management, IEEE Transactions on*, vol. 55, no. 2, pp. 316–328, May 2008.

[116] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with rf energy harvesting: A contemporary survey," *Communications Surveys Tutorials, IEEE*, vol. 17, no. 2, pp. 757–789, 2015.

[117] H. Ostaffe, "Rf-based wireless charging and energy harvesting." [Online]. Available: https://www.mouser.ca/applications/rf_energy_harvesting/

[118] S. S. Kumar and K. Kashwan, "Research study of energy harvesting in wireless sensor networks," *International Journal of Renewable Energy Research (IJRER)*, vol. 3, no. 3, pp. 745–753, 2013.

[119] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on fpgas," in *Reconfigurable Computing and FPGAs (ReConFig), 2010 International Conference on*. IEEE, 2010, pp. 298–303.

[120] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded systems design with FPGAs*. Springer, 2013, pp. 245–267.

[121] A. Alvarez, W. Zhao, and M. Alioto, "14.3 15fJ/b static physically unclonable functions for secure chip identification with $<$2% native bit instability and 140x Inter/Intra PUF hamming distance separation in 65nm," in *IEEE International Solid- State Circuits Conference (ISSCC)*, Feb. 2015, pp. 256–257.

[122] P. Pongle and G. Chavan, "A survey: Attacks on rpl and 6lowpan in iot," in *2015 International Conference on Pervasive Computing (ICPC)*, Jan 2015, pp. 1–6.

[123] C. Mahapatra, P. Kamalinejad, T. Stouraitis, S. Mirabbasi, and V. C. M. Leung, "Low-complexity energy-efficient security approach for e-health applications based on physically unclonable functions of sensors," in *2015 IEEE International Conference on Electronics, Circuits, and Systems (ICECS)*, Dec 2015, pp. 531–534.

[124] "AFE4400 Integrated Analog Front-End for Heart Rate Monitors and Low-Cost Pulse Oximeters," http://www.ti.com/lit/ds/symlink/afe4400.pdf, Accessed: 2015/10/20.

[125] C. Mathas, "Infrared sensors evolve from military to iot applications," Electronic Products, NewYork, , Sept 2014.

[126] V. Paliouras and T. Stouraitis, "Novel high-radix residue number system architectures," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 47, no. 10, pp. 1059–1073, Oct 2000.

[127] D. Schinianakis and T. Stouraitis, "Multifunction residue architectures for cryptography," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 4, pp. 1156–1169, April 2014.

[128] T. Stouraitis, "Efficient convertors for residue and quadratic-residue number systems," *IEE Proceedings-G: Circuits, Devices and Systems*, vol. 139, no. 6, pp. 626–634, 1992.

[129] Y. Chen, J.-S. Chou, and H.-M. Sun, "A novel mutual authentication scheme based on quadratic residues for RFID systems," *Computer Networks*, vol. 52, no. 12, pp. 2373–2380, 2008.

[130] D. J. Soudris, V. Paliouras, T. Stouraitis, and C. E. Goutis, "A vlsi design methodology for rns full adder-based inner product architectures," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 44, no. 4, pp. 315–318, Apr 1997.

[131] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.

[132] "LMV793/LMV794 88 MHz, Low Noise, 1.8V CMOS Input, Decompensated Operational Amplifiers," http://www.ti.com/lit/ds/snosax6d/snosax6d.pdf, Accessed: 2017/01/03.

[133] "Noise Analysis of FET Transimpedance Amplifiers," http://www.ti.com/lit/an/sboa060/sboa060.pdf, Accessed: 2017/01/03.

[134] "LMP2231 Single Micropower, 1.6V, Precision Operational Amplifier with CMOS Inputs," http://www.ti.com/lit/ds/symlink/lmp2231.pdf, Accessed: 2017/01/03.

[135] R. Maes and I. Verbauwhede, “Physically unclonable functions: A study on the state of the art and future research directions,” in *Towards Hardware-Intrinsic Security*. Springer, 2010, pp. 3–37.

[136] J. Deepakumara, H. M. Heys, and R. Venkatesan, “Fpga implementation of md5 hash algorithm,” in *Canadian Conference on Electrical and Computer Engineering 2001. Conference Proceedings (Cat. No.01TH8555)*, vol. 2, 2001, pp. 919–924 vol.2.

[137] D. Eastlake 3rd and P. Jones, “Us secure hash algorithm 1 (sha1),” Tech. Rep., 2001.

[138] H. Krawczyk, R. Canetti, and M. Bellare, “Hmac: Keyed-hashing for message authentication,” 1997.

[139] G. de Meulenaer, F. Gosset, O.-X. Standaert, and O. Pereira, “On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks,” in *IEEE International Conference on Wireless and Mobile Computing*, Oct. 2008, pp. 580–585.

[140] A. Kaur, “Energy analysis of wireless sensor networks using rsa and ecc encryption method,” *International Journal of Scientific & Engineering Research*, vol. 4, no. 5, p. 2212, 2013.

[141] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, “Energy analysis of public-key cryptography for wireless sensor networks,” in *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*. IEEE, 2005, pp. 324–328.

[142] A. G. Reddy, A. K. Das, E. J. Yoon, and K. Y. Yoo, “A secure anonymous authentication protocol for mobile services on elliptic curve cryptography,” *IEEE Access*, vol. 4, pp. 4394–4407, 2016.

[143] C. Klein and G. Kaefer, “From smart homes to smart cities: Opportunities and challenges from an industrial perspective,” in *International Conference on Next Generation Wired/Wireless Networking*. Springer, 2008, pp. 260–260.

[144] C.-F. Liao and P.-Y. Chen, “Rosa: Resource-oriented service management schemes for web of things in a smart home,” *Sensors*, vol. 17, no. 10, p. 2159, 2017.

[145] T. D. Mendes, R. Godina, E. M. Rodrigues, J. C. Matias, and J. P. Catalão, “Smart home communication technologies and applications: Wireless protocol assessment for home area network resources,” *Energies*, vol. 8, no. 7, pp. 7279–7311, 2015.

[146] W. Ejaz, M. Naeem, A. Shahid, A. Anpalagan, and M. Jo, “Efficient energy management for the internet of things in smart cities,” *IEEE Communications Magazine*, vol. 55, no. 1, pp. 84–91, January 2017.

[147] Y.-L. Hsu, P.-H. Chou, H.-C. Chang, S.-L. Lin, S.-C. Yang, H.-Y. Su, C.-C. Chang, Y.-S. Cheng, and Y.-C. Kuo, “Design and implementation of a smart home system using multisensor data fusion technology,” *Sensors*, vol. 17, no. 7, p. 1631, 2017.

[148] T. Daily, *survey of commercial and institutional energy use, 2014*. Statistics Canada, 2016. [Online]. Available: http://www.statcan.gc.ca/daily-quotidien/160916/dq160916c-eng.htm

[149] S. DMO, *Smart Home Report*. Statista Digital Market Outlook, 2016. [Online]. Available: https://www.statista.com/study/42112/digital-market-outlook-smart-home-market-study/

[150] S. A. P. Kani and M. H. Nehrir, “Real-time central demand response for primary frequency regulation in microgrids,” *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, pp. 1–1, 2013.

[151] S. Borenstein, M. Jaske, and A. Rosenfeld, “Dynamic pricing, advanced metering, and demand response in electricity markets,” *Center for the Study of Energy Markets*, 2002.

[152] P. Palensky and D. Dietrich, “Demand side management: Demand response, intelligent energy systems, and smart loads,” *IEEE transactions on industrial informatics*, vol. 7, no. 3, pp. 381–388, 2011.

[153] E. M. Rodrigues, R. Godina, M. Shafie-khah, and J. P. Catalão, “Experimental results on a wireless wattmeter device for the integration in home energy management systems,” *Energies*, vol. 10, no. 3, p. 398, 2017.

[154] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, “MQTT-s : A publish/subscribe protocol for wireless sensor networks,” *Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on*, pp. 791–798, 2008.

[155] C. M. Bishop, *Pattern recognition and machine learning*. springer, 2006.

[156] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg *et al.*, “Scikit-learn: Machine learning in python,” *Journal of Machine Learning Research*, vol. 12, no. Oct, pp. 2825–2830, 2011.

[157] R. S. Sutton and A. G. Barto, *Reinforcement learning: An introduction.* MIT press Cambridge, 1998, vol. 1, no. 1.

[158] A. M. Andrew, A. Zakaria, S. Mad Saad, and A. Y. Md Shakaff, “Multi-stage feature selection based intelligent classifier for classification of incipient stage fire in building,” *Sensors*, vol. 16, no. 1, 2016. [Online]. Available: http://www.mdpi.com/1424-8220/16/1/31

[159] M. L. Puterman, *Markov Decision Processes: Discrete Stochastic Dynamic Programming*, 1st ed. John Wiley & Sons, Inc., 2014.

[160] C. J. Watkins and P. Dayan, “Q-learning,” *Machine learning*, vol. 8, no. 3, pp. 279–292, 1992.

[161] D. Ernst, P. Geurts, and L. Wehenkel, “Tree-based batch mode reinforcement learning,” *Journal of Machine Learning Research*, vol. 6, pp. 503–556, 2005.

[162] M. Riedmiller, “Neural fitted q iteration–first experiences with a data efficient neural reinforcement learning method,” *European Conference on Machine Learning*, pp. 317–328, 2005.

[163] O. o. E. E. Natural Resources Canada, *Energy consumption of major household appliances shipped in Canada, summary report.* Energy Publications, 2012. [Online]. Available: http://oee.nrcan.gc.ca/files/pdf/publications/statistics/cama12/cama12.pdf

[164] J. Park and I. W. Sandberg, “Universal approximation using radial-basis-function networks,” *Neural computation*, vol. 3, no. 2, pp. 246–257, 1991.

[165] I. E. S. O. (IESO), *ontario power stats.* canadian energy issues, 2017. [Online]. Available: http://canadianenergyissues.com/ontario-power-stats/

[166] G. Yang, C. K. Ho, and Y. L. Guan, “Dynamic resource allocation for multiple-antenna wireless power transfer,” *IEEE Transactions on Signal Processing*, vol. 62, no. 14, pp. 3565–3577, July 2014.

[167] G. Yang, V. Y. F. Tan, C. K. Ho, S. H. Ting, and Y. L. Guan, “Wireless compressive sensing for energy harvesting sensor nodes over fading channels,” in *2013 IEEE International Conference on Communications (ICC)*, June 2013, pp. 4962–4967.

[168] H. Sharma and P. Balamuralidhar, “A transmission scheme for robust delivery of urgent/critical data in internet of things,” in *2013 Fifth International Conference on Communication Systems and Networks (COMSNETS)*, Jan 2013, pp. 1–7.

[169] L. Shu, Z. Yuan, T. Hara, L. Wang, and Y. Zhang, “Impacts of duty-cycle on tpgf geographical multipath routing in wireless sensor networks,” in *2010 IEEE 18th International Workshop on Quality of Service (IWQoS)*, June 2010, pp. 1–2.

[170] D. Bertsekas, *Nonlinear Programming*. Athena Scientific, 1995. [Online]. Available: http://books.google.ca/books?id=QeweAQAAIAAJ

Appendix A

Proof of the Lemma 2

We define $\bar{E}^1$ and $\bar{E}^2$ in $\Re^{|N|+|L(i)|}$ as $E_{TX}(1+E(T,h_i))+E_{RX}(1+E(T,h_i))$ and $E_{PR}(1+E(T,h_i)P^{'})+R_{ij}E_{SN}$ respectively. If we denote ∞-norm as $\|.\|_\infty$ and q-norm as $\|.\|_q$, the lifetime objective functions of (2.17) are represented by -$\|\bar{E}^1 r+\bar{E}^2 R\|_\infty$ and -$(1/(\varepsilon+1))\|\bar{E}^1 r+\bar{E}^2 R\|_{\varepsilon+1}$ respectively. Suppose $\{r^*,R^*\}$ and $\{r^*_\varepsilon,R^*_\varepsilon\}$ be the optimal solutions for the two objective functions. Then we have the following inequalities using approximation of $\|.\|_\infty$ from [170]

$$\begin{aligned} &\|\bar{E}^1 r^*_\varepsilon+\bar{E}^2 R^*_\varepsilon\|_\infty \\ &\leq \|\bar{E}^1 r^*_\varepsilon+\bar{E}^2 R^*_\varepsilon\|_{\varepsilon+1} \\ &\leq \|\bar{E}^1 r^*+\bar{E}^2 R^*\|_{\varepsilon+1} \\ &\leq |N|^{1/(\varepsilon+1)}\|\bar{E}^1 r^*+\bar{E}^2 R^*\|_\infty \end{aligned} \tag{A.1}$$

The corresponding network lifetimes become T_i=$1/\|\bar{E}^1 r^* + \bar{E}^2 R^*\|_\infty$ and T_i^ε=$1/\|\bar{E}^1 r_\varepsilon^* + \bar{E}^2 R_\varepsilon^*\|_\infty$. From (39) we have,

$$\frac{1}{|N|^{1/(\varepsilon+1)}} T_i \leq T_i^\varepsilon \leq T_i \tag{A.2}$$

At $lim_{\varepsilon \to \infty}\ T_i^\varepsilon = T_i$, and thus the lemma holds.

Appendix B

Proof of the Proposition 2

From (27), the gradient of the objective function $D(\lambda,\mu)$ w.r.t λ_l,

$$\begin{aligned} \nabla_\lambda D(\lambda,\mu) =& \alpha \sum_{i\in N}\sum_{j\in N_i} \nabla_\lambda U_i(R_{ij},P_s) - (1-\alpha)s_i^\varepsilon \cdot \nabla_\lambda s_i \\ &\leq \alpha \sum_{i\in N}\sum_{j\in N_i} \nabla_\lambda U_i(R_{ij},P_s) \leq \alpha\overline{U} \end{aligned} \tag{B.1}$$

By **Definition 1** and **Assumption 1** in Chapter 2, we can find the error in the cost estimation of the link price λ_l when iteration $c \rightarrow c+1$

$$\begin{aligned} \|D(\lambda(c+1)) - D(\lambda(c))\| &\leq \|\nabla_\lambda D(\lambda)^T(\lambda(c+1)-\lambda(c))\| \\ &\leq \|\nabla_\lambda D(\lambda)\| \cdot \|(\lambda(c+1)-\lambda(c))\| \\ &\leq \overline{L}^{1/2}\alpha\overline{U}\|(\lambda(c+1)-\lambda(c))\| \end{aligned} \tag{B.2}$$

From the above inequalities, we see that function is Lipschitz. Thus the solution generated with step size φ_c is optimal [170]. Let the update at each iteration c is given by

$\Delta\lambda(c)$. Then,

$$|\Delta(\lambda(c))| = |\frac{r_{ij}(c)}{\alpha\nabla_{\lambda}U_i(R_{ij},P_s)}\nabla_{\lambda}D(\lambda)| \quad \leq \frac{\overline{R}}{\alpha}|\nabla_{\lambda}D(\lambda)| \tag{B.3}$$

$$\frac{|\nabla_{\lambda}D(\lambda)^T\Delta(\lambda(c))|}{\|\Delta(\lambda(c))\|^2} \leq \frac{\frac{\overline{R}}{\alpha}\|\nabla_{\lambda}D(\lambda)\|^2}{(\frac{\overline{R}}{\alpha})^2\|\nabla_{\lambda}D(\lambda)\|^2} \quad = \frac{\alpha}{\overline{R}} \tag{B.4}$$

According to [170], the step size satisfies $0<\varphi_c<\frac{2}{\overline{L}^{1/2}\overline{U}\,\overline{R}}$. Similarly, the step size bound can be proven for ψ_c.