

ADAPTIVE VLSI DESIGN FOR WIRELESS COMMUNICATION SYSTEMS

THESIS

Submitted by

JOYASHREE BAG

DOCTOR OF PHILOSOPHY(ENGINEERING)

Dept. of Electronics and Telecommunication Engineering,

Faculty Council of Engineering & Technology

Jadavpur University

Kolkata, India

2016

Dedicated to
my father late Ananta Maity
and
my mother Smt. Nirmala Maity

**JADAVPUR UNIVERSITY
KOLKATA-700032
INDIA**

**FACULTY OF ENGINEERING & TECHNOLOGY
DEPARTMENT OF ELECTRONICS AND TELE COMMUNICATION
ENGINEERING**

CERTIFICATE FROM THE SUPERVISOR

This is to certify that the thesis entitled "**Adaptive VLSI Design for Wireless Communication Systems**" submitted by **Mrs. Joyashree Bag**, who got her name registered on 17.01.2013 for the award of Ph. D (Engineering) degree of Jadavpur University is absolutely based upon her own work under the supervision of **Prof.(Dr) Subir Kumar Sarkar** and that neither her thesis nor any part of the thesis has been submitted for any degree / diploma or any other academic award anywhere before.

[Prof. Subir Kumar Sarkar]

Signature of the Supervisor

and date with Official Seal

JADAVPUR UNIVERSITY
KOLKATA-700032
INDIA

1. Title of the thesis

INDEX NO. 114/13/E

"ADAPTIVE VLSI DESIGN FOR WIRELESS COMMUNICATION SYSTEMS"

2. Name, Designation, and Institution of the Supervisor

Prof.(Dr) Subir Kumar Sarkar,

Dept. of Electronics and Telecommunication Engineering,

Jadavpur University,

Jadavpur, Kolkata -700032.

India.

3. List of Publications

JOURNAL PUBLICATION

- [01]. Joyashree Bag, Subhashis Roy, P.K.Dutta and Subir Kumar Sarkar, "FPGA Implementation of DPSK Modem using CORDIC algorithm"—**IETE Journal of Research, Taylor & Francis**; vol.60,no.5, Pages:355-363;2014, ISSN: 0377-2063;
- [02]. Joyashree Bag, Subhashis Roy and Subir Kumar Sarkar, "Advanced Multi-step Security Scheme(AMSS) using PCA for RFID system and its FPGA Implementation" Int. **Journal of RFID technology and Applications, Inderscience, IJRFITA**, Vol. 4, No. 4, 2015, Pages: 325-341.
- [03]. Joyashree Bag, and Subir Kumar Sarkar, "Design and VLSI Implementation of a Data Security scheme for RFID system using Programmable Cellular Automata", Int. **Journal of RFID technology and Applications, Inderscience, IJRFITA**. Vol. 4, No. 2, Pages: 197-211, 2013.

- [04]. Joyashree Bag, Rashmi Ranjan Sahoo, Pranab Kishore Dutta and Subir Kumar Sarkar, "Processor Design and Hardware Implementation of Power efficient Object Localization and Image processing Algorithm for Large Wireless Sensor Network" Int. **Journal of High Performance System Architecture, IJHPSA, Inderscience**, vol.4, No.4, Pages.204-217, April 2013;
- [05]. Joyashree Bag, K M Rajanna, Subir Kumar Sarkar, "FPGA Implementation of EPC Gen-2 protocol and its performance evaluation," **IUP Journal of telecommunications**, vol VI, no.1, Pages :58-71, 2014;
- [06]. Joyashree Bag, K. M. Rajanna, and Subir Kumar Sarkar, "Design and VLSI Implementation of a Zigbee enabled processor for RFID Reader suitable for power efficient home/office Automation" **European Journal of Scientific Research**, Vol.97, No.4, Pages: 592-602, March 2013;
- [07]. Sudip Dogra, Joyashree Bag, Rajanna K.M. and Subir Kumar Sarkar, "Development & VLSI Implementation of a new scheme for Traffic Management using RFID with least stoppage time facility to Priority Cars." Int. **Journal on Recent Trends in Engineering & Technology, 2011, IJRTET, ACEEE** ;Pages 177-181;
- [08]. Joyashree Bag, Manas Chandra Nayak, Souvik Sarkar and Subir Kumar Sarkar, "Hardware Implementation of a Novel water marking system based on Phase Congruency and SVD"—**AEU, International Journal of Electronics and Communications**, under review, 2016

CONFERENCE PUBLICATION

- [01]. Joyashree Bag, Subhashis Roy, and Subir Kumar Sarkar, "Power efficient Query Tree Protocol for RFID technology and its VLSI Implementation"—**PCITC, IEEE** conference, 2015.
- [02]. Subhashis Roy, Joyashree Bag, and Subir Kumar Sarkar, "Design & VLSI Implementation of a Robot navigation processor using CORDIC algorithm deploying RFID technology"—**INDICON, IEEE** conference 2015.
- [03]. Joyashree Bag, and Subir Kumar Sarkar, "A Novel Trusted Key Distribution Server based Data Security Scheme for RFID system and its VLSI Implementation"—**ACCT 2015, IEEE Explore**'2015.
- [04]. Joyashree Bag, Subhashis Roy, and Subir Kumar Sarkar, "FPGA Implementation of Advance Health care system using Zig-bee enabled RFID technology" **IEEE** conference on Advance computer and communication systems, pp.899-904, **IACC**2014.

- [05]. Joyashree Bag, Subhashis Roy, and Subir Kumar Sarkar, "Realization of Low power sensor node and its FPGA Implementation" **IEEE** conference on Advance computer and communication systems, pp.101-104, **IACC2014**.
- [06]. Joyashree Bag, Subhashis Roy, Anita.Panda, Souvik.Sen and Subir Kumar Sarkar, "Design and Hardware Implementation of Passive RFID Based System to enhance Museum visiting experience" International Conference on Advances in Computing, Communications & Informatics Advances, **IEEE ICACCI 2014**, Workshop proceedings.
- [07]. Joyashree Bag, Rajanna K.M. and Subir Kumar Sarkar, "Data Security for EPC Gen-2 and its VLSI Implementation". International Conference on Advanced Computing and Communication Technologies. **ACCT-2013. IEEE** explore, Pages: 330-336.
- [08]. Joyashree Bag, and Subir Kumar Sarkar, "Design and VLSI Implementation of an Automatic home surveillance system using Zigbee technology" International Conference on Computations and Communication Advancements: **IC3A-2013**. Pages: 213-216.
- [09]. Joyashree Bag, K. Senthil Kumar, Souvik Sarkar, Anup Sarkar and Subir Kumar Sarkar, "VLSI Implementation of priority Selection Algorithm to select tags using RFID system". **IET** Conference proceedings of, 2011. Pages:598-600.
- [010]. Joyashree Bag, and Subir Kumar Sarkar, "Anti-collision algorithm for RFID system using adaptive Bayesian Belief Networks and it's VLSI Implementation", **ICECS, IEEE** conference 2016.

4. List of Patents

NIL

5. List of Presentations in National / International Conferences

02

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to my guide Dr. Subir Kumar Sarkar, Professor, Department of Electronics and Telecommunication Engineering, Jadavpur University, Kolkata-700032 for his directive instructions, constructive suggestions, constant supportive encouragement, and affectionate behaviors for the last four years. He always inspired me by dedicating his invaluable time, sharing his upgraded knowledge, recent trends in innovative research areas, and many advices.

I gratefully acknowledge the active support and encouragement obtained from Vice Chancellor, Jadavpur University, Pro-Vice Chancellor, Jadavpur University, Dean, Faculty of Engineering and Technology (FET), Jadavpur University and Head of the Department, Electronics & Tele-Communication Engineering, Jadavpur University.

It's my pleasure to greatly acknowledge to Mr.P.K.Dutta, Mr.Bijoy Kantha, Mr.Sudip Dogra, Mr.K.M.Rajanna, Mr. Subhashis Roy, for their continuous support and encouragement perusing my research work. I will remain ever grateful to them.

I am grateful to Mr. Subhashis Roy, Mr.Rashmi Ranjan Sahoo, for their sincere assistance, co-operation and innovative suggestions during this research work.

Finally, I express my great appreciation to my family members, my husband Mr. Ramkrishna Bag, my son Master Debmalya Bag and my daughter Miss Shreemoyee Bag for their valuable suggestions, encouragement, kind and friendly cooperation to carry forward this research work.

Needless to say, without all the above help and support, the writing and production this thesis would not have been possible.

.....

(Mrs. Joyashree Bag),

Senior Research Scholar,

Dept. of Electronics and Telecommunication Engineering,

Jadavpur University, Jadavpur,

Kolkata, India.

ABSTRACT

Advanced VLSI design using programmable logic devices and FPGAs is suitable to meet the new generation requirements due to their ability to take advantage of new process technologies and geometries. Wireless Communication is one of the most active areas of technology development of recent time, as it is rapidly changing with new features and technology. Wireless Communication today covers a very wide array of applications. Radio Frequency Identification technology and Wireless sensor Network systems are most important field of Wireless Communication system. The candidate has chosen the field of RFID and WSN as the areas of work to venture some Adaptive VLSI design. Hardware implementation up to RTL schematic level has been performed. In order to substantiate the design and real time verification, synthesizable modules are downloaded on the high performance FPGA kit. Designs are performed using high syntax VHDL code language and simulation results are obtained with Xilinx ISE 14.3 simulator. Virtex 5, Spartan 6 and Kintex-7 FPGA boards have been used as a hardware implementation platform. Performance evaluation and comparative study with related work is performed, wherever it is possible. Processor implementation for RFID based power saving appliance, Hardware implementation of anti-collision algorithm for RFID technology, FPGA realization of novel data security scheme for RFID, Power efficient FPGA based wireless sensor node implementation with efficient localization algorithm for large Wireless sensor network system and finally, low power, low cost CORDIC algorithm based DPSK modem realization with FPGA are the contribution of this research work and are described in this thesis.

CHAPTER INDEX

Chapter	Page no.
Chapter 1: Introduction and Organization of Thesis	01
1.1 Introduction.....	01
1.2 Organization of the Thesis.....	05
Chapter 2: Basics of Adaptive VLSI Design, RFID technology and Wireless Sensor Network	09
2.1 Adaptive VLSI Design.....	09
2.1.1 Adaptive Design Process	10
2.1.2 VLSI Design and FPGA.....	11
2.1.3 FPGA Design flow.....	11
2.1.4 VHDL-Very high speed Integrated Circuit Hardware Description Language.....	13
2.2 RFID Technology.....	14
2.2.1 General Operating Principle of RFID.....	14
2.2.2 Advantages of RFID systems	15
2.2.3 Comparison between various Auto-ID Systems.....	15
2.2.4 Components of RFID System	16
2.2.5 History of RFID technology.....	17
2.2.6 Types of RFID Tags and Readers	19
2.3 Zig Bee technology.....	22
2.4 Wireless Sensor Network	22

Chapter 3: VLSI Implementation of a Processor for RFID based Power efficient Home/Office Automation along with Surveillance system	24
3.1 Introduction.....	24
3.2 Literature Review.....	25
3.3 Design and Implementation of Processor for RFID based Power efficient Home/Office Automation	27
3.3.1 Operational flow chart	28
3.3.2 Proposed Algorithm.....	29
3.3.3 Operational Block diagram	30
3.3.4 Principle of Operation.....	31
3.3.5 Hardware Implementation and simulation results	33
3.3.6 FPGA Implementation	39
3.4 Design and Implementation of Processor for RFID based automatic home surveillance system	42
3.4.1 Brief overview of existing surveillance systems.....	42
3.4.2 Proposed System	43
3.4.3 Components of the system.....	44
3.4.4 Hardware Implementation of proposed system.....	46
3.4.5 Operational Block Diagram	47
3.4.6 Simulation Results.....	48
Chapter 4: VLSI Design and Hardware Implementation of RFID Anti-collision Algorithm	49
4.1 Introduction.....	49
4.2 Literature Review.....	50
4.3 Power efficient anti-collision algorithm for RFID technology with added data security feature and its Implementation in VHDL.....	56
4.3.1 Design and implementation of Query tree protocol:	56
4.3.2 Operational flow chart and block diagram for the Query tree protocol	57
4.3.3 Hardware Implementation Results	60

4.4 EPC Gen protocol and its Implementation in VHDL	63
4.4.1 EPC Gen-2 Protocol.....	63
4.4.2 Key points of EPC Gen-2 tags	64
4.4.3 Q-Algorithm:.....	65
4.4.4 Components of EPC Gen module:	66
4.4.5. Design & Implementation of EPC GEN-2 Protocol.....	69
4.4.5.1 Standard Data Frame of EPC tag & proposed data frame	69
4.4.5.2 Operational Block Diagram of EPC tag ID generator and reader processor.....	70
4.4.6 Test bench Simulation results	73
4.4.7 RTL Schematic diagrams for Reader processor and EPC Tag	75
4.4.8 Synthesis report.....	76
4.5 Efficiency Calculation of EPC Gen 2 Protocol	78

Chapter 5: FPGA based Implementation of a data security scheme suitable for RFID system	81
5.1 Introduction.....	81
5.2 Literature Review.....	83
5.3 Different Data Security schemes.....	86
5.3.1 Smart Tag Approach for data security for RFID.....	87
5.3.2 Rewritable Tag Approach for data security.....	88
5.3.3 Physical Blocking Approach for data security	88
5.3.4 Block cipher based cryptography	88
5.3.5 Pseudo-random number generators for RFID data security.....	88
5.3.6 Stream cipher based cryptography	89
5.3.7 Elliptic curve cryptography (ECC)	89
5.4 VLSI Implementation	90
5.4.1 Proposed System	90
5.4.2 Generation of Secret code 'Sc' using cellular automation rules.....	91
5.4.3 Operation of Tag.....	94

5.4.4 Operation of the Reader.....	95
5.5 Simulation Results.....	96

Chapter 6: Low power VLSI Design for large Wireless Sensor Network103

6.1 Introduction.....	103
6.2 Literature Review.....	106
6.3 Realization of a Low power Sensor node processor for Wireless Sensor Network and its VLSI Implementation.....	111
6.3.2 Design Metrics:.....	111
6.3.3 Design and Implementation:.....	111
6.3.3.1 Functional Details of a sensor node.....	111
6.3.3.2 Sensor Node Functional Diagram.....	113
6.3.4 Hardware Implementation.....	114
6.4 Design and VLSI Implementation of Power Efficient Processor for object localization in Large WSN.....	118
6.4.2 Sensor Network as Assumed in this work.....	119
6.4.3 Considerations for the experimental implementation of the proposed algorithm.....	120
6.4.4 Proposed Algorithm:.....	122
6.4.5 Designs and Implementation.....	125
6.4.5.1. 'N' data generator.....	126
6.4.5.2. Data frame 'N' processor.....	127
6.4.5.3. Beacon data frame 'mi' generator.....	128
6.4.5.4. Region code 'Ci' generator.....	128
6.4.6 Efficiency Calculation.....	129
6.4.7 Synthesis Report.....	130

Chapter 7: CORDIC algorithm based VLSI Design134

7.1 Introduction.....	134
7.2 Literature Review.....	135
7.3 Different Modulation and Demodulation techniques.....	137

7.3.1 BPSK Modulation/Demodulation	138
7.3.2 DPSK Modulation/Demodulation.....	139
7.3.3 QPSK Modulation/ Demodulation.....	139
7.4 Cordic Algorithm	140
7.5 Proposed DPSK Modem Module	141
7.5.1 Functional Block diagram	141
7.6 Implementation of proposed DPSK modem module	145
7.7 Simulation results.....	148
Chapter 8: Concluding remarks and Future Scope of Thesis.....	154
8.1 Concluding Remarks.....	154
8.2 Future Scope of the Thesis.....	156
REFERENCES.....	158

LIST OF FIGURES:

Chapter 2:

Fig. 2.1 FPGA Design flow

Fig. 2.2 RFID System

Fig. 2.3 (a) Passive Tag

Fig. 2.3 (b) Semi-passive Tag

Fig. 2.3(c) Active Tags

Fig. 2.3 (d) Sticker type Tags

Fig. 2.3 (e) Key type Tags

Fig. 2.3 (f) Roll of paper type Tags

Fig. 2.3 (g) Tag on human body

Fig. 2.4 (a) Active RFID Reader

Fig. 2.4 (b) Passive Reader

Fig. 2.4(c) Handheld Reader

Chapter 3:

Fig. 3.1 Flow chart of the operation

Fig. 3.2 Block Diagram of the Controller Unit

Fig. 3.3 Room Organization

Fig. 3.4 RTL view showing two parts of the Processor

Fig. 3.5 Simulation result: Final output of the Processor

Fig. 3.6 Zone selection

Fig. 3.7 ID detection as per zone selection

Fig. 3.8 Output of Light control unit

Fig. 3.9 RTL schematic view of the Light control unit

Fig. 3.10 Output of Temperature control unit

Fig. 3.11 RTL schematic view of Temperature control unit

Fig. 3.12 Screen shot of FPGA Implementation

- Fig. 3.13 Technology schematic of Temperature control unit
- Fig. 3.14 Technology schematic view of the final processor (with brake in page)
- Fig. 3.15 Zig-Bee module and board embedded with Zig-Bee module
- Fig. 3.16 Occupancy sensor and wireless camera used for home surveillance
- Fig. 3.17 Pictorial description of home surveillance system
- Fig 3.18 Operational flow chart of the proposed system
- Fig. 3.19 Block diagram of proposed system
- Fig. 3.20 Test bench simulation for ID detection module in the controller section.

Chapter 4:

- Fig. 4.1 State transition diagram for Query tree protocol
- Fig. 4.2 Query Search Tree
- Fig. 4.3 Operational Flow chart diagram for Tag
- Fig. 4.4 Operational Flow chart diagram for Reader
- Fig. 4.5 Functional Block Diagrams of tag and reader
- Fig. 4.6 RTL Diagram (reader) for proposed algorithm
- Fig. 4.7 Q-Algorithm
- Fig. 4.8 A Data structure of 96 bit EPC Class1 Gen2 tag
- Fig. 4.9 Standard data frame of tag
- Fig. 4.10 Proposed data frame of tag
- Fig. 4.11 Block diagram of reader processor
- Fig. 4.12 Flow chart of Reader Operation
- Fig. 4.13 Block diagram of tag
- Fig.4.14 Flow chart of Tag operation

Chapter 5:

- Fig. 5.1 Pictorial description of RFID Data Security System
- Fig. 5.2 State transition diagram for PCA
- Fig. 5.3 Structure of Secret code generator using Programmable Cellular Automata (PCA)
- Fig. 5.4 Flow chart for tag operation

Fig. 5.5 Flow chart of Reader operation

Fig 5.6 Test bench simulation wave form for Sc_Generator

Fig. 5.7 Test bench simulation result for Tag ID generator

Fig. 5.8 Test bench simulation result for the reader processor.

Fig 5.9 RTL schematic view of Sc_Generator (secret code generator)

Fig. 5.10 Report of Synthesized and placed & routed module of RFID data security Reader processor

Fig. 5.11 RTL schematic for Tag ID generator including Sc_Generator

Fig. 5.12 RTL schematic of Reader processor including Sc_generator module.

Chapter 6:

Fig. 6.1 A Typical Wireless Sensor Network Topology

Fig. 6.2 Flow chart for the basic node functions

Fig.6.3 Data format transmitted by beacon (24 bit)

Fig.6.4 A Typical sensor network routing

Fig.6.5 Architectural diagram of a typical sensor node

Fig.6.6 Operational Block diagram of a typical sensor network (Beacon & Node)

Fig.6.7 RTL schematic view of a typical beacon processor of a sensor network

Fig.6.8 RTL schematic view of a typical sensor node processor of a sensor network

Fig.6.9 Test bench simulation of the beacon processor

Fig.6.10 Test bench simulation of the sensor node processor

Fig.6.11 Network Topology assumed in this work

Fig.6.12. Network with image/obstacle; Different region codes, virtual corners and the estimated position of object

Fig.6.13 Flow chart showing algorithm

Fig.6.14 Operational block diagram

Fig.6.15 Detected obstacle area by B1, B2, B3 and B4

Fig.6.16 Detected obstacle area by B5, B6, B7 and B8

Fig. 6.18 Data frame 'N'

Fig. 6.19 Output of N_processor

Fig. 6.20 Output of 'mi' generator

Fig. 6.21 Structure of 12 bit 'mi' data frame

Fig. 6.22 Output of code 'c' generator

Fig. 6.23 RTL schematic of Node_gen

Fig. 6.24 RTL schematic view of code generator

Fig. 6.25 RTL schematic view of the processor including code generator, 'N' data generator with control clock

Fig. 6.26 RTL schematic view of the v_corner block

Chapter 7:

Fig.7.1 Functional Block diagram of DPSK Modem

Fig.7.2. CORDIC module block diagram

Fig.7.3 DPSK Modulator Block diagram

Fig. 7.4 DPSK Demodulator Block diagram

Fig. 7.5 Implemented CORDIC Block RTL schematic to serve as waveform generator or carrier generator

Fig.7.6 RTL schematic view of the Implemented DPSK modulator using Xilinx ISE 14.3 tools

Fig.7.7 Expanded view of the DPSK modulator using Plan Ahead 14.3

Fig. 7.8 RTL schematic view of the DPSK modem

Fig.7.9 Expanded view of the DPSK modem using Plan Ahead 14.3

Fig. 7.10 Sinewave & Co-Sinewave generation

Fig. 7.11 DPSK Modulator output result

Fig.7.12 DPSK demodulator output result

Fig. 7.13 The DPSK modulator design using Simulink, Matlab10 (Xilinx block on SDR)

Fig. 7.14 DPSK Modulator output result in Simulink model

Fig.7.15 Bar-chart showing different parameters of different blocks

LIST OF TABLES:

- Table 2.1: Comparison between various Auto-ID Systems
- Table 2.2: History of RFID technology
- Table 2.3: Frequency band of RFID applications
- Table 3.1: Hardware requirements for Final processor and other controlling units
- Table 4.1: Performance of the Crypto processor based on different crypto algorithms
- Table 4.2. The Operating Process of QTA
- Table 4.3: Comparative study with different anti-collision algorithms [ID of 8 bit]
- Table 4.4: Synthesis Report
- Table 5.1: Comparison table with other works
- Table 5.2: Comparative study of different crypto-algorithms
- Table 5.3. Rules that update the next state of the cells
- Table 5.4: List of hardware requirements
- Table 6.1: An overview of related work
- Table 6.2: HDL synthesis/Device utilization summary [Node_Processor]
- Table 6.3: Obstacle area detection efficiency calculation
- Table 6.4: List of hardware requirements, Device Utilization and Delay Report
- Table 7.1: Advanced HDL Synthesis Report
- Table 7.2: A comparative study of Device utilization summary of DPSK modem

APPENDIX

ASK	Amplitude shift keying
ABS	Adaptive Binary Splitting Tree Search
AES	Advanced Encryption Standards algorithm
ADC	Analog-to-digital conversion
ASICs	Application specific integrated circuits
B-array tree	Binary Array Tree
BPSK	Binary Phase Shift Keying
CMOS	Complementary MOS technology.
CORDIC	COordinate Rotation DIgital Computer algorithm
CCTV	Closed Circuit TV
CDMA	Code Division Multiple Access
CODEC	Coder/Decoder
DAC	Digital-to-Analog conversion.
DFSA	Dynamic Frame Slotted ALOHA
DPSK	Differential Phase Shift Keying
DOL	Distributed Object Localization algorithm
DNS	Domain Name System
EPC Gen2	Electronic Product Code Generation 2
ECC	Elliptic curve cryptography algorithm
FSA	Frame Slotted ALOHA
FSK	Frequency shift keying
FSA	Finite state automaton
GPS	Global positioning system
IQTA	Improved Query tree
LUT	Look -up-table,
NRE	Non Recurring Cost
ONS	Object Naming Service
PCA	Programmable Cellular Automata

PLD	Programmable Logic Device
PGA	Programmable Gain Amplifier
PSK	Phase shift keying
QPSK	Quadrature Phase Shift Keying
QTA	Query Tree Algorithm
RFID	Radio Frequency Identification
RTL	Register-Transfer Level
RN16QTA	RN16-based QTA
ROM	Random Access Memory
RN	Random number
SoCs	Systems on chips
SN	Slot Number
SDR	Software Defined Radio
Tag ID	Tag Identity
TID	Tags temporary ID
TEA	Tiny Encryption Algorithm
UHF	Ultra High Frequency
VLSI	Very Large Scale Integration
VHDL	Very high speed Integrated Circuit Hardware Description Language
WSN	Wireless Sensor Network technology

CHAPTER 1

INTRODUCTION AND ORGANIZATION OF THE THESIS

Chapter1: Introduction and Organization of Thesis

1.1 Introduction:

In the modern age of advanced electronics, technology up gradation has introduced revolutionary changes in the field of wireless communication systems, like RFID technology, Wireless Sensor Network technology, Mobile communication, etc. Integrated VLSI design of various components and circuits are the key factors of this revolution. Low cost design with high performance, high data handling capacity with minimum chip fabrication area, and high frequency application with minimum noise and error probability is the major contribution of today's VLSI design technology. Advanced VLSI design using programmable logic devices and FPGAs is suitable to meet these new generation requirements due to their ability to take advantage of new process technologies and geometries [1- 5].

In this respect, Adaptive VLSI design is a viable solution to fabricate any system very cost effectively and without degradation of system performance. Reconfigurable computing allows incremental design flow, thus can serve as an affordable, fast, and accurate tool to verify electronic designs. Design can be sent to market with minimum requirements and additional features can be added without any change in physical device or system. FPGAs are feasible alternatives to custom microprocessors as they can offer a shorter time cycle to the market, zero NRE cost, and re-usable IP options. Moreover, it can be used across many platforms and PCBs to reduce inventory costs and when using them in combination with a soft core embedded processor, it can solve the device obsolescence problem [1- 3].

As the digital circuit design technology is changing rapidly, mostly in the field of wireless communication based systems, design portability is an important advantage of adaptive VLSI design. By using a standard hardware description language, the designer can focus only on the required functionality of the desired circuit. As VHDL is a technology independent design language, the design may be implemented in different types of chips. It may be implemented with CAD tools of different manufacturing companies, without having to change the VHDL specification.

These features, along with the advantage of easy reuse and remodeling of circuits, and emerging trends of RFID applications in almost every sphere, encourage us to design wireless communication system models with standard VHDL code. This allows faster development of new product where existing VHDL code can be adapted to add new features and functionality to the developed model. There are considerable research works in the recent years in developing new wireless technology of greater intelligence. Development of novel digital signal processing, modulation and transmission technique is the key aspects of the research efforts. High performance FPGA based hardware has gained extensive use and popularity in applications like: wireless sensor network system, RFID technology.

The pivotal function of wireless sensor network system is to confirm the position of the event, where it occurs, and the position of the obstacle which causes disturbance on proper delivery of data packets [6- 8]. In large forest area or in the area with small rocks where manual tracing is not possible, the properly designed wireless sensor network system is useful to detect the object which causes disturbance in the network system [9- 11]. The deployment of large scale sensor networks is limited because of lack of effective protocol support, network spectrum capacity limit, energy consumption, node size and cost. An integrated hardware and protocol suite capable of supporting 1000+ nodes flexible to adjust different requirements and suitable for inexpensive, very large scale integrated (VLSI) circuit implementation is required to realize these sensor network goals [12- 20].

The sensor node of a wireless sensor network must have the capability of sensing, processing, and communication elements [21- 24]. They must be cheap, power efficient and long lasting. WSN is a new direction for researchers to provide more energy efficient, reliable and low cost system. Prolonging network lifetime for these sensor nodes is a critical issue. Modern electronics systems are moving towards the self-adjusting and adaptive circuit architecture that can quickly and efficiently respond to real time changes. The reconfigurable hardware fabric can be easily modified or upgraded to enhance its performance without much effort, time or cost.

In the fast developing wireless communication based systems, demand for low power, low cost with small chip area is well concerned. Smaller chip area with minimized power consumption is a challenge to the chip designer. The demand for new wireless technology with higher capacity is now growing at a rapid pace. As we know, bandwidth and transmitter

power, both of these two resources are limited in the deployment of modern wireless networks. So, the new process technology has been adapted to provide a more efficient wireless system with increased capacity [25- 26].

The sophisticated FPGA based processor is also gaining popularity in the field of RFID technology and its applications. Here, we will focus on the various applications and utilities of this technology. RFID technology finds its applications in various fields like, logistics, healthcare, security and identification systems, toll system, ticket, etc. One of the most famous RFID applications is supply chain management. RFID tags are attached to goods, items or parts in the supply chain and all items are tracked by RFID readers from manufacture point to point of sales. Megatrux, a top 100 logistics company in the world, has applied Motorola RFID plan to its supply chain management [27]. Using RFID we can track the total system from handling to product delivery. The present location and movement direction also can be traced with RFID tag attached with the product. The express DHL tracking tools have developed a global infrastructure to track all packages throughout the world and updated information can be obtained by any mobile phone or PC connected to DHL by 2015 [28- 29]. We also found that the Federal Express applied RFID technology to track the location, temperature, humidity levels, and delivery status of target item [30].

RFID technology is now effectively used to facilitate an electronic toll collection system, especially in highways. The Modern car parking system is also monitored by RFID technology in various countries. RFID technology enables vehicles to check-in and checkout automatically, while passing through a toll plaza under a fast and secure environment. Tracking of a car is also possible using this technology [31]. This RFID based automatic toll systems solve the traffic jam problem caused by human operated toll system and save time also for car owners.

Tremendous advancement in RFID technology has developed more flexible and smaller tags and antennas. This up gradation has flourished the wide use and application of low cost RFID in different fields, like e-tickets for exhibitions, stadiums, theme parks and other important entries. In World cup 2006, Beijing 2008 Olympic Games, the application of RFID tags in tickets abolish the chance of fake tickets and provide satisfactory performance in flow control of people and other formalities like registration of players, security identification, even payment process [38].

We have found the application of RFID largely in Healthcare for handling and distribution of drugs, track patients and medical equipments, collect medical information, monitor the stock, etc [34- 37]. From automatic screening, admitting, till full treating process, the patient is monitored and it helps the doctor and other staffs to identify the correct patient in need [37]. Stealing or exchange of a newborn baby can be controlled using RFID tag attached to the baby and mother, ensuring identification and alert system will alert the staff immediately if someone attempts to take away the baby. A report from IDTechEx estimated that the total RFID market value in 2015 is worth \$8.89 billion. IDTechEx forecast a high of \$27.31 billion by 2024[39- 45].

Collection of patient health information wirelessly has made a drastic change over traditional health care system. A context aware RFID system was developed by the researchers at the University of Aarhus in Denmark who work in close collaboration between patients and clinicians. This system used RFID tags on patients and clinicians and other applications of the system were adapted to the context in which they are running. This study aims the introduction of RFID technology in development of Hospital infrastructure and applications [40].

Currently printing tags with organic materials seems to be a promising approach. Using printing tags, the cost-intensive assembly of the two main components, antenna and chip, can be eliminated. RFID technology is already being used in several US states, Australia, Belgium, and Canada. Cases like baby abduction, inadvertent mix-up, wrong surgery, misplacement of medical reports, delay regarding different report, manual records, etc. have placed health care system as a challenging issue [41- 43]. In US states, Australia, Belgium, Canada Health care system has successfully used RFID to reduce these problems to a minimum. US health care units and hospitals, RFID enabled bracelet, 'hugs and kisses' RFID system, an implantable RFID device with sensors are successfully adopted [44- 45].

New RFID based implants can also serve as biosensors and act as micro-electromechanical system for monitoring the health condition, like blood pressure, oxygen level, electrocardiogram images. The system is currently deployed in a Belgian university hospital [43]. An Australian health care for elderly people uses Wi-Fi based RFID system to enable them to quickly access them, easily call for help in an emergency [44].

In view of the above declaration, it is obvious that there are still some scopes of research work in the field of wireless sensor network and RFID technology. Till now, many applications are based on ASIC or PIC microcontroller. But other than reconfigurable architecture, ability of pipelining and parallel processing is another important feature that makes FPGA superior in many areas. FPGA can process larger data with few clock cycles, i.e, in high speed due to this feature. So, FPGA solution is suitable for high speed, high performance, and larger data processing applications. For other processor, data flow is limited by processor bus and processing speed. Gradual up gradation and ever-changing wireless communication systems has requirement of such FPGA based solutions [50- 54].

Being motivated with these scope of work, some Adaptive VLSI design of wireless communication systems has been developed in this research work. As the wireless communication is a vast area, the RFID Technology and wireless sensor network are chosen.

1.2 Organization of the Thesis

The low cost and high speed adaptive processor development for wireless communication based systems are presented and described in details in this thesis work. Hardware Implementation up-to Register Transfer Level is performed. Synthesizable modules are successfully downloaded on high performance FPGA kit in order to substantiate our design and real time verification. Performance evaluation and comparative study are included for developed system models with respect to most recent research works.

The thesis is organized by incorporating different chapters and chapters are organized as:

❖ In Chapter 2, the concept of Adaptive VLSI design, its design procedure and advantages are described in brief. The basics of RFID technology, its operating principles, different components, characteristics, and applications are explained along with its advantages over other auto-ID systems. We have also included an overview of the Wireless sensor network technology in this chapter.

❖ In Chapter 3, hardware realization and VLSI implementation of power efficient processor for RFID based home/office automation along with home surveillance systems are described. In this work, a small, smart light and temperature controlling unit has been designed and simulated .The operating principle is based on position estimation of the tag in a

room and for this position estimation a multi sensing mechanism has been used. A multi sensing reader can transmit signal at different power levels periodically with a regular interval. In determining the position of the tag the lights of that particular area are turned on while those of the other regions are either switched off or power is given to secondary low power consuming lights. The temperature control unit controls the temperature of the room within a specified range, not only that, the 'alarm' generator signal becomes high to 'on' a buzzer for 'fire-alarm', whenever the temperature of the room exceeds a specified high temperature. So, we achieve our desirable power saving model, which works on RFID technology. The high syntax VHDL code is used to design the processor and realized with FPGA(Virtex5). This reconfigurable processor has the design flexibility to incorporate more features to the existing processor.

❖ In Chapter 4, hardware Implementation of RFID anti-collision algorithm is presented. The Query tree protocol is implemented with some added features of priority and data security in this work. In our research work, we have implemented the protocol as low power single chip solution. We have included a PCA based data security scheme in this protocol for secured data transmission. We have also implemented other anti-collision protocols with different bit size and a comparative study of device utilization and performance has been provided. The hardware for EPC Gen2 protocol is also developed and described in this chapter. The hardware realization of the EPC Gen2 protocol on FPGA board is performed successfully in this work. The developed model has been simulated for different Q values to achieve the maximum success for tag identification using Matlab 6.

❖ Chapter 5 describes the VLSI Implementation of programmable cellular automata based data security scheme for RFID tags. As the RFID tag store information, hackers can easily hack the data permitting the unauthorized scanning of tags. But in an RFID system, tags have only a few hundred of logic gates whereas most of the encryption scheme requires several hundred / thousands of gates. The proposed data authentication system in this work, uses the programmable cellular automata rules [90 & 150 rules] for data authentication. It is implemented with a key generator, rule selector, few simple logic gates(XOR,OR) and multiplexer, which minimizes the computational overhead, hardware utilization, and made it suitable for the RFID tags. In this scheme, only the authentic reader will be provided by the PCA rules and the secret key to decrypt the data received from the tag. The design is

simulated on Xilinx 14.3 simulator and verified with high performance FPGA(Kintex7) board.

❖ In Chapter 6, Low power VLSI Design for Wireless Sensor Networks is described. In a large sensor network, localization of an object and detecting its boundary is very important for successful and fast data transmission from one node to another. Adopting a novel distributed object localization algorithm, a beacon and node processor has been developed on FPGA. Low cost, prolonged life and power efficient sensor node are very much important to the network designer. Considering these design metrics a FPGA based low power sensor node processor has been developed having a low range power dissipation rate. The VLSI implementation of the proposed processor and its hardware realization has been achieved through Xilinx ISE 14.3 simulation tool and downloaded into the Virtex-V FPGA kit. The Processing speed is very high (2.357ns) as circuit complexity is negligible due to simple hardware requirements. Power consumption is of the order of 0.012mW with a quiescent current of near about 1.27mA only. The proposed design gives better performance in comparison with the result of recent work of low power sensor node designers. The same is subsequently verified using MATLAB environment. This algorithm has been simulated and verified for three different figures to evaluate the obstacle area detection efficiency in this research work.

❖ In Chapter 7, CORDIC algorithm based VLSI design is described for Wireless communication systems which minimizes the circuit complexity and power consumption. Differential Phase Shift Keying or DPSK modulation has the magnificent features of limited bandwidth, resistivity against interference, multipath fading and almost constant envelope which are very important for mobile communication systems for providing the output in accordance to the customers/designers' requirements. This work presents the FPGA implementation of DPSK modulator/demodulator incorporating the CORDIC sine-cosine block as a carrier wave generator. A CORDIC algorithm based simple DPSK modem for wireless communication system is proposed and hardware realization is performed as FPGA (Kintex7)based single chip processor. The quality of the modem performance is compared with a non-CORDIC modem which is developed using the standard SDR(Software Defined Radio) platform using available simulink modules. It is observed that the hardware requirement is minimized up to one third and speed increases by almost nine times with a very low power dissipation rate.

❖ In Chapter 8, the candidate has concluded the research work done in this thesis. The low cost and high speed adaptive processor for wireless communication systems are developed in this research work. Hardware Implementation up-to Register Transfer Level is performed. Synthesizable modules are successfully downloaded on high performance FPGA kit in order to substantiate our design and real time verification. Performance evaluation and comparative study are included for the developed system models with respect to most recent research works.

CHAPTER 2

**BASICS OF ADAPTIVE VLSI DESIGN, RFID TECHNOLOGY,
AND WIRELESS SENSOR NETWORK**

Chapter2: Basics of Adaptive VLSI Design, RFID technology and Wireless Sensor Network

2.1 Adaptive VLSI Design:

Adaptive VLSI design introduces flexibility to the design of electronic devices, which is changing rapidly including new features and functionality. To cope up with the growing electronic industry, the designers need to understand the requirement of the system, depending on the application area and the customer satisfaction. The word ‘Adaptive’ means ‘made to fit’, so the design is made in such a way that it can be fitted or integrated in any system which efficiently executes its functionality and also can be modified at any time [4].

Design of low cost, high speed and power efficient processor with adaptive mode is now an excellent field of research. In a wireless communication system, portable devices with such adaptive processors have created a growing and demanding market. Modern Electronic Industry is looking for such processors rather than custom microprocessors and microcontroller based systems. Designs in hardware description language codes like Verilog and VHDL are popular due to their simplicity, ease of circuit development and technology independence.

Design with VHDL code is accepted and supported by most companies that offer digital hardware technology due to its adaptive feature. VHDL source code has the flexibility to include the explanation of how the circuit works within the code. So, the designer/fellow designer easily can modify the design to adapt with the new requirement without much concerned about the technology in which it will be implemented finally using FPGA. Hardware architecture of FPGA is user defined and controlled, thus adaptive by nature, means the designer has the flexibility and opportunity to add different functions, improve performance only by modification of code. Also, pipelining and parallel processing may be adopted to enhance the throughput in FPGA.

2.1.1 Adaptive Design Process:

Adaptive design is a set of designs that focus on the requirement of user/application and the whole design process involves the imagination of a designer, and implementation of a novel system. It generally precedes much like building a structure.

- The Designer selects features and components to be used. If a chip is a rework of an existing design which needs design shrink or few added features, etc, then the architecture design is simple modification.
- Study of user's specification and requirement according to application is very important in this system design.
- Then the designer defines subsystems of the model. According to working algorithm and operational flow chart of the target model these subsystems are defined.
- Design of each subsystem is simulated to get desired output within permitted parameters and specification and synthesized.
- After that, the designer incorporates subsystems into a final system to shape the actual structure of model.
- Designer verifies the functionality and performance of the structure. The final structural VHDL model is synthesized to get the device utilization chart, RTL schematic diagram, power analysis and delay report.
- Designer optimizes the design if it is required. As the VHDL coded design is self-optimized, the need is minimized too some extent.
- Finally, the design is tested for justification for adaption.

The demand for portable devices and processors on a single chip at low cost, low power, high speed and adaptive nature in wireless communication systems is now growing in market. Processor design and hardware level implementation up to RTL schematic level with enormous functionality was a challenging job to support these full-service systems. This was performed after total investigation of the system to be developed and its requirements, shortcomings, problems and application area. After collecting all the required information, we planned and designed our algorithm to satisfy the criteria.

2.1.2 VLSI Design and FPGA:

Programmable Logic Devices provide a revolutionary alternative to custom logic chips due to its flexible nature, ability to reconfigure or modify functionality, without time delay or cost overheads Life cycle costs have a significant impact on the design process of an electronic system. Now, obsolescence of microprocessor is a major problem for electronic industry, which can be solved using programmable processor [5]. Programmable processor can be integrated and deployed such application wherever it is needed. Custom processor has to scrap away if the project is failed or cancelled, whereas programmable processor can redeploy. FPGA based design is a valuable solution to the custom processor based design as it can be reprogrammed and upgrade products in the field.

This up-gradation can be performed remotely without changing basic hardware. High Syntax Verilog and VHDL are the standard languages used in an expansive scale for the design of hardware systems in the recent times. The design provides optimum performance with adaptive feature. In wireless communication based system design process, where portable device and processor has demanding market this design is suitable due to its design integration feature. Design integration feature provides the facility to put the effective system on a single chip.

Secure data transaction is another important and demanding task of Networking, wireless communication systems. Several algorithms are developed to encrypt/decrypt data to provide security. We have developed novel data security algorithm for RFID system and hardware realization has been performed using VHDL and FPGA-the programmable processors.

2.1.3 FPGA Design flow:

A design methodology is frequently called a design flow. The flow of data in the methodology shows some basic steps.

- **Specification:** The customer specifies the basic functions of the chip, the processing speed requirement, etc., it is a set of requirements, not a design.
- **Behavior:** The behavioral description is much more precise, it is the model of the device written in some executable program.

- **Design Entry:** HDLs are well suited for highly complex designs, especially when the designer has a good handle on how the logic must be structured
- **RTL Simulation:** After design entry, the design is simulated at the register-transfer level (RTL). RTL simulation offers the highest performance in terms of speed. The next step following RTL simulation is to convert the RTL representation of the design into a bit-stream file that can be loaded onto the FPGA.
- **FPGA synthesis:** Synthesis translates the VHDL or Verilog code into a device netlist format that can be understood by a bit-stream converter.

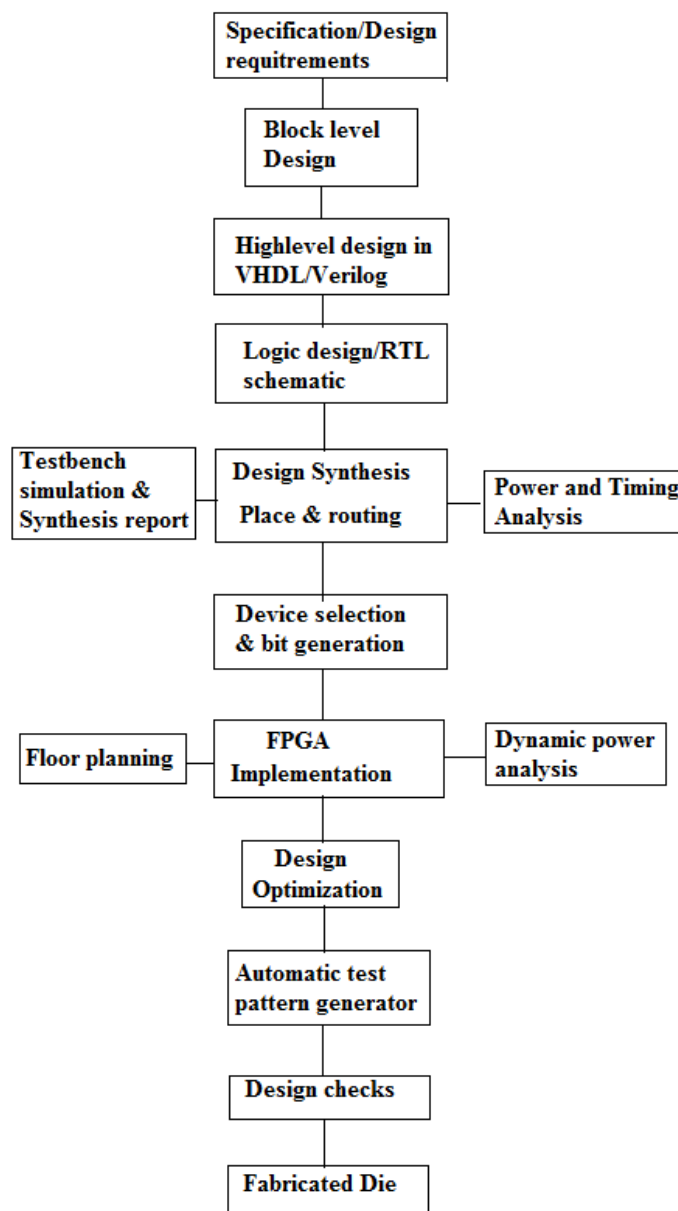


Fig. 2.1 FPGA Design flow

FPGA Design flow is shown in fig 2.1.

Synthesis Process:

The synthesis process requires the following three steps.

Step1: The HDL code is converted into device netlist format.

Step2: The resulting file is converted into a hexadecimal bit-stream file, or .bit file. This conversion of the list of required devices and interconnects into hexadecimal bits is necessary to download onto the FPGA.

Step3: The .bit file is downloaded to the physical FPGA. This step completes the FPGA synthesis procedure by programming the design onto the physical FPGA.

Gate Level Simulation Process:

After synthesis, the functional simulation is performed before physical implementation. This ensures correct logic functionality with full timing information.

Static timing analysis calculates the timing of combinational paths between registers and compares it against the designer's timing constraints

2.1.4 VHDL-Very high speed Integrated Circuit Hardware Description Language:

VHDL is one of the dominant hardware description languages that are used for hardware design and synthesis. It's flexibility lies in the fact that it is a very broad language containing constructs that can be used to describe sequential behavior, concurrent behavior and structure, including data abstraction, all using modeling language.

VHDL is a strongly and richly typed language. Derived from the Ada programming language, its language requirements make it more verbose than Verilog. The additional verbosity is intended to make designs self-documenting. Also, the strong typing requires additional coding to explicitly convert from one data type to another (integer to bit-vector, for example). Several related standards have been developed to increase the utility of the language. Any VHDL design today depends on at least IEEE-Std 1164 (std_logic type), and many also depend on standard Numeric and Math packages as well. The development of related standards is due to another goal of VHDL's authors: namely, to produce a general language and allow development of reusable packages to cover functionality not built into the language. VHDL does not define any simulation control or monitoring capabilities within the language. These capabilities are tool dependent. Due to this lack of language-defined simulation control commands and also because of VHDL's user defined type capabilities, the

VHDL community usually relies on interactive GUI environments for debugging design problems. We have developed such kind of embedded systems basing on VHDL.

2.2 RFID Technology:

In the recent years the process of automatic identification (Auto-ID) has become very popular in many industries related to service, purchase and distribution logistics.. Automatic identification procedures are responsible to provide information about goods and products in transit, even people and animals too. The trend in the automated industry is to move towards fast and real-time identification and high level of accuracy. Such a level of real-time knowledge is often called ambient intelligence. There are various methods of automatic identification techniques. But among these methods Radio Frequency Identification (RFID) is the most reliable way to electronically identify, data capture, control, track, and inventory items using RF communication [25- 26]. Today RFID has a very broad use, but most of the time such systems are invisible or are not recognized by the users. Realization in the business community of the benefits of widespread adoption coupled with advances in manufacturing techniques and efficient data-handling methodologies is fostering the explosive growth of radio frequency identification systems. RFID-enabled applications have grown at a tremendous rate with system deployments in a number of industries. An important aspect of RFID technology is its utilization in a wide spectrum of applications [27- 41].

2.2.1 General Operating Principle of RFID:

There are four basic operating procedure of interaction between RFID transponder and reader, in particular the power supply to the transponder and the data transfer between transponder and reader:

- i. *EAS radio frequency procedure:*
- ii. *EAS Frequency Divider procedure:*
- iii. *Inductive coupling procedure:*
- iv. *Electromagnetic backscatter coupling:*

Electromagnetic backscatter coupling: RFID systems in which the gap between reader and the transponder is greater than 1m are called *long-range systems*. These systems

are operated at the *UHF frequencies* of 868MHz (Europe) and 915MHz (USA), and at the *microwave frequencies* 2.5 GHz and 5.8 GHz [25,55,56].

2.2.2 Advantages of RFID systems:

There are several advantages of RFID systems compared to the other Auto-ID systems which actually motivate people/manufacturer/electronic industries to adopt RFID for automatic identification of objects [55,56].

The main advantages of the RFID over other technologies are as follows:

- Battery less (for passive tags only). Supply voltage is derived from the RF field
- No line-of-sight is required for the communication to take place.
- Read and write capability of the tag memory.
- High communication speed & High data capacity.
- Data encryption/authentication capability.
- Multiple tag read capability with anti-collision (50–100tags).
- Reusability of the Tag.
- Hands free operation.
- Miniaturized (IC size 1mm^2).
- Very low power requirement.

2.2.3 Comparison between various Auto-ID Systems:

Due to the above reasons the scope of the RFID technology is increasing day by day, especially in the object tracking application. A comparison between various Auto-ID processes is given in Table 2.1. Also, there are some application processes like item tracking, require extended capabilities of the ID system which cannot be achieved by the Auto-ID system like a barcode. In these applications, RFID systems can surpass the limitations of the others identification systems.

Table 2.1 Comparison between various Auto-ID Systems

System parameters	OCR	Barcode	Biometry	Smart Card	Voice recognition	RFID systems
<i>Influence of dirt/weather</i>	Very high	Very high	-	May degrade performance	-	No influence
<i>Influence of covering</i>	Failure	Failure	degrade performance	-	-	No influence
<i>Influence of direction</i>			-	Uni-directional	-	No influence
<i>Data density</i>	Low	Low	High	Very high	High	Very high
<i>Authorization security</i>	Very low	Very low	High	High	Low	High
<i>Speed of handling data</i>	Low ~3s	Low ~4s	Very low >5s	Low ~4s	Very low >5s~10s	Very fast 0.05s
<i>Max. distance between reader & tag</i>	<1cm	0-50cm	Direct contact	Direct contact	0-50cm	0-5m Microwave

2.2.4 Components of RFID System:

RFID is a generic term for technologies which use radio waves to identify living and non-living objects automatically. There are several methods of identification, the most common of which is to associate the RFID tag unique identifier with an object or person [55-56]. An RFID system will typically comprise the following components: (Fig.2.2).

- a) An RFID tag (sometimes called a transponder), composed of a semiconductor chip, an Antenna, and sometimes a battery.
- b) An interrogator or reader, which is associated with an antenna and an RF module, and a control module.
- c) A host system or controller, which most often takes the form of a PC or a workstation connection to an enterprise system.



Fig. 2.2 RFID system

RFID is seen as the inevitable replacement for bar codes for article security to more sophisticated use. RFID is the technology of automatic identification that is gaining momentum and is considered to emerge as one of the most pervasive computing technologies in modern electronic history. RFID represents more significant and improved technology over bar codes in terms of non-optical proximity communication, information density, and two-way communication ability. RFID systems involve tags and readers interacting with each other and database systems to provide information.

2.2.5 History of RFID technology:

Table 2.2 provides the history of the RFID technology including step by step development during different time period.

Table 2.2: History of RFID technology [25- 26]

Sl. no.	Period	Development of RFID technology
1.	1940–1950	RFID was invented by Harry Stockman in 1948.
2.	1950–1960	Early explorations of RFID technology take place, laboratory Experiments were performed.
3.	1960–1970	Development of the theory of RFID technology and start trials for application field.
4.	1970–1980	Explosion of RFID development and trials of RFID accelerated. Implementations of RFID technology started.
5.	1980–1990	Commercial applications of RFID started.
6.	1990–2000	Emergence of standard RFID applications and widely deployed. RFID becomes a part of everyday life. Developments continued in the 1990s with integrated circuit development and size reduction and microwave RFID tags were reduced to a single IC chip.
7.	2000- till now	RFID flourished along with ZigBee network and settled its position in various important and secured zones. Researchers' interest accelerated and RFID is entering new areas of technical revolution every day.

In 1950s, there was a number of pioneering research and scientific papers being published on RFID techniques. RFID prototype systems are developed by various inventors and researchers during the 1960s. Commercial applications of RFID started, the system with the electronic article surveillance (EAS) equipment launched which can be used as an anti-theft device. In 1970s, researchers and developers from academic institutions like Los Alamos Scientific Laboratory and the Swedish Microwave Institute Foundation had a great deal of interest in RFID. There was a rapid development of work using RFID technology in this period and applications such as animal tagging became commercially available. By 1980s, in Europe animal tracking systems became widespread and toll roads in Italy, France, Spain, Portugal and Norway were based on RFID technology. It was significant with the widespread adoption of electronic toll collection in the United States by 1990s. An electronic tolling system opened in 1991 in Oklahoma, where vehicles could pass toll collection points at highway speeds without waiting. Not only in Europe, but there was also considerable

interest in RFID applications including toll collections, rail applications and access control in many countries, including Brazil, New Zealand, Argentina, Hong Kong, South Africa, Australia, Japan, China, Mexico, Malaysia, South Korea, Canada, Thailand, Singapore. In the 1990s, developments continued with integrated circuit development and size reduction and finally the microwave RFID tags were reduced to a single integrated circuit [25- 45, 55- 56].

2.2.6 Types of RFID Tags and Readers:

a) RFID Tags:

RFID Tags devices fall into two broad categories: Active, those with a power supply (a battery) and Passive, those without power supply. Passive tags draw their power from the transmission of the reader through inductive coupling and inductive coupling usually requires close proximity. So, the range of detection is a few centimeters to meter only. Active tags communicate through propagation coupling and respond to the reader's transmission drawing on internal power to transmit. The range of detection is much higher than of passive tags. An RFID device that actively transmitted to a reader is known as a transponder (TRANSMITTER/resPONDER). Active tags are typically read/write devices, whereas passive tags are mostly read only. Active tags are more expensive than passive tags, but the use of battery limits the life of the device while passive tags have an unlimited life, smaller, lighter and cheaper. The trade-off is limited data storage capability, reasonably shorter detection range and requirement of a higher-power reader. In electromagnetically "noisy" environments performance of these type tags degraded. Another type is semi-passive tags where tags having battery, but the battery run the chip's circuitry only. The device communicates by drawing power from the reader. Some commonly used tags are shown in figures fig. 2.3(a), 2.3(b), 2.3(c), 2.3(d), 2.3(e), 2.3(f), and fig. 2.3(g).



Fig.2.3 (a) Passive Tag Fig.2.3 (b) Semi-passive Tag Fig.2.3(c) Active Tags

Tags are available in various shape, size and protective housing. Tags used for animal tracking, which are injected beneath the skin, are approximately 10mm long with a diameter of nearly 1 mm. Some tags are encapsulated in credit card sized packages, typically building access cards. The smallest devices commercially available measure 0.4 mm and are thinner than a sheet of paper. Tags can incorporate read only memory (ROM), volatile read/write random access memory (RAM) or write once/read many memory (WORM).

Within the tag, ROM is used to store security data, a unique device identifier and operating system instructions. RAM is used for data storage during interrogation and response to the reader.



Fig.2.3 (d) Sticker type Tags



Fig.2.3 (e) Key type Tags



Fig.2.3 (f) Roll of paper type Tags



Fig.2.3 (g) Tag on human body

The enormous advantages of RFID system, which made it an emerging technology, are the non-contact, non-line-of-sight characteristics. RFID Tags can be detected and information can be read without line of sight and in a variety of environmentally challenging conditions like dust, snow, ice, fog, paint, grime, inside containers and vehicles and also while in storage. An RFID reader can read several hundred tags instantaneously with a response time of nanosecond range. Several applications find Tags coupled with sensors which can provide important information on the state of the articles and control or alarm action can be monitored effectively [25, 55].

b) RFID Readers:

A typical RFID reader is comprised of an RF module, a general purpose computing module, and a network interface unit. Generally, the general purpose computing unit is a low-end microcontroller or an embedded processor. All RFID readers provide the base services like: read the data contents of an RFID tag, write data to the tag (in the case of smart tags), relay data to and from the controller and power the tag (in the case of passive tags). Depending on the capabilities of the computing unit, different reader types provide different data processing services.



Fig.2.4 (a) Active RFID Reader Fig.2.4 (b) Passive Reader Fig.2.4(c) Handheld Reader

RFID interrogators are able to perform three more critical functions: Implementing anti-collision measures to ensure simultaneous RW communication with many tags, Authenticating tags to prevent fraud or unauthorized access to the system and Data encryption to protect the integrity of data. Some commonly used reader are shown in figures fig.2.4(a), 2.4(b), and fig.2.4(c).

In Table 2.3, frequency bands with their characteristics for various RFID applications are summarized.

Table 2.3: Frequency band of RFID applications [25- 49]

Frequency band	Characteristics	Typical applications
Low 100–500 kHz	Short to medium read range; Inexpensive; low reading speed	Access control; animal identification; inventory control; car immobilizer
Intermediate 10–15 MHz	Short to medium read range; Inexpensive; medium reading speed	Access control; smart cards; library control
High 850–950 MHz, 2.4–5.8 GHz	Short to medium read range; expensive; Long read range; high reading speed; line of sight required;	Railway vehicle monitoring; toll collection systems; Pallet and container tracking; vehicle tracking.

2.3 Zig Bee technology:

The Zig Bee standard was created to address the need for a cost effective, standards-based wireless networking solution that supports low data-rates, low-power consumption, security, and reliability [57]. Zig Bee supports self-healing mesh networking, which is a decentralized network topology very similar to the Internet. It allows nodes to find new routes throughout the network if one route fails, making Zig Bee a robust wireless solution. Basically, it is a most suited specification of higher level protocol for communication system with a low power solution. Zig bee specification is based on IEEE 802.15.4 standard for personal area network. It finds its useful application in many fields, including wireless switches, control etc. with comparatively low cost and simplicity than other WPANs like Bluetooth [57- 59]. Zig Bee has a defined rate of 250 kbps best suited for periodic or intermittent typically sell integrated radios and microcontrollers with between 60 KB and 256 KB flash memory.

IEEE 802.15.4 Standard Basics:

- Channel access is via CSMA with collision avoidance and Multilevel security.
- Three bands, 27 channels specified: 2.4 GHz: 16 channels, 250 kbps; 868.3 MHz: 1 channel, 20 kbps and 902-928 MHz: 10 channels, 40 kbps
- Message acknowledgment and an optional beacon structure.
- Works well for controllers, sensors, remote monitoring and portable electronics.
- Configured for maximum battery life, has the potential to last as long as the shelf life of most batteries.

2.4 Wireless sensor Network:

The Wireless sensor Network consists of a large number of wireless sensor nodes deployed randomly or in a specific pattern based on the application or situation. These tiny sensor nodes are consisting of sensing, data processing, and communicating components. The sensor network protocols and algorithms have the self-organizing capabilities. Sensor nodes are fitted with on-board processor, which has the ability to carry out simple computations and transmit only the required and partially processed data. One of the most important constraints on sensor node is the requirement of low power consumption. Traditional networks aim to achieve high quality of service factor (QOS), wireless sensor network focus on power

consumption. Sensor nodes are used for continuous sensing, event detection, localizing etc. Modern industry found many applications of WSN in areas like military command and control, surveillance, targeting, environmental disaster relief etc. The features of rapid and easy deployment, self-organizing property, fault tolerance and scalability make WSN a very promising technology for important and security applications [60- 64].

Optimization techniques in the Sensor Network Design:

Design optimization techniques aim to place the sensor nodes deterministically in order to meet the desired Network performance. The network topology can be established through careful planning of node densities and fields of view. However, in general, sensors deployment is random. But the nodes' distribution and positions affect network performance metrics numerously such as increased energy consumption, transmission delay, and reduced throughput.

For ubiquitous computing, the requirements of the sensor network infrastructure are quite different from the one for conventional environmental monitoring. Hence, when designing the practical sensor network architecture for the future ubiquitous computing environment, it is desirable that requirements of the applications be ensured. Designers have to take more care of hardware constraints which involves size, power, and cost on designing low-powered wireless sensor nodes.

CHAPTER 3

**VLSI IMPLEMENTATION OF A PROCESSOR FOR RFID
BASED POWER EFFICIENT HOME/OFFICE AUTOMATION
ALONG WITH SURVEILLANCE SYSTEM**

Chapter3: VLSI Implementation of a Processor for RFID based Power efficient Home/Office Automation along with Surveillance system

3.1 Introduction:

In the recent years, the process of automatic identification (Auto-ID) has become very popular in many industries, related to service, purchase, and distribution logistics. Automatic identification procedures are responsible to provide information about goods and products in transit, even people and animals too. The trend in the automated industry is to move towards fast and real-time identification and high level of accuracy. Such a level of real-time knowledge is often called *ambient intelligence*. There are various methods of automatic identification techniques. But among these methods Radio Frequency Identification (RFID) is the most reliable way to electronically identify, data capture, control, track, and inventory items using RF communication [25]. Today RFID has a very broad use, but most of the time such systems are invisible or are not recognized by the users.

In this work, VLSI design, and hardware Implementation up to the Register transfer level (RTL) schematic of an automated Home/Office power saving appliance, using RFID technology is described. The design has been made following ZigBee Network Standard (IEEE 802.15.4), since the RFID is most effective for short distance communication. Here, we have tried to integrate the above mentioned components of a typical RFID system into a FPGA based adaptive VLSI solution. Thus, all the controlling units being integrated into a single chip, increase speed of the processor, as the interconnect delays get reduced due to decreased RC - time constant. Trends suggest a reduction in size also brings a decrease in cost. It will also increase the overall system reliability and reduce the system size.

A home surveillance system using the same concept also has been developed and simulated as the second stage of this work. This work defines how this system is better in different aspects over the commercially available CCTV surveillance system. Here, besides the use of tiny wireless cameras, RFID technology has been introduced for identification of

any suspicious/ unknown entry. The total surveillance system is controlled by a controller PC using a Zigbee network. As the total system is wireless and without requirement of line-of-sight it can alarm the concerned person about the security threat of this specific home, it is much more suitable for modern lifestyle. As the system is self powered, it is similarly active during a power cut condition. Through 'SMS alert' technology a person can aware of the home security from a far distance also and take necessary steps immediately.

3.2 Literature Review:

RFID applications are now popularly accepted by each possible area due to its ease of use and enormous advantages. In a Taiwan hospital, RFID was used for In the US, over 400 hospitals currently use , 'hugs and kisses' RFID system to stop the cases of baby abduction or inadvertent mix-up. In this system, a 'hugs' tag is attached to the baby's foot and mother wears a 'kisses' tag as wrist band. If wrong baby is picked up, alarming sound will be activated. In Taiwan, HP and PDC (Precision Dynamics Corporation) have implemented a RFID based patient management system in CGMH (Chang Gung Memorial Hospital). In this system, accurate patient identification and automatic data gathering have improved the efficiency of health service. From the literature review, we gather sufficient information about the use of RFID technology to provide efficient health care service, well organized hospitals and its advantages [65- 67].

Woodwards Laboratories have developed a hygiene monitoring device that uses RFID to identify users. The i-Hygiene system is designed for both healthcare and the food industry and it is capable of monitoring that the organization hand hygiene policies are followed. The system consists of RFID tags placed on badges, gel dispensers equipped with RFID readers and computers with data systems. The i-Hygiene system collects information about the user each time he washes his hands. The system also generates reports of the hygiene and checks that proper hand hygiene is maintained [68]. The RFID technology is increasingly being used in everyday scenarios ranging from tracking and inventory control to patient management in healthcare. The RFID tag's very low price at high volumes and the benefits compared to the bar technology are a big factor behind this widespread phenomenon. Additionally, the RFID technology promises to help and automate many supply chain processes, and it has been shown useful in other areas such as baggage handling and aircraft maintenance. A common

factor for all of these applications is that they benefit from dedicated RFID middleware that provides reader management functionality, routing, and data processing. Also, RFID holds the promise to eliminate many existing business problems by bridging the costly gap between the real world of logistics and business units and the virtual world of IT systems [69].

In manufacturing plant, two portal tests are performed to determine the technical feasibility of RFID applications. In the first study, active UHF tags were attached to 50-83 pipe spools that were loaded on a trailer, and as the trailer passed through a gate where four antennas were installed, the pipe spools were automatically identified at different truck speeds. The challenge in this test was that some components might not be identified since the pipe spools were made of metal and they were in a very congested environment. In the second study, an active UHF tag was attached to a precast concrete component which was loaded on a trailer and the component was automatically identified as the trailer passed through a fictional gate where an antenna was installed. For both portal applications, identification of tags was tested at different truck speeds to determine the most appropriate speed.

A similar problem was identified in precast concrete manufacturer's storage yard where precast components were mislocated [70]. Precast components were stored in a large storage area and since they were relocated multiple times, precast manufacturer lost track of some components. In this storage area, the components were stored at fixed locations and mobile cranes were used to relocate the components. To overcome the misplaced component problem, researchers developed an approach and a corresponding prototype that identified the precast component being picked up by a crane and integrated the ID information with the location information received from GPS. The prototype was tested in a precast storage yard as a piece was relocated by a crane. Active tags were attached to components and RFID reader, antenna and GPS were placed on the crane that is used to relocate the components. Another study focused on the problem of mislocated materials at a construction site. The Construction site is a less controlled environment when compared with a manufacturer's storage yard, i.e., at construction site materials can be stored at any location and are relocated both by workers or equipment. To locate the materials that are scattered at a construction site, Song (2006) developed an approach that combined RFID and GPS [70]. This approach leveraged automatic reading of tagged materials by field supervisors or materials handling equipment that are equipped with a RFID reader and a global positioning system receiver. To

assess the technical feasibility of this approach, a mathematical model has been formulated where the job site is represented as a grid and the location of materials within the grid is determined by combining proximity reads from a discrete range.

Tracking tools and related information: Goodrum et al.(2006) proposed to use RFID for improving efficiency of tool tracking at construction sites and for storing operations and maintenance information on the tools [71]. To test the technical feasibility of this system, RFID tags were installed in the tool handles and these tools were identified at varying distances using a handheld reader. Also, the ability of the tags to store uncorrupted data was tested by storing some data and accessing it during site visits.

Tracking activities of labor: Navon and Goldschmidt (2003) highlighted the need for automatically identifying labor inputs, which is an important project performance indicator in construction projects [72]. They developed a conceptual RFID based data collection system, which is designed for indoor environments to automatically collect worker's location data at regular time intervals. This location information will be converted into labor inputs using algorithms. In this approach, RFID tags would be attached to building elements and workers would carry personal units that have RFID readers, which record the information from the tags that the worker passes by. This data would be downloaded once a day and workers' locations would be calculated.

In view of the above study, it appears that there are still some scopes to explore some RFID applications and their adaptive VLSI implementation suitable for wireless communication systems.

3.3 Design and Implementation of Processor for RFID based Power efficient Home/Office Automation

A fully automated small business/home wireless network using RFID technology is presented here. The RFID system consists of a reader and a tag which may be active or passive in nature. The passive RFID tags are powered up on receiving RF signals from the readers. In this work, a small, smart light and temperature controlling unit has been designed and simulated .The operating principle is based on position estimation of the tag in a room

and for this position estimation a multi sensing mechanism has been used [73]. A multi sensing reader can transmit signal at different power levels periodically with a regular interval. In determining the position of the tag the lights of that particular area are turned on while those of the other regions are either switched off or power is given to secondary low power consuming lights thereby saving the power wastage unnecessarily. Also here a temperature controlling, and monitoring unit has been designed where temperature sensors and digital thermometers have been used to monitor the room temperature. The temperature controlling system is activated by the presence of the tagged object in the room. The temperature controlling unit takes care of the air conditioners present in the room to keep the temperature within a specified comfortable range. Also, using this temperature controlling unit a fire alarm system has been proposed. For the ease of design and analysis the whole idea has been presented in small segments and each segment has been explained separately. In order to substantiate the proposed scheme, the performance of the scheme is studied with suitably designed test benches. The performance of the proposed scheme has been found satisfactory.

In this section the main controller unit of the RFID Zig-Bee processor has been briefed. At the very beginning the architectural view of the controller unit has been described.

3.3.1 Operational flow chart:

The design algorithm and operational flow chart are shown in Fig 3.1. The architectural block diagram of the system is shown in Fig 3.2. The Algorithm starts with the search of tags for long range sense, for our design clarity, we have named three zones as zone1, zone2 and zone3. Zones are detected by the Reader after a time interval, as zone1, zone2 and zone3. We consider that IDs detected in zone1 are ID1, for zone2 are ID2 and for zone3 are ID3. Lights in zone1 are L1, L2, in zone2 are L3, L4 and in zone3 are L5, L6. There are two air-conditioners, named as AC1 in zone1 and AC2 in zone3. There are also digital thermometers for measuring room temperature. We have assigned three level of temperature, named as t1 or temp1 for low level, t2 or temp2 for high level and t3 or temp3 for excess high temperature. TC1 and TC2 are two sensor terminals activated by zone1 and zone3 respectively, which is fed to the ADC unit and the digital signal 'D1' is fed it to the temperature control unit of the processor. The processor compares it with the level of temperature already stored in its memory as t1,t2 & t3. If D1=t1, ac1_off signal becomes high and switch off AC1. If D1=t2, ac_off signal becomes low and switch on AC1. If D1=t3

or room temperature touches the excess high temperature, 'alarm' signal becomes high, by which we can generate a fire alarm buzzer on.

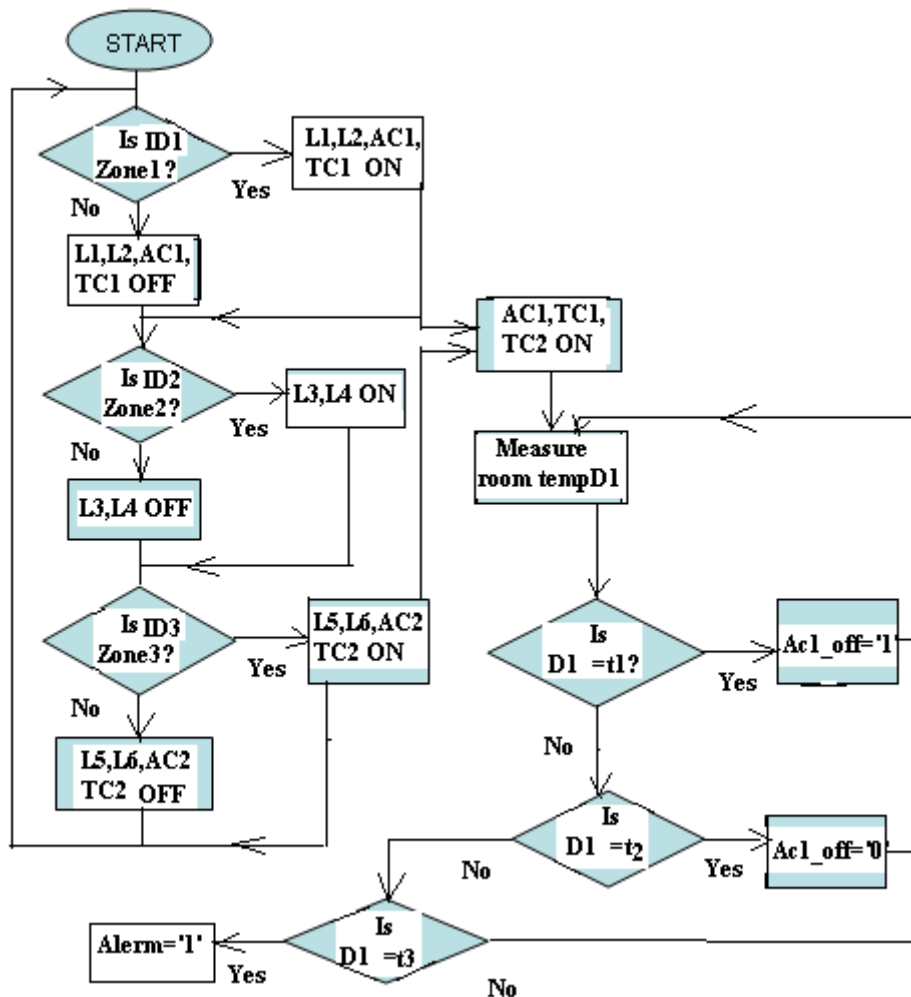


Fig 3.1 Flow chart of the operation

3.3.2 Proposed Algorithm:

Step1: Search tag for zone1, if identified, switch on the lights and AC of this zone. Suppose there are two lights L1, L2, Air conditioner AC1 and a temperature sensor signal TC1.

Step2: If there is no tag, reader searches tag for zone2. L1, L2, AC1 and TC1 remains 'off'.

Step3: If searching for tags for zone2 identifies any tag, switch on the lights of this zone. Let the lights are L3 and L4. For larger environment, AC can be taken into account but in our design we have chosen two ACs, one in zone1 another in zone3.

Step4: if there is no tag in zone2, searching of tag for zone3 starts immediately. Actually Reader searches tags for three zones at a regular interval of certain nanoseconds. If any tag is identified by reader, power is on for this particular zone otherwise 'off'.

Step5: In zone3, suppose there are lights L5, L6 Air conditioner AC2 and temperature sensor TC2. So, if any tag is found in this zone by the reader, these points are ‘on’, otherwise ‘off’.

Step6: When ACs are ‘on’, temperature sensors are also ‘on’ which continuously get the reading of the thermometer D1, compares the temperature with the temperature levels t1,t2,t3 predefined in the processor memory.

Step7: if $D1=t1$, the low temperature level, an ac_off1 signal is high (‘1’) which we can use to forcefully off the AC for that moment.

Step8: if $D1=t2$, the high temperature level, the ac_off1 signal is low (‘0’) which we can use to forcefully ‘on’ the AC for that moment.

Step9: if $D1=t3$, the excess high temperature level, the ‘alarm’ signal becomes high (‘1’) which we can use to generate a sound like a fire alarm to draw the attention

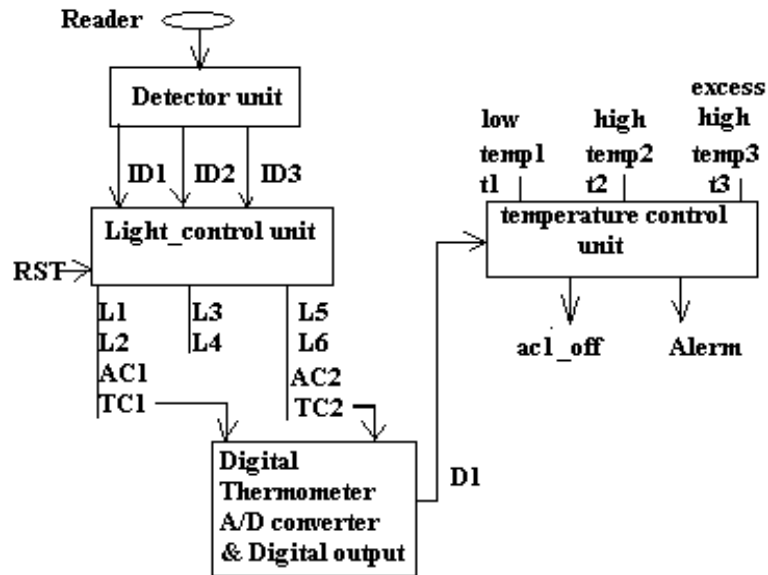


Fig 3.2 Block Diagram of the Controller Unit

3.3.3 Operational Block diagram:

As shown in Fig 3.2, the block diagram of the system, there are two major blocks in the processor by which it controls the system. These are the ‘*light control unit*’ and the ‘*temperature control unit*’. As reader switch over to different zone as per our consideration, we have designed a ‘*detector unit*’ which selects the IDs of different zones, as ID1, ID2 or ID3. TC1 and TC2 are two temperature sensor signals for two zones fed to the digital

temperature recording or digital thermometer and ADC module. D1 is the signal fed to the temperature control unit indicating the temp of the room.

a) **Detector unit:** To describe this unit we have to first discuss about the zone determination according to the different range of transmission of the RFID Reader. If we consider a rectangular room as shown in Fig 3.3, the reader covers different region at different transmission range, and we have considered the regions as zone1, zone2 and zone3. When it is higher range of transmission, ID of zone1 is detected, when it is medium range, ID of zone2 is detected and when it is low range, ID of zone3 is detected.

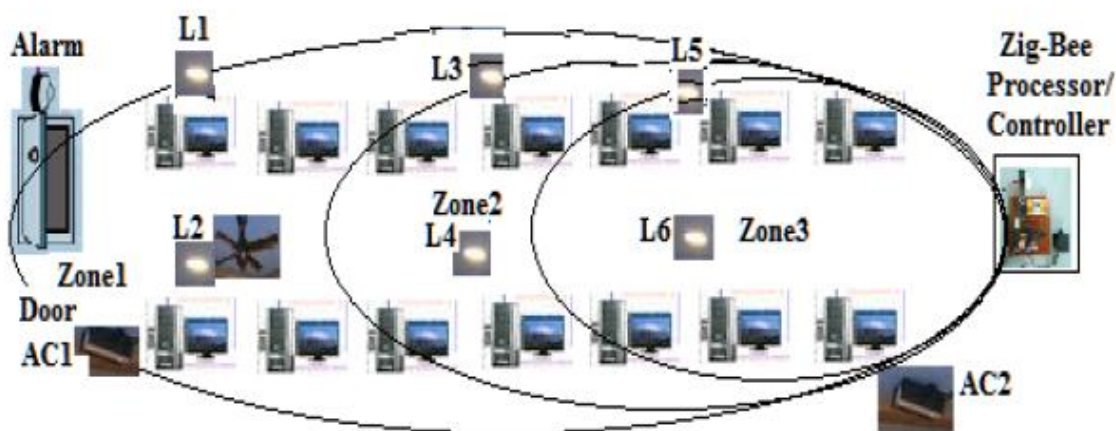


Fig 3.3 Room arrangement

b) **Light control unit:** This unit checks the IDs. When ID1 is detected of zone1, lights L1, L2, AC1 and TC1 becomes ‘on’, when ID2 is detected of zone2, lights L3, L4, becomes ‘on’ and similarly when ID3 is detected of zone3, lights L5, L6, AC2 and TC2 becomes ‘on’, when there is no ID detected, the power is in ‘off’ condition in the respective zone. Thus, the utilization of power becomes restricted as per requirement, saving power consumption as a result.

c) **Temperature control unit:** The operation of temperature control unit depends on the detector unit and light control unit. Thus, they are closely related to each other. It has two output terminals ‘ac_off’ and ‘Alarm’. As soon as the AC and the thermometer input TC are ‘on’, the temperature control unit continuously monitors the temperature of the room. As per our design, we have previously set the high/low/extremely high temperature in the memory of the processor; it will compare and set the ‘ac_off’ and ‘Alarm’ terminals high accordingly.

3.3.4 Principle of Operation:

The room organization is shown in the adjoining figure (Fig 3.3). The reader is mounted on the wall opposite to the door. The lights L1 to L6 (here) are arranged in three zones, zone1, zone2 and zone3 respectively. TC1 and TC2 are the two temperature sensors. AC1 and AC2 are the two air conditioners. There is a remote database system inside the room to which the reader may be connected. The light control system should be designed to save energy. The reader should have multi level power transmitting capability (3 here). Here the antenna is considered to radiate power at three different levels shown by the lobes in Fig. 3.3.

When the tagged object enters the room it's detected by the reader instantaneously. Let, first the tag is in zone1, so it will be detected by the maximum power radiation. Next, after 1 ns (say) the reader radiates at the intermediate power level and again after 1ns it radiates at lowest power level. So, when the tag is in zone1, of course it won't be detected by intermediate and lowest power radiation. So, then the lights of this regions only are switched on. But that time, the other lights are either switched off or power is given to the secondary very low power consuming lights depending on the requirement. Now if the tag is in region 2 then it'll be detected by both maximum and intermediate power radiations. Then the lights of this zone are switched on and the others are switched off. Similarly, if the Tag is in zone3 then it'll be detected by all the three radiations and hence the lights of this zone are switched on while the others are put out. In temperature controlling operation the temperature sensors plays important role. The digital thermometers DT1 and DT2 are kept for recording and displaying the room temperature. The temperature of the room is to be fixed within a specified range. The air conditioners are turned on by the presence of the tagged object in the room. Now TC1 and TC2, two temperature sensor signals are used to monitor the temperatures of the different portions of the room and fed a signal D1 to the temperature control unit. If these sensors can sense a temperature that drops below the expected lower specified temperature of that area, then the air conditioner of that area is turned off. Again, when the temperature of that area exceeds the expected high specified temperature, then the air conditioner is turned on. Now there is a maximum specified temperature that is not supposed to be exceeded under any circumstances and if yes then a fire alarm is turned on.

3.3.5 Hardware Implementation and simulation results:

Now we will observe step by step implementation and simulation result of each block and the final processor showing the satisfactory performance. Following the operational flow chart and block diagram we have designed the processor and simulation results are shown in the following figures. The RTL view of processor and its components are also shown. Fig 3.4 shows the internal view showing the two parts synchronized by 'rst'. In the test bench waveforms id1, id2, id3 represents three IDs for three separate zones, temp1, temp2, temp3 are predetermined temperature level which we can set any time for any desirable temperature of the room. Room temperature is denoted as 't' here, which has been chosen randomly for simulation purpose.

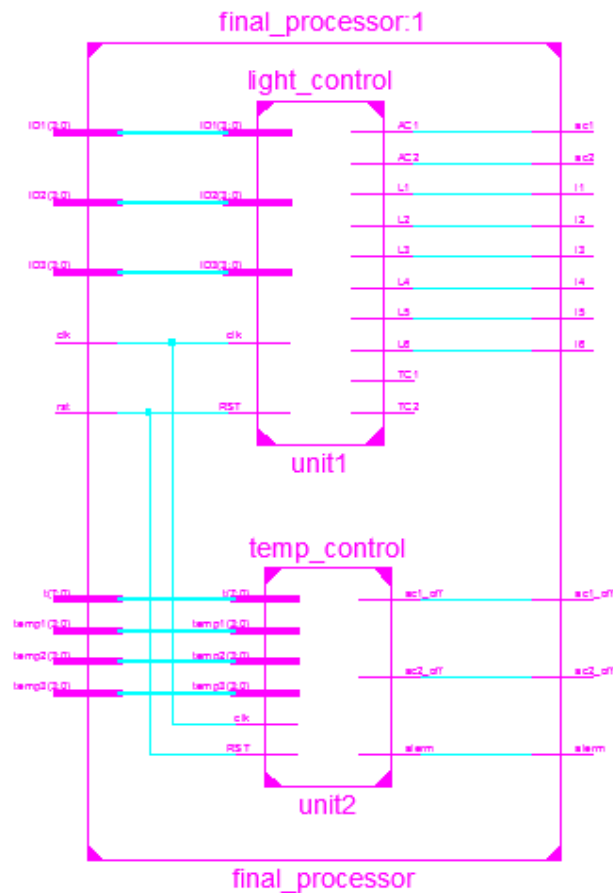


Fig 3.4 RTL view showing two parts of the Processor

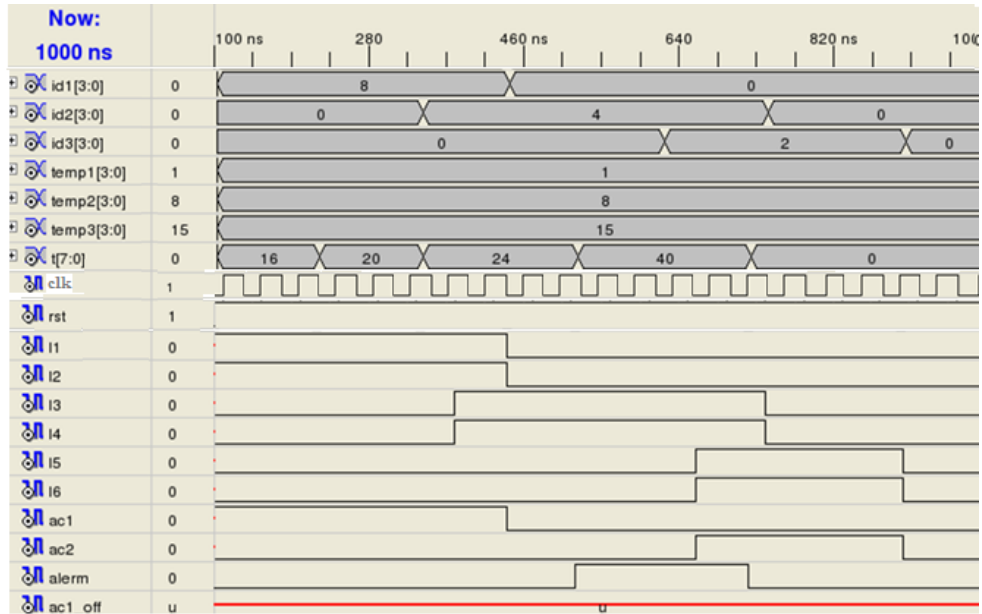


Fig 3.5 Simulation result: Final output of the Processor

Fig 3.5 shows the final output of the Processor which has two parts, the light control unit and the temperature control unit, the description, simulation result and the RTL schematic of both has been discussed in the following paragraphs.

a) Detector unit:

The ID detection unit is the vital part of the processor. According to the selected zone, ID is detected and the control unit controls the power of the respective zone accordingly. Firstly we observe the output of the zone selection unit which selects the zone for proper functioning of the final processor.

Zone selection unit:

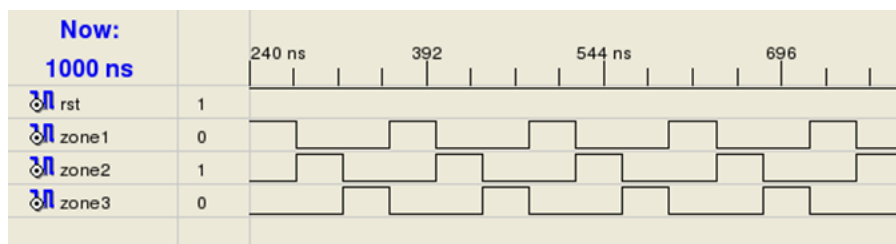


Fig 3.6 Zone selection

Fig 3.6 shows the simulated waveform for zone selection unit. In the above said waveform we observe that three zones are selected, each for similar time duration and so on. Fig 3.7 shows us the ID detection as per activated zone.

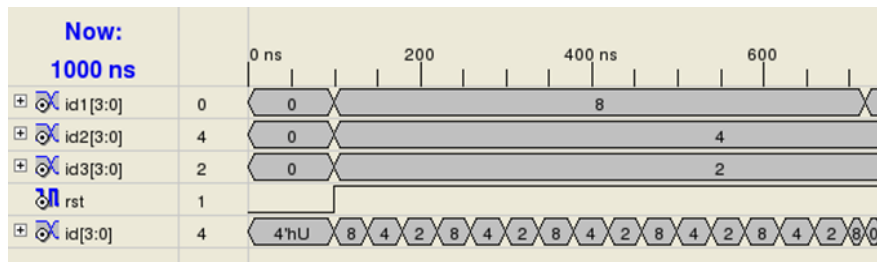


Fig 3.7 ID detection as per zone selection

As per our block diagram shown above, the detector unit detects the IDs present in the activated zone using the zone selection unit as a component. In Fig 3.7 we observe the required result of the detector output that ID1, ID2 and ID3 (here these are considered as 8, 4 and 2) are detected at alternate time interval.

b) Light control unit:

According to selected zone, IDs are detected, and the light control unit controls the power on/off of lights and ACs. Here we will observe the simulated output of this unit.

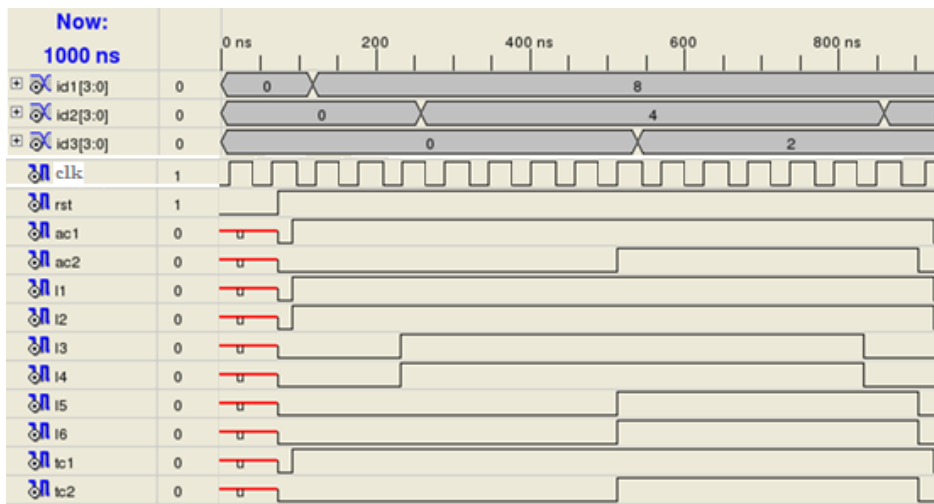


Fig 3.8 Output of Light control unit showing ‘on’ / ‘off’ of lights and ACs of activated zones according to presence of ID

In Fig 3.8 we observe the simulated output of the light control unit. From the waveform we see that as per our requirement, only the lights and ACs of respective activated zones are ‘on’ during that period when the IDs are present. Otherwise power of this zone is off. Here power on indicates level ‘1’ and power off indicates level ‘0’.

Fig 3.9 shows the RTL schematic view of the processor of the Light control unit.

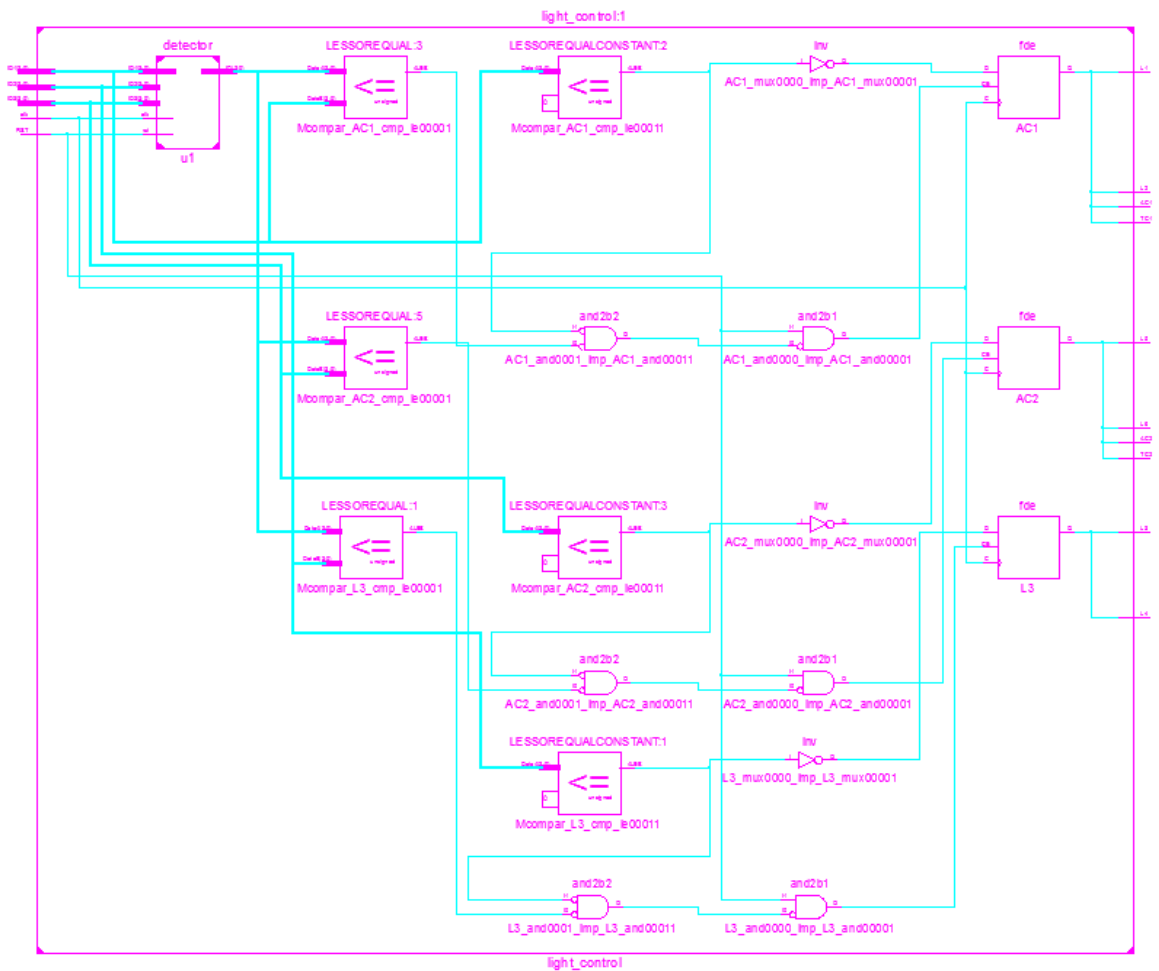


Fig 3.9 RTL schematic view of the Light control unit

c) Temperature control unit:

To control the room temperature within a specified temperature range and to generate an alarm signal when temperature of the room touches a limit of excess high temperature we design another part of the system which is fed by the output of two digital Thermometers. Fig 3.10 shows the simulated test bench wave form of this ‘Temperature control unit’.

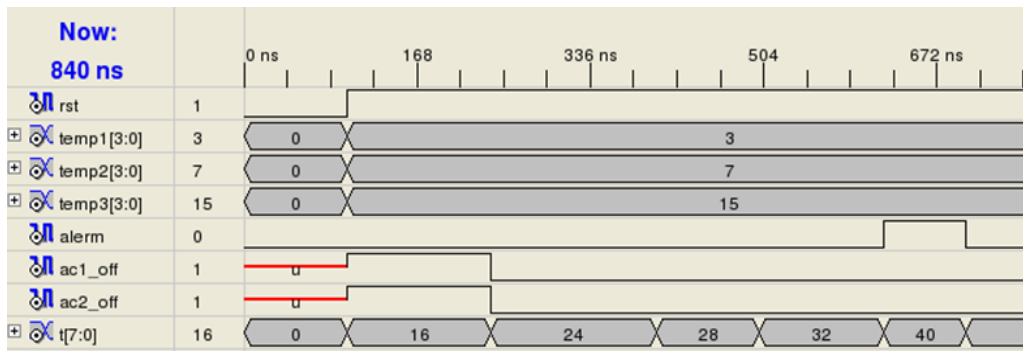


Fig 3.10 Output of Temperature control unit

For simulation purpose we have chosen input from thermometer as ‘t’. The three level of temperature also chosen as ‘3’, ‘7’ and ‘15’, for experimental purpose. For our temperature control unit, when room temperature ‘t’= ‘16°C’, AC1 & AC2 should be ‘off’ or the ‘ac1_off’ signal and ‘ac2_off’ signal should be high, when temperature ‘t’= ‘24°C’ both the signal are low, AC1& AC2 will be ‘on’. When ‘t’= ‘40 °C’ or reaches the extreme level of temperature, the ‘alarm’ signal should be high. From Fig 3.10 we observe our desired result. We kept AC2 unaffected, but we have flexibility in our design for more generalize the system.

Synthesis Results:

After successful synthesis of the design, we achieve the list of hardware requirements and device utilization chart of the Final processor and other controlling units as tabulated in Table 3.1. We can optimize the design in a more generalized form and modify our system any time according to customers’ requirement using reconfigurable Field Programmable Gate Array kit. VHDL code has high level scripts to design hardware without a long effective time requirement and efficient labour.

Table 3.1: Hardware requirements for Final processor and other controlling units

Parameters	Final Processor	Light Control unit	Temperature Control unit
32x4 bit ROM	1	-	1
1 bit Latch	10	3	2
4 bit Latch	5	1	4
4 bit Comparator	9	6	3
1 bit to 4 bit Multiplexer	3	3	-
4 bit XOR2	3	-	3
No. of 4 input LUTs	47	18	29
No. of Slice Flip-Flops	23	7	16
No. of Bonded IOBs	44	23	24
IOB Flip-Flops	3	-	3
Total memory usage	77732kb	76028kb	76860kb

Maximum period: 3.784 ns (Maximum frequency: 264.306 MHz)

Minimum input arrival time before clock: 6.768 ns

Maximum output required time after clock: 6.897 ns.

The RTL schematic view of the Temperature control unit is shown in Fig 3.11.

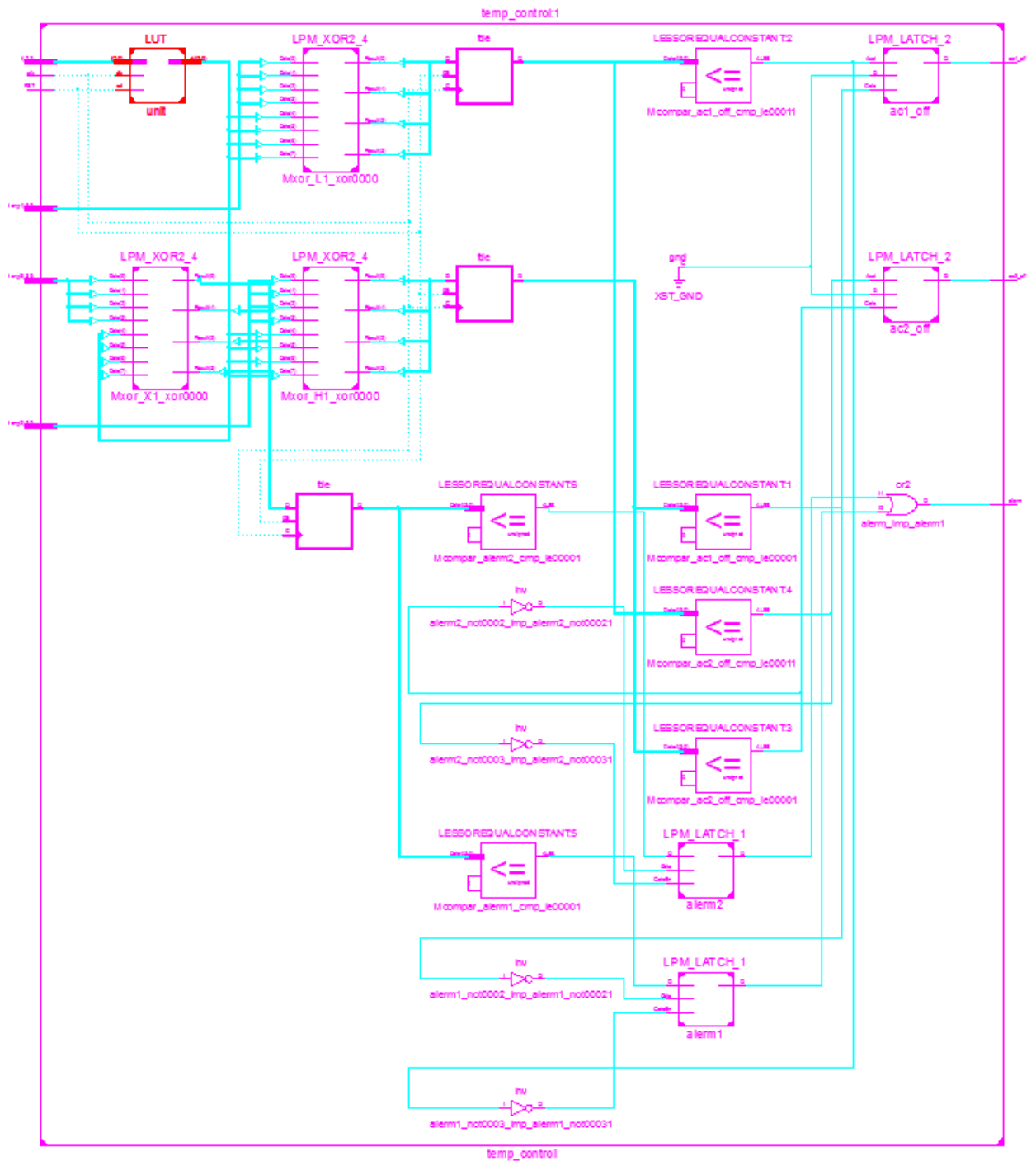


Fig 3.11 RTL schematic view of Temperature control unit

3.3.6 FPGA Implementation:

The working of the processor in real time environment is verified using FPGA kit. XPower and Datasheet may have some Quiescent Current differences. This is due to the fact that the quiescent numbers in XPower are based on measurements of real designs with active functional elements reflecting real world design scenarios. In order to substantiate the feasibility and effectiveness of the proposed system along with temperature monitor/sensor device, alarming buzzer device the performance of the scheme is simulated, synthesized, and tested with a virtual home automation system using the FPGA device. We have checked our designed processor using an FPGA kit successfully. In Fig. 3.12, the screen shot of FPGA implementation is shown.

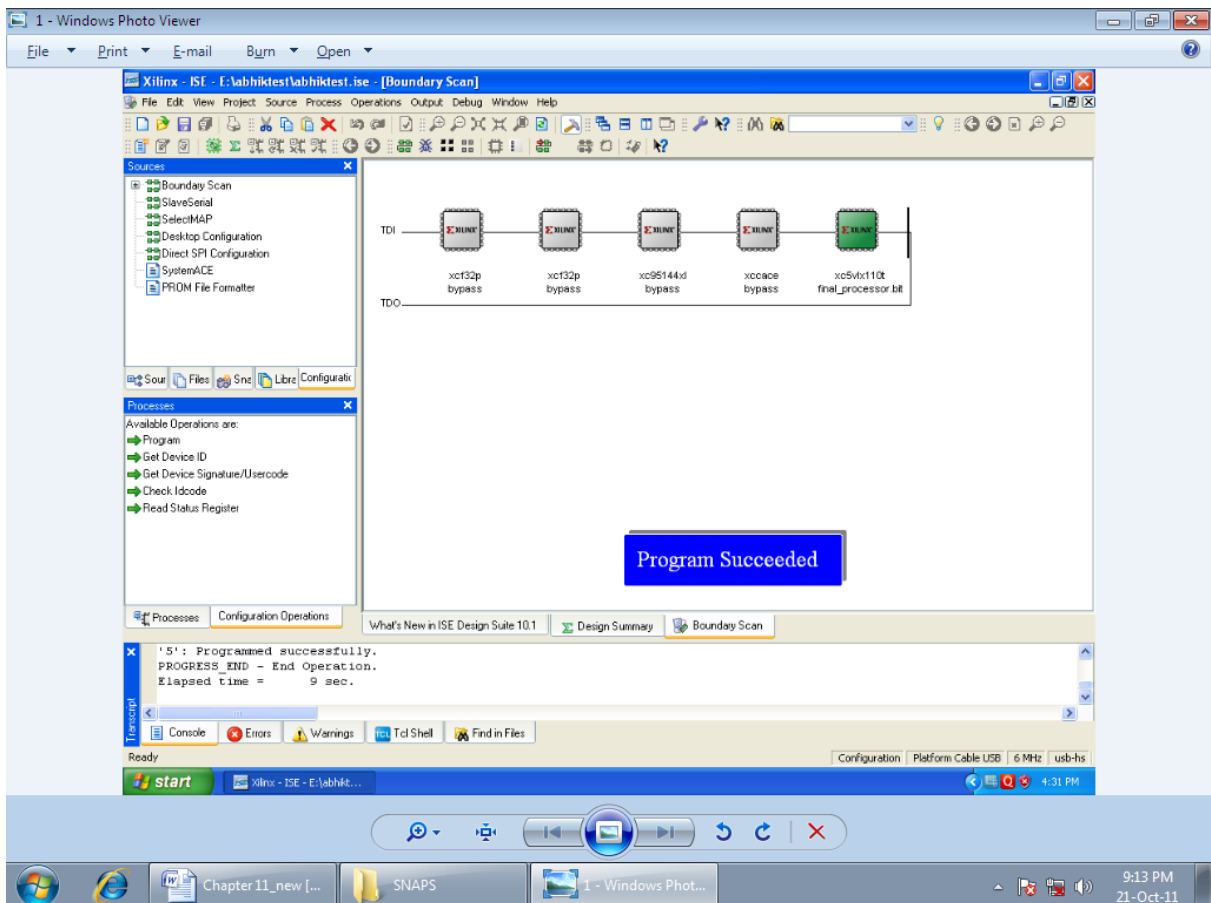


Fig. 3.12 Screen shot of FPGA Implementation

Fig 3.13 and Fig 3.14 shows the technology schematic view of the Temperature control unit and the final processor.

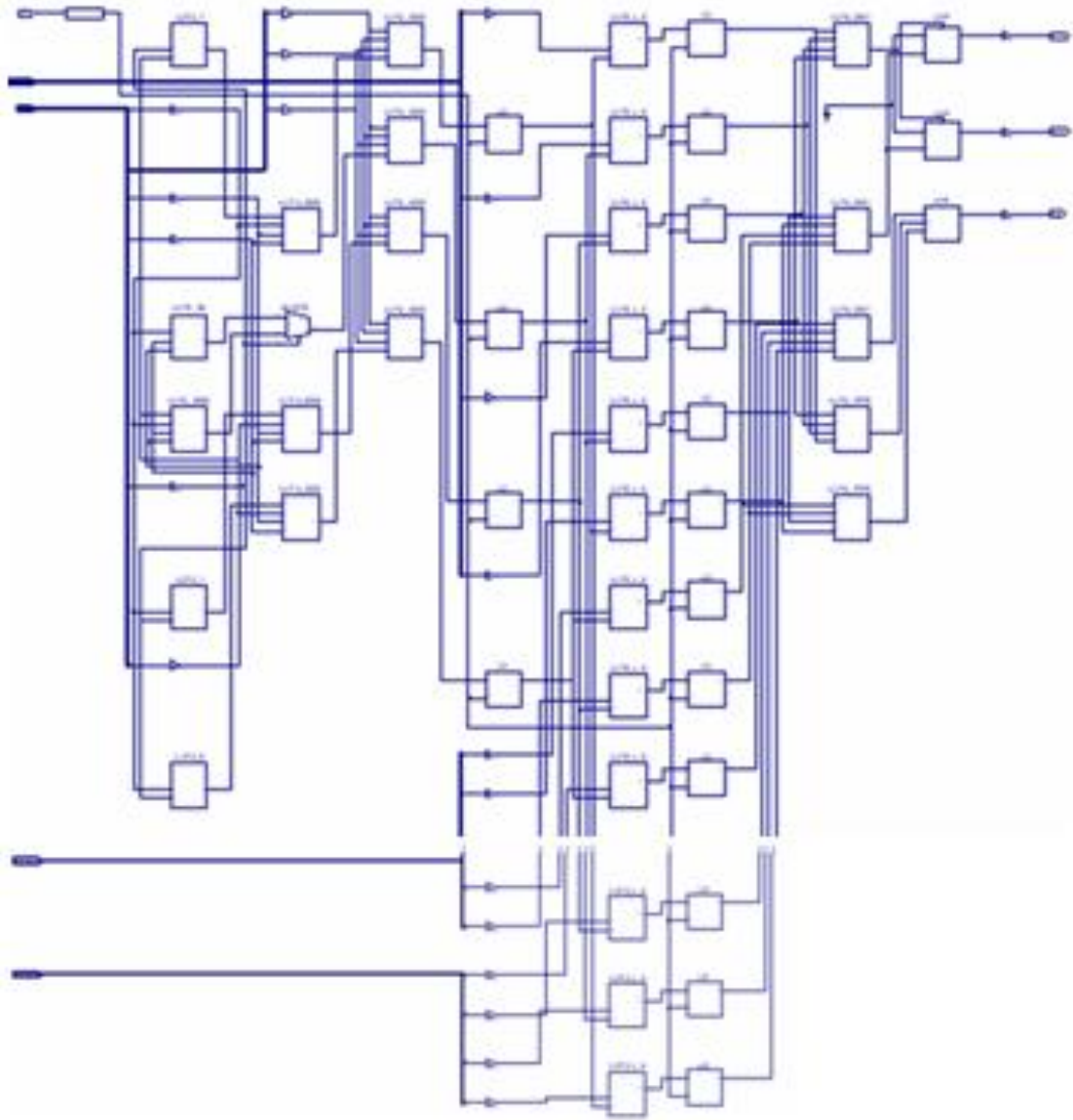


Fig 3.13: Technology schematic of Temperature control unit

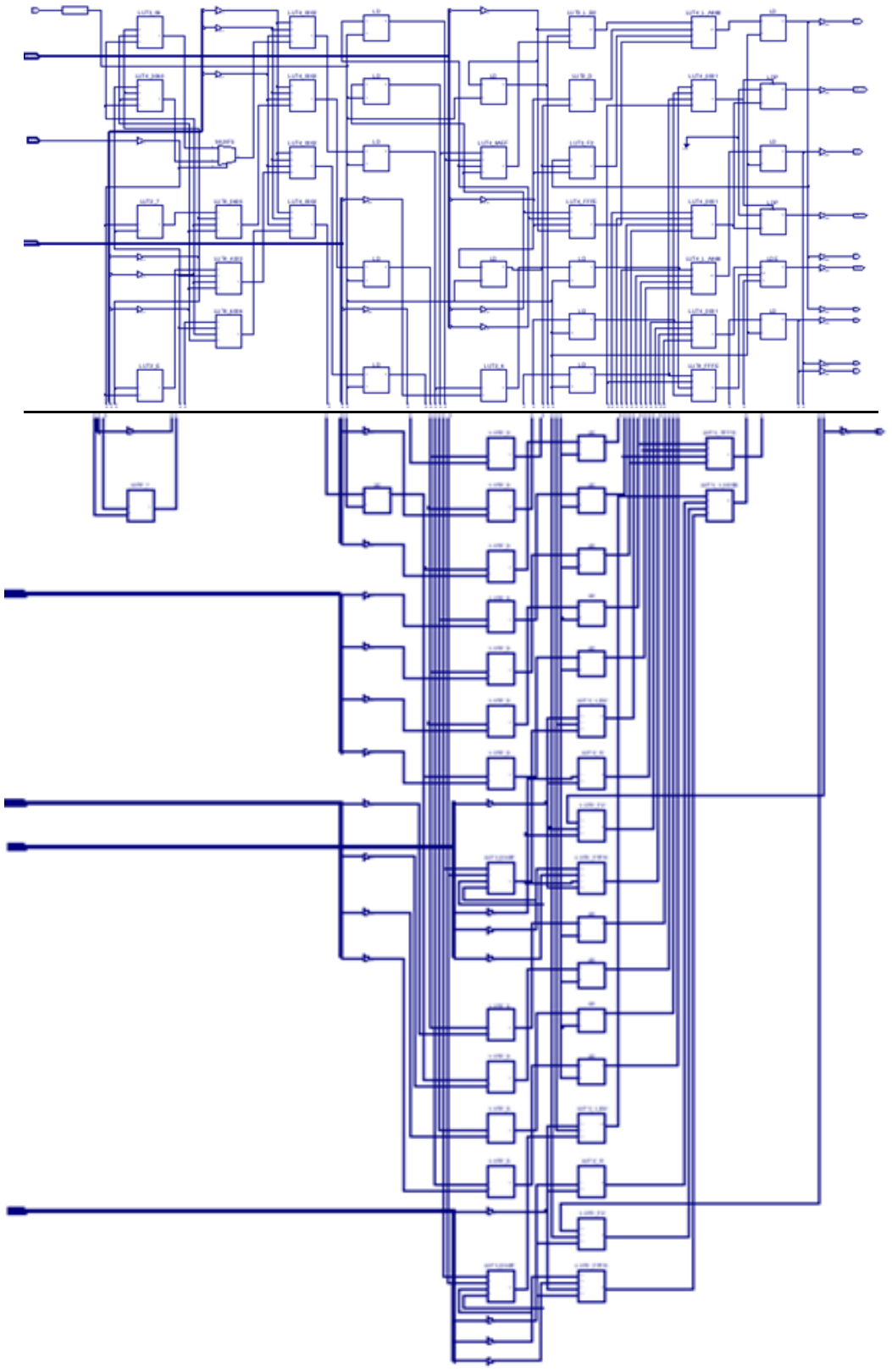


Fig 3.14: Technology schematic view of the final processor (with brake in page)

3.4 Design and Implementation of Processor for RFID based automatic home surveillance system:

The use of surveillance camera is now increased globally in different field. UK is the highest user of surveillance camera, almost one million for 55 million people. If we want to integrate the advantages of advanced Zigbee technology and cost effective, low power wireless concept in a single application like domestic surveillance, it will bring a great challenge among the researchers and will create an attractive system. We have proposed one such a system in the present work to interact with the new technological wave. We have designed and implemented the processor up to the RTL schematic level. Our system is useful for domestic surveillance. Whether we are at home or out of the station, surveillance system designed by us will somehow manage to protect our home from unwanted entry of any unknown person. Further, it will alert the assigned neighbors also with its inbuilt automatic system to switch on the flood light or alarming tune or by message through a cell phone/pager.

3.4.1 Brief overview of existing surveillance systems:

Wireless technologies deliver opportunities for rapid ad hoc connections and the possibility of automatic, unconscious connections between devices. Wireless technologies will virtually eliminate the need to purchase additional or proprietary cabling to connect individual devices, thereby creating the possibility of using mobile data in a variety of applications. Crimes are reduced effectively and criminals can be identified immediately. With this respect, India is also progressing and adopting the use of surveillance camera. In stations, shops, malls and multiplexes, airport everywhere we notice CCTVs are using for the surveillance system.

But this is not full proof and has some disadvantages, like:

- It has close circuitry and wired system which can be damaged or failed any time.
- It is power dependent, so power failure can cause the system dull, but wireless can be opted with battery.
- In this system one should always check the monitor or within a predetermined time period, otherwise all data images will be lost.

To overcome these so many problems we have chosen the RFID technology, which is neither a wired system, nor a power dependent system and it becomes more reliable. With the rapid development, RFID technology, the digital information exchange and data transfer has also improved tremendously in regards of highly secured data transfer. The global commerce has improved the modern R & D on the identification and tracking techniques of tagged items using RFID systems.

ZigBee protocols are intended for embedded applications requiring low data rate and low power consumption. The resulting network will use very small amounts of power; individual devices must have a battery life of at least two years. ZigBee is based on IEEE 802.15.4, that provides users with a cost effective standard, with the ability to run for months or years on inexpensive primary batteries for typical applications. ZigBee devices operate in unlicensed bands of 2.4 GHz. The range of ZigBee can be extended from 10 meters to 100 meters and is dependent on the power output of the devices and the coverage area. ZigBee achieves its attractive low power consumption. Once a node is associated with it communicates and returns to sleep mode, lowering the power consumption effectively [57-59].

The advantages of our Zigbee enabled RFID home surveillance system as follows:

- ❖ It is a wireless system.
- ❖ It is not power dependent, though the Zigbee chip uses its own inbuilt battery power, so it can work without any interruption.
- ❖ The system is not weather dependent and minimum probability of damage.
- ❖ It has a self alarming system and if an alarm is detected it can be programmed to inform a person through a computer monitor display, or cellular phone or audible alarm.
- ❖ A Zigbee module with special processor will monitor and control the overall system.

3.4.2 Proposed System:

Features of our system:

- CDMA protocol is used to transfer information between other nodes and the controller.
- Tracking cameras with Zigbee chip is fitted with a movable robot and works as active nodes. It sends data images in the form of digital or binary numbers.

- The Processor can take decision based upon the received data images.
- The processor controls the total system and it is the heart of the system.
- If occupancy sensors are present, they can also be used as burglar alarms.
- To reflect the control action a buzzer, a flood light or blinker or specific alarm tune is set or a person can be informed through a computer monitor display, or cellular phone or audible alarm.
- The system will adopt sleep scheduling for the working of the Zigbee module so that we can save more power and enhance the lifetime of the system. The sleep time will be two minutes or more as per preference.

3.4.3 Components of the system:

1. Zigbee module---- The communication medium. Zigbee protocol is used because of its simple technology, high performance, high detection range and it is less expensive than other WPANs. It has a long battery life, highly secured and supports low power mesh networking. Zigbee chip is an integrated radio and micro-controller with 60 to 256 kB flash memory.
2. Wireless camera---- It is fitted with ZigBee chip, which monitor the environment and transmit data images to the receiver attached to the computer display. A USB TV card is required for the interface.
3. Personal Computer---- It receives data images from the wireless camera, display on the monitor. Zigbee receiver and the processor designed by us is attached with it, which is the controller of the system.
4. X-CTU software----- It is used for configuring Zigbee. A USB adaptor for Zigbee is needed for that purpose or to set up the network working.



Fig 3.15 Zig-Bee module and board embedded with Zig-Bee module

In Fig. 3.15, the Zig-Bee module and the board embedded with Zig-bee module used for controller section is shown.



Fig 3.16: Occupancy sensor and wireless camera used for home surveillance

In Fig.3.16 we observe the occupancy sensor and wireless camera used for home surveillance system development. An occupancy sensor is an energy saving device designed to detect the presence of human occupants in a given area. The 5 in 1 Stagnant Occupant Sensor, is useful for both automation and security purpose. It has PIR Detection Angle = 110 Degrees and PIR Adjustable detection range 10 meters diameter. Occupancy sensor generates an occupancy signal indicating the presence of one or more persons within a predefined area.

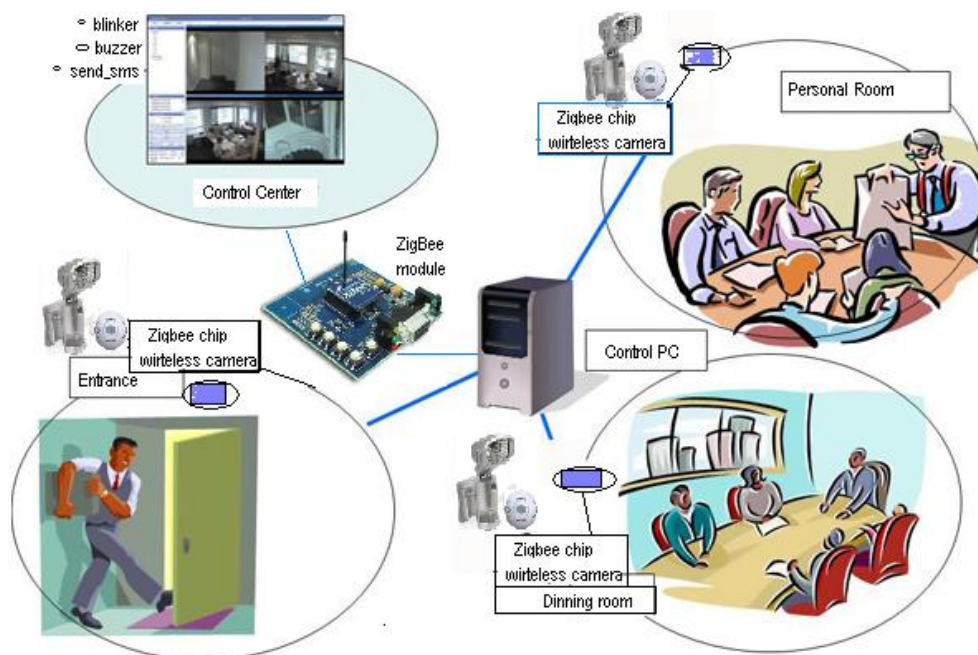


Fig 3.17: Pictorial description of home surveillance system

In Fig 3.17 we focus on the pictorial description of the proposed home surveillance system. We can place the wireless camera anywhere in our home including terrace, main door, and confidential room like bed room or other important places together with an occupancy sensor.

3.4.4 Hardware Implementation of proposed system:

System Algorithm:

Step 1. Store about ten known images or ID (P_i) for family members/friends in memory for 'No Action' state.

Step 2. Wireless camera capture image and with the mobility sensor it checks if the target is static or dynamic and transmit data image to the receiver end accordingly.

Step 3. Computer compares the image and verify

Step 4. If the received data image matches with any of P_i , the 'No Action' state;

Else

'Suspicious node' S_i is activated.

Step 5. As ' S_i ' activates, it displays an alarming message on the monitor along with the image.

Step 6. Wait for 10 seconds. If the user ignores it, transmits control data ' C_i '.

Else

Go to Step 2.

Step 7. The Node receives ' C_i ' and process it.

Step 8. A red blinker will be 'ON' for 30 seconds or till the user takes any action.

Step 9. An audible alarming 'Buzzer' will be 'ON' if no action is taken even after 30 seconds.

Step 10. If the user takes no action within 60 seconds, or any other predetermined period, 'send SMS' terminal activates;

Else

Go to Step 2.

Step 11. If 'send SMS' terminal is activated then

Zigbee module (smart energy 2.0) informs the user/other person through pager/computer/cell phone.

Else

Go to Step 2.

In Fig 3.18 the operational flow chart of the proposed surveillance system is described. When a suspicious image or image of an unknown human being is captured by the camera, a red blinker will be 'ON' and alert the user. User can check the image immediately on monitor display and may press 'Exit' or not. If the user is not aware of the blinker, sleeping or in the toilet or far from the blinker, system will wait for 30 sec and then an audible alarming buzzer will be 'ON' automatically if there is no response from the user side.

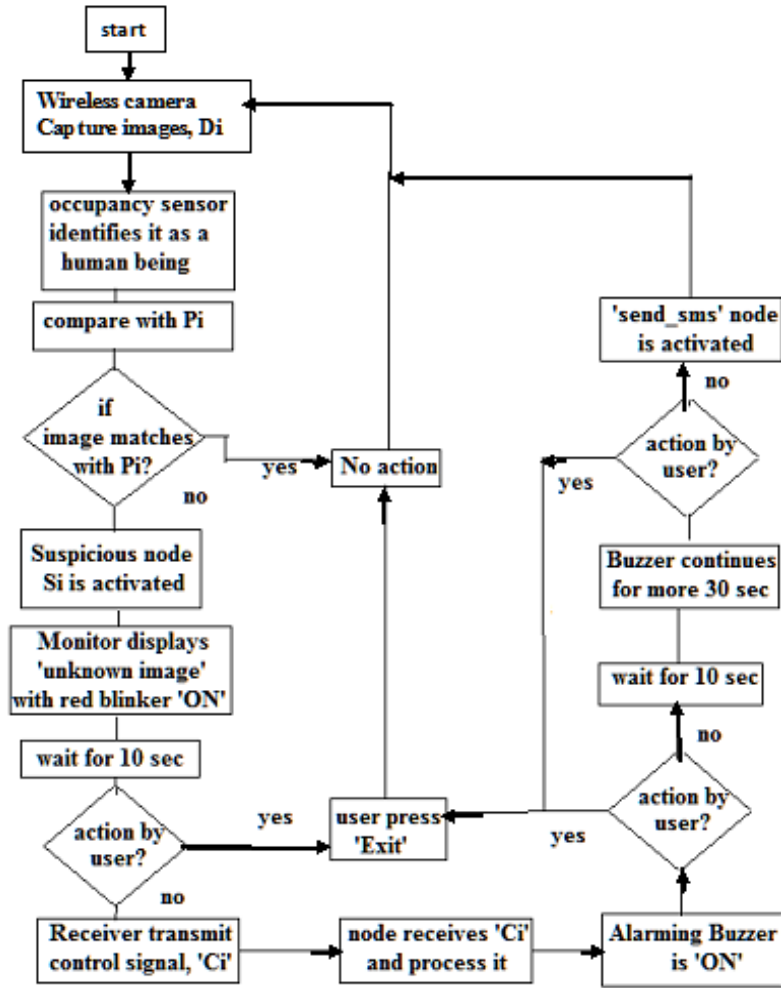


Fig 3.18: Operational flow chart of the proposed system

3.4.5 Operational Block Diagram:

According to operational algorithm, we get the flow chart of system activities, thus we achieve the operational block diagram as we observe in Fig 3.19. In Fig 3.19, we have assigned two major blocks, named as Monitoring camera node and Controller node.

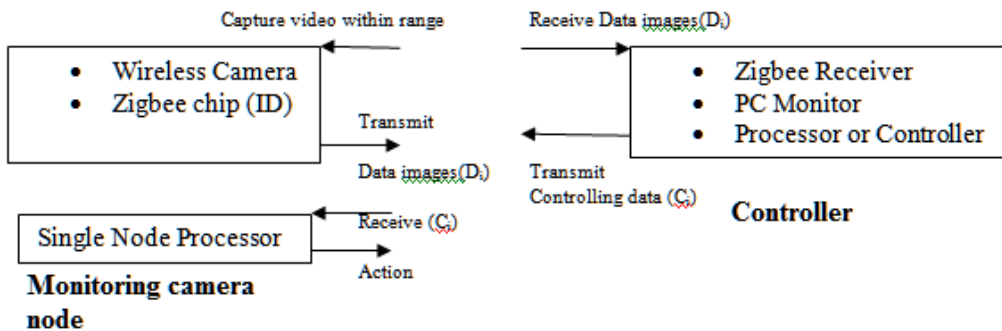


Fig 3.19 Block diagram of proposed system

Monitoring camera node consists of wireless camera, Zig-Bee microchip with single node processor. It is a very tiny assemble to keep anywhere of a building for monitoring the environment. The Controller does the major part of the surveillance system. It consists of the Zig-Bee Receiver interfaced with a personal computer and the processor designed by us to transmit the controlling signal according to our algorithm as described in Fig 3.18.

3.4.6 Simulation Results:

We have designed different operational blocks as per required conditions as shown in Fig. 3.20. The designs in VHDL code are simulated using Xilinx9.2 ISE simulation tools.

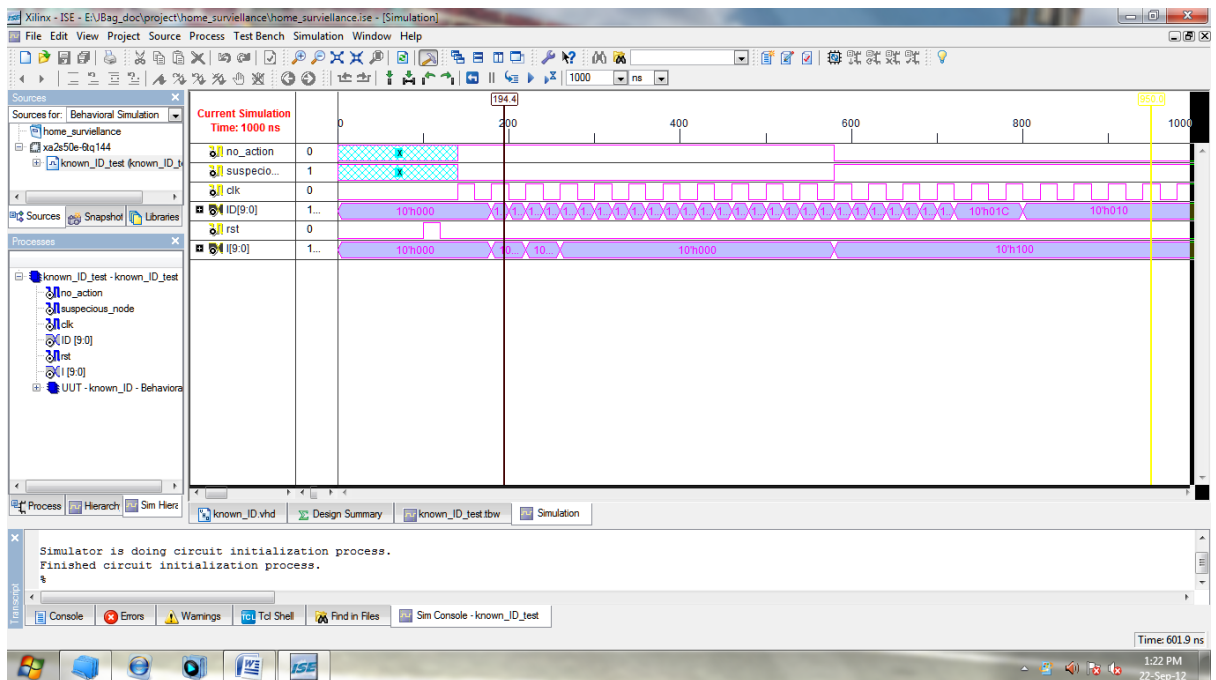


Fig 3.20: Test bench simulation for ID detection module in the controller section.

The test bench simulation results we observe in Fig 3.20. After successful simulation, we achieved the synthesizable module of the processor for both Monitoring camera node and the controller unit which we implemented easily in the FPGA to check the performance of our processor. The simulated output of each block is described in the form of test bench (ns) simulation. Known ID give the result of 'no_action' port high and 'suspicious_node' port low and vice versa.

CHAPTER 4

VLSI DESIGN AND HARDWARE IMPLEMENTATION OF RFID ANTI-COLLISION ALGORITHM

Chapter 4: VLSI Design and Hardware Implementation of RFID Anti-collision Algorithm

4.1 Introduction:

In the Radio Frequency identification system, the communication between the tag and the reader is established using radio frequency wave. The electronic passive tags are energized by the electromagnetic waves emitted by the RFID reader. The tag scatters back the wave energy to the reader and thus transmit the data. But when more than one tag try to respond to the same reader at a time, the tag collision problem takes place [74- 77]. The reader cannot identify the tag IDs. Hence, several anti-collision schemes have been developed, like binary tree search, ABS, Query tree, etc [78- 89].

RFID tag anti-collision protocols can be grouped into two broad categories like Aloha based protocols and tree-based protocols. The different types of Aloha based protocols are as follows: ALOHA, Slotted ALOHA, Frame Slotted ALOHA (FSA) and Dynamic Frame Slotted ALOHA (DFSA). Whereas the well known tree-based protocols are as follows: Binary tree protocol, Adaptive Binary Splitting Tree (ABS), Query tree protocol, the 4-array Query tree and Improved Query tree protocol [80]. Tag selects their transmission time randomly in ALOHA but in Slotted Aloha based protocol, tags can try to transmit at the beginning of a time slot. The ABS algorithm continuously split the group of colliding tags in to subgroups until the reader detects all the tags within its range.

Query Tree Algorithm (QTA) is another type of binary anti-collision algorithm and has an advantage in easy implementation due to its operating modes. QTA sets the random query bits and identifies tag by iterating the round of query. It reduces the number of iteration but yet causes the idle cycles that can results unnecessary slots and delay [80- 89]. All these anti-collision algorithms have their own merits and demerits. Bagnato et.al has presented a performance analysis of these anti-collision algorithms in their paper in 2009 [80]. The anti-collision protocols have been devised and applied with the levels of performance in respect of the number of tags that can be detected at a time and the time required detecting them

successfully. So, the anti-collision performance and the cost to produce the circuit is an important consideration in many applications.

In their paper, author J.Myung & Lee analyzed the tree based anti-collision algorithm and it uses the time domain method in the developed circuit [82, 83]. The VLSI system design implementation is essential to improve the functionality and the cost of the anti-collision circuit. To design a power efficient protocol, we must consider the circuit level power optimization of the tag and reader. Since the anti-collision circuit constitutes the most important part of the base-band processing unit on a tag and the tag has limited power, it is more important for tag. Without hardware realization, evaluation of power consumption and its optimization at the circuit level cannot be performed accurately [90]. So, we get motivation of hardware level implementation of anti-collision algorithms for RFID tag and reader circuitry.

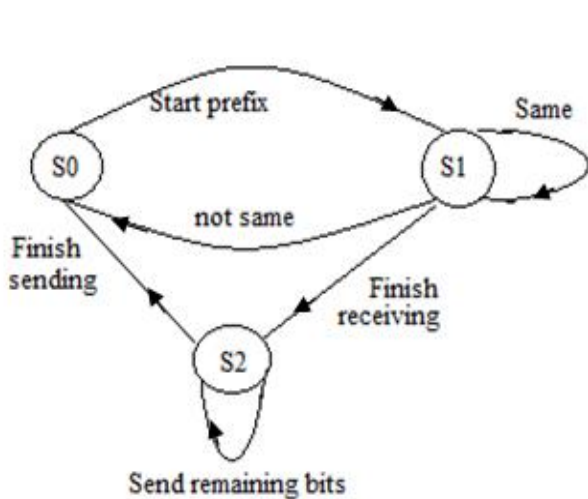
In this research work, a Power efficient anti-collision algorithm for RFID technology with added priority and security features has been implemented using VHDL code and simulated using Xilinx ISE14.3 simulation tool up to RTL schematic level. The hardware level implementation of simplified EPC Gen protocol is also presented in this work.

4.2 Literature Review:

Radio Frequency Identification (RFID) is a contactless, low power wireless technology. It has been developed for many years and getting its new applications in many fields. The RFID system consists of three main components: RFID reader, RFID Tag and Middleware [74- 77]. In RFID system, all the tags of a RFID system communicate with reader with the same frequency. There is always a possibility of data collision at the reader end when multiple tags try to send their identity data to reader at the same time instant. This type of collision is called Tag collision. Many anti-collision algorithms have been developed to overcome this anti-collision problem [78- 89]. The reliability and efficiency of an RFID system are highly decided by its efficiency of anti-collision algorithm. The efficiency of any anti-collision algorithm is decided by following factors: lower time slots, simple in calculation, low cost, lower power, and faster reading speed [90- 98].

A Tree based anti-algorithm can be expressed as a B-ary tree ($B \geq 2$), where each leaf node of the tree is the tags identified by a reader in an RFID system. The tree based algorithms are the deterministic algorithm which can predict the process of the identification. These algorithms operate by sequentially traversing the tree from top to bottom, where each node of the tree has an additional component of a tag's information. Drawbacks of these algorithms are the number of iterations involved before the reader can identify any specific tag and the complexities of circuits required in the tag itself to respond to readers. In order to be identified all tags in a tree structure, B should be in the form of $2^n (n \geq 1)$. Therefore, this cannot be used when the value of B is 3, since the tag which cannot be identified is produced. Also, an increase in the value of B results in a decrease in the number of collision cycles, while the number of idle cycles gradually increases [80, 91].

In the *Query Tree search* protocol, the reader transmits a prefix in each query round and tags simply respond with their IDs if the prefix is matched with their IDs. If there is a collision, the reader neglects the round and transmits one-bit-longer prefix then. The identification efficiency of this protocol is low for dense the tag population or sparse distribution of tag ID address [85, 86].



S0: Standby mode; S1: Receiving mode;
S2: Sending mode

Fig. 4.1 State transition diagram for Query tree protocol

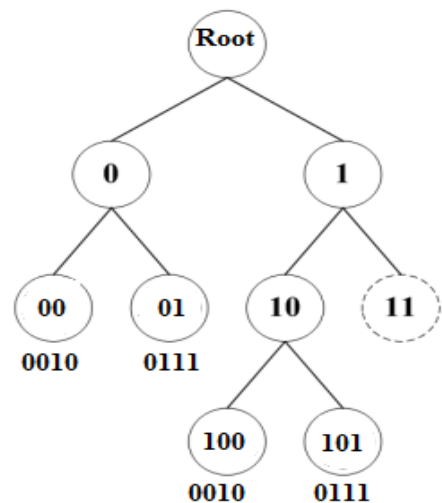


Fig. 4.2 Query Search Tree

The Improved Query Tree Algorithm is proposed to remove the idle cycles effectively. In this algorithm, if a collision occurs, the IQTA uses the Bits Change Method to eliminate the idle cycles by detecting only the tag IDs that actually exist. Hence, it can

quickly identify all tags by reducing the number of query-responses and decreasing collision cycles [87, 92].

Choi et al. proposed a RN16- based QTA (RN16QTA) for RFID tag anti-collision [93]. RN16QTA treat random number RN16 as the temporary ID (TID) of tags, and then basic QTA is applied to identify this TID. After the successful identification, the Reader sent an ACK signal to the tag. The tag having this RN16 now sends its whole EPC to the Reader after receiving the acknowledgement. RN16QTA successfully reduces the time delay for tag identification. However, the short length of RN16 is not sufficient to avoid tag collision effectively in real environment. It is also not useful for a large number of tags. ERN16QTA solves the problems regarding RN16QTA. Yang et.al. proposed this effective RN16QTA by XOR-ing RN16 and every 16-bit tuple of EPC as multiple TIDs [94]. This algorithm solves the tag collision caused by the short length of RN16. ERN16QTA also returns the lesser responded bits than RN16QTA. It is effective for any number of tags in real environment.

Adaptive Binary Splitting Tree algorithm splits a group of colliding tags into two subgroups until the reader receives signals of tags without collision. A time frame is defined as the time elapsed for identifying all the tags within the reader's transmission range. The reader can adaptively decide the length of the data frame, beginning and terminating the frame. The frame consists of time slots which are certain time periods. ABS schedules tag's transmission in a consecutive communications between a reader and a tag. The tag has three states: wait state, active state and sleep state. The tag maintains values of a progressing slot number and allocated a slot number. This algorithm is very fast compared to other anti-collision algorithms [82, 83].

Considering several standards, which developed for RFID, Electronic Product Code (EPC) standard has better compatibility and more recognized in the market. It is developed by Auto ID lab and sponsored by MIT and EPC Global Inc. Real-time RFID-related data can be shared over the Internet with this standard [95, 96]. Each RFID-tagged item can be tracked and traced via the complete descriptive information shared under the umbrella of EPC global. A number of EPC RFID- based systems have been proposed in the literatures, but the integration of mobile devices and EPC-RFID-based system can provide a more user-friendly and self-validated product authentication solution to the customer as well as a service provider. As such integration is in an interesting stage of development, more attention is paid

by researchers to discuss the issues posed by developing and deploying such systems [95-98].

During 2004, under the leadership of EPC global, a growing number of users and vendors are developed and agreed upon the final specification of the EPC Gen-2 protocol and tags. At the end of the year, the work started on developing commercial products that met the EPC Generation-2 requirements [1.96-1.108]. As defined in EPC Gen-2, the probability that any two or more tags have the same sequence of RN16, for 10,000 tags, should be less than 0.1%. If the population of tags which remains to be identified in the inventory round can be estimated, the protocol can also adjust the Q value to achieve better performance. DFSAV-I and DFSAV-II methods proposed by Vogt (Vogt, 2002)[109], DFSAC-I and DFSAC-II methods proposed by Cha et al. (Cha and Kim, 2005)[1.110] etc. are well known methods to estimate the tag population, according to the number of idle, success and collision slots achieved in a frame. The accurate tag estimation method is proposed by Web. Tzu. Chen (2006) [111]. Among all these methods, DFSAV-II method has higher accuracy which performs population estimation based on Cheby-shev's inequality.

In the Auto-ID Labs White Paper WP-HARDWARE-047, March 2009 [112] Bo Li, Yuqing Yang et.al has focused on the anti-collision issues in EPC Gen2 Protocol, which is specified for passive UHF RFID system, and module available in the market is entirely implemented on the DSP. It is developed on the basis of EPC specifications and EPC Class 0 and Class 1 protocols. It is designed to accommodate EPC Gen 2 protocol also by allowing adding some variables in function calls. This module consists of DSP, is capable to provide functions for generating EPC Class 1 Gen 1 commands and interpreting the tag's reply. This module can communicate with EPC 64 bit and 96 bit tag code structure and has the ability of handling anti-collision protocols.

But, to achieve more powerful, efficient, and flexible structure, Software defined hardware came into the scenario. With the minimization of hardware requirements for different protocols and software implementation of RFID modules, SDLR achieves superior performance over hardware cost and software flexibility. Here, analog to digital and digital to analog conversion, functions like modulation, demodulation, and channel coding and other needful processing tasks are performed in software. This design allows user to make changes to the code and it can be upgraded in field lowering the costs also.

From the literature review, it is revealed that many data security schemes are proposed, implemented, and verified by many researchers several times [113]. At the earlier stage, there were three primary approaches,

- i. Physical block approach,
- ii. Rewritable tag approach and
- iii. Smart tag approach.

In physical tag approach, kill commands are used in EPC protocol, which are protected by a PIN and a Faraday cage enclosure was used to prevent the side channel attack or power attack by hackers. But these measures are not so effective and create problem to identify the tag when it is required. Rewritable tag approach for security purpose is better than a physical approach but needs refreshing the memory each time to store new ID. This approach requires a significantly high running cost and made it unsuitable for RFID applications. The Smart Tag approach is one step advanced than those two approaches. Here, cryptographic functions like Hash function, public key or common key is used to protect data, and a ROM is embedded within each tag. K-step ID matching using Hash function is also implemented and verified for security purpose [114- 118].

Among those all schemes, cost of tag varies, but is quite high compared to normal tags. This high cost of tag not in favor of low cost RFID systems.

Different crypto algorithms like,

- i. Advanced Encryption Standards (AES) algorithm,
- ii. DES Encryption algorithm,
- iii. Elliptic curve cryptography (ECC) algorithm, etc. is implemented and synthesized in 0.25/0.35 μm CMOS technology.

Hardware implementation of the Crypto processors based on these crypto algorithms provide an overview on the performance of these processors in terms of power consumption, silicon area, etc. as shown in Table 4.1.

Table 4.1: Performance of the Crypto processor based on different crypto algorithms

Crypto algorithm	Frequency	Power consumption	Silicon Area	Time delay	Gate count	CMOS techn.
AES algorithm[26]	10 MHz	~12 mW (8 bit)	~1.18mm ²	1000 clk-cycles for 128 bit	3868- 4400	0.25μm
DES algorithm[27]	500 kHz	~5 mW (8 bit)	~0.98mm ²			0.25μm
ECC algorithm[24]	18 MHz	95mW (173bit)	1.31mm ²	7.56 ms	6300- 7800	0.25μm
Hash function	10 MHz				545 per PUF	0.2 μm
Tiny Encryption Algorithm	50 MHz		0.21 mm ²	32-bit TEA		0.35μm

Developing novel anti-collision algorithms for RFID technology and integrating it with advanced VLSI Implementation is the foundation of this research work. But, data transmission or exchange of data is another important task of wireless communication. Sometimes hackers may hack the data and may alter it or steal information. The consequences may be unwanted if and when the data is pirated or stolen. So, to provide security to data during transmission is another challenge for the designers. Proliferation of RFID tags in a large level security has raised many privacy and security concerns. To prevent unauthorized access to personal information stored in a tag, password protection is provided by EPC Gen RFID specification. So, our motivation of this research work is to add security features in the anti-collision algorithm. VLSI implementation of EPC Gen 2 protocol, its password protection scheme, and realization of this protocol on FPGA board and performance evaluation of the developed processor is described in this work.

4.3 Power efficient anti-collision algorithm for RFID technology with added data security feature and its Implementation in VHDL

In the field of RFID technology, a power efficient tag anti-collision protocol plays important role in the entire system based on this technology. The Query Tree scheme is one of the most important anti-collision protocols for RFID technology. Researchers have developed different Query algorithms with improved features each time, reducing the number of query iterations and idle slots. The EPC Gen protocol uses this anti-collision algorithm which is popularly known and globally accepted for its secured data transmission feature but having a huge load of data itself. Low power design and implementation of the anti-collision protocol is another challenging area for cost effective RFID system. In our research work, we have implemented the protocol as low power single chip solution. Furthermore, we have included a data security scheme in this protocol for secured data transmission. We have also implemented other anti-collision protocols with different bit size and a comparative study of performance evaluation has been provided.

4.3.1 Design and implementation of Query tree protocol:

The Query Tree search anti-collision algorithm for RFID technology is well known algorithm and much more efficient to draw the researchers' attention due its property of high anti-collision ability and easy implementation. We have found many articles proposing more improved Query Tree protocol in different aspects [84- 88, 92- 94]. In this work, this protocol has been implemented in hardware to provide low cost, single chip solution with very little silicon area. Low power, high speed architecture is another feature of this proposed system. To provide security to the tag ID and data stored within the tag is the responsibility of the designer in recent days. The EPC Gen2 protocol has own password and scheme to hide information, but has overhead of a large frame size [95- 99]. In this regard, QTA is quite simple algorithm and has no such overhead. We include data security with this protocol; it will be the better choice for the designer with less hardware and comparatively less complex circuitry. It is not only power efficient but also cost effective solution in the field of RFID technology. This proposed protocol has also the added feature of priority.

Table 4.2. The Operating Process of QTA

Round	Query	Tag 1 (0010)	Tag 2 (0111)	Tag 3 (1000)	Tag 4 (1010)	Remarks
1	0	0010	0111	No response	No response	Collision
2	1	No response	No response	1000	1010	Collision
3	00	0010	No response.....			Tag 1 detected
4	01	No response	0111	No response	No response	Tag 2 detected
5	10	No response	No response	1000	1010	Collision
6	11				No response
7	100	No response.....	1000		No response	Tag 3 detected
9	101	No response.....			1010	Tag 4 detected

The operating process of QTA has been described in Table 4.2. The Reader sends the prefix of Query and tag matches its ID with the prefix. If it matches with the prefix, tag responds. Reader takes it as collision round if it receives more than one response and again send prefix of another combination. Once a tag is detected, it quits.

4.3.2 Operational flow chart and block diagram for the Query tree protocol:

This section describes the operational details for the Tag and Reader respectively. If the tag is detected by the reader without collision, the reader will send an acknowledgement, 'ACK'. When the tag receives 'ACK', it transmits the important data or information stored within it. For security of data, this data is stored as an encrypted form. This data encryption is performed using a secret key and PCA rules. The Reader must know this specific secret code and PCA rules to decrypt the data. This introduces data security to the proposed protocol. In RFID technology, data Security is a critical issue to prevent any unauthorized access to important or personal data or information stored in the RFID tag. PCA based data security for RFID technology is very much suitable for VLSI implementation which in turn results low power, single chip solution. Processor for reader and tag has been designed and implemented using the algorithm and operating flow chart. The reader consists of a random number generator like EPC Gen2 protocol. According to the response of tags, the prefix changes and the final information store within the tag is encrypted using the programmable cellular automata rules and secret keys.

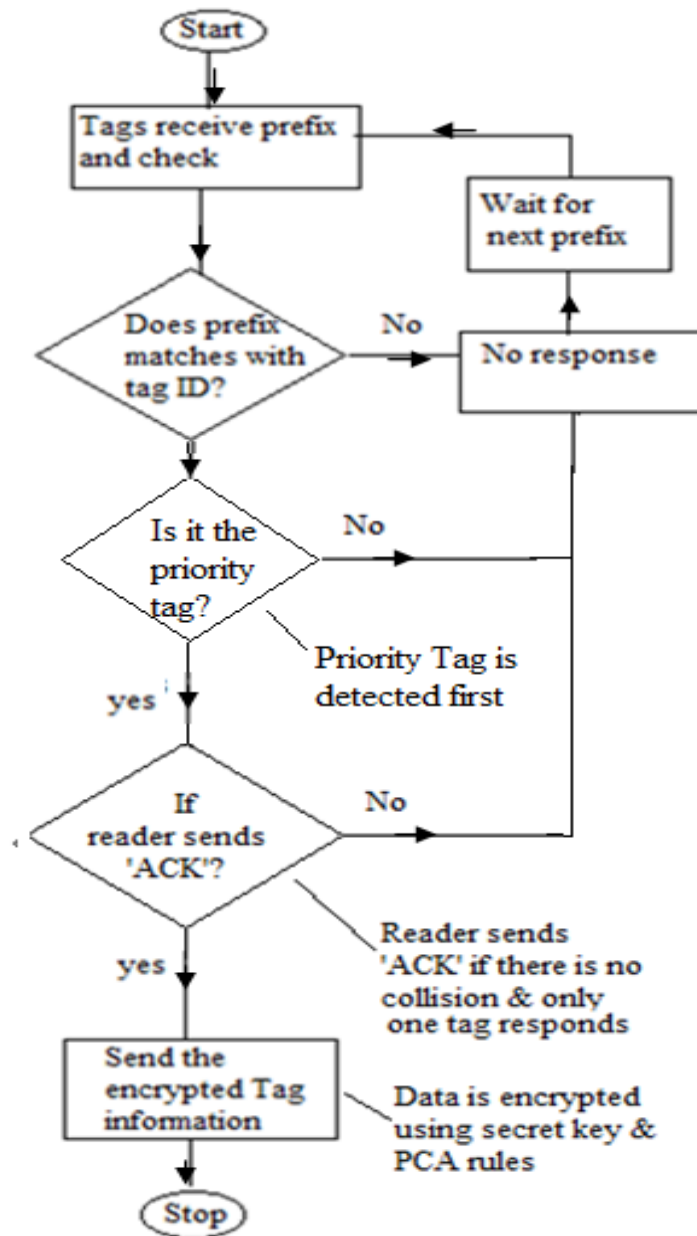


Fig. 4.3 Operational Flow chart diagram for Tag

Fig. 4.3 describes the operational flow chart for the Tag operation.

- Tags receive prefix and check whether the prefix matches with the tag ID
- If matches then it checks if it is the priority tag or not and thus the priority tag is detected first
- After detection the information is transmitted in encrypted form using secret key and PCA rules.

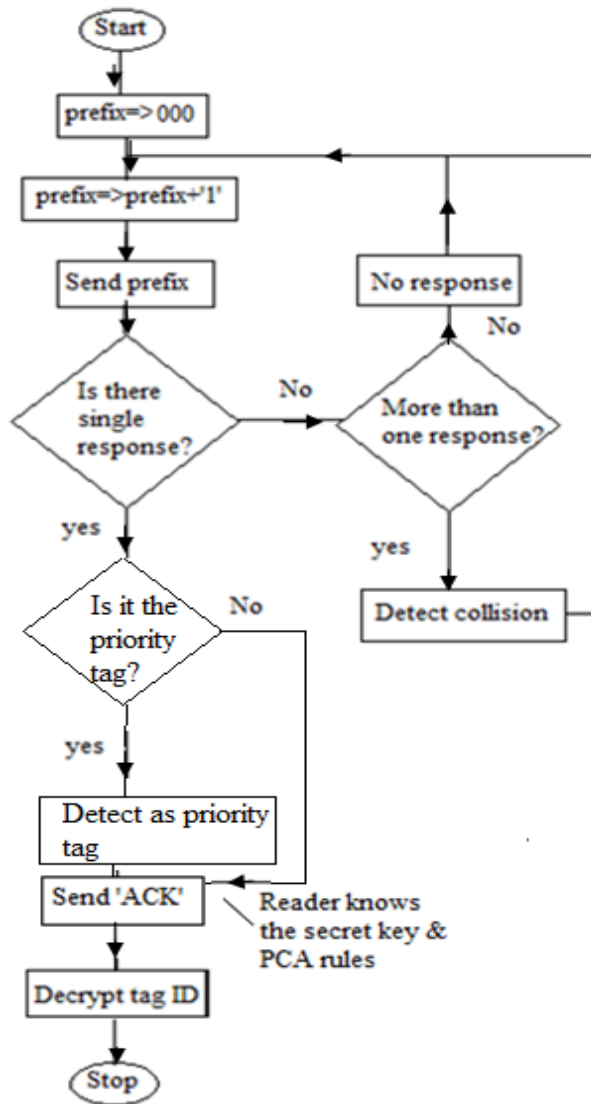


Fig. 4.4 Operational Flow chart diagram for Reader

Fig. 4.4 describes the operational flow chart for the Reader operation.

- Select prefix “000” first and then send ‘prefix = prefix + 1’ according to the response received from tag end
- Priority tag is detected first
- After detection reader decrypt the information using secret key and PCA rules.

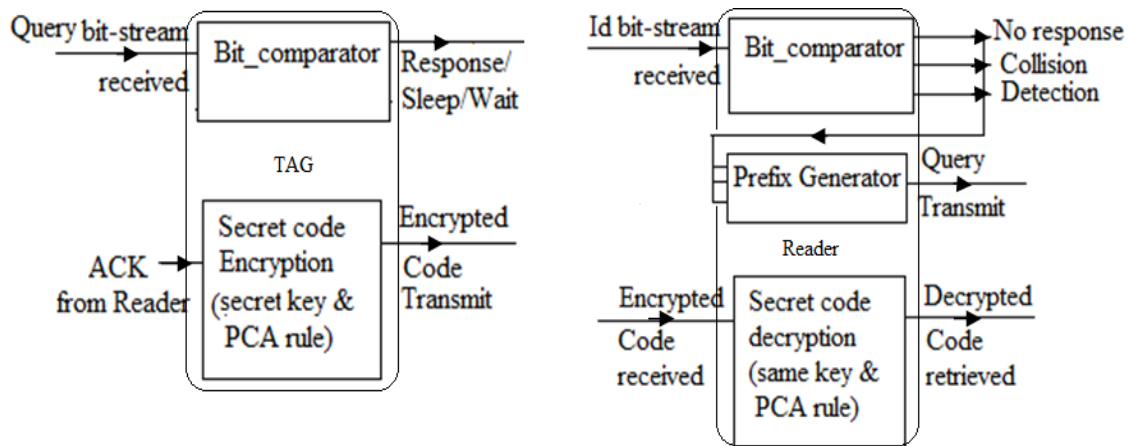


Fig. 4.5 Functional Block Diagrams of tag and reader

Fig. 4.5 shows the functional block diagrams (Tag and Reader) for the proposed algorithm. The tag is consists of two major operational blocks, Bit comparator and ID generator block. When the tag receives the prefix, the comparator block compares with the tag id and responds accordingly. Using the secret key and PCA rules the ID generator generates the encrypted data which is transmitted when the tag receives acknowledgement signal from reader end.

The reader processor consists of bit comparator, prefix generator and a data read module. The prefix generator generates the prefix and sends it. The Reader receives response/signal from tag ends and comparator detects whether it is a collision, detection or no response and change prefix bit accordingly. After detection, the data read module retrieve the data using the same secret key and PCA rules.

4.3.3 Hardware Implementation Results:

The algorithm is verified with suitable test bench simulations using Xilinx ISE 14.3 simulator. High syntax hardware description language code VHDL is used for design purpose and high performance FPGA board is used for implementation [2- 5].

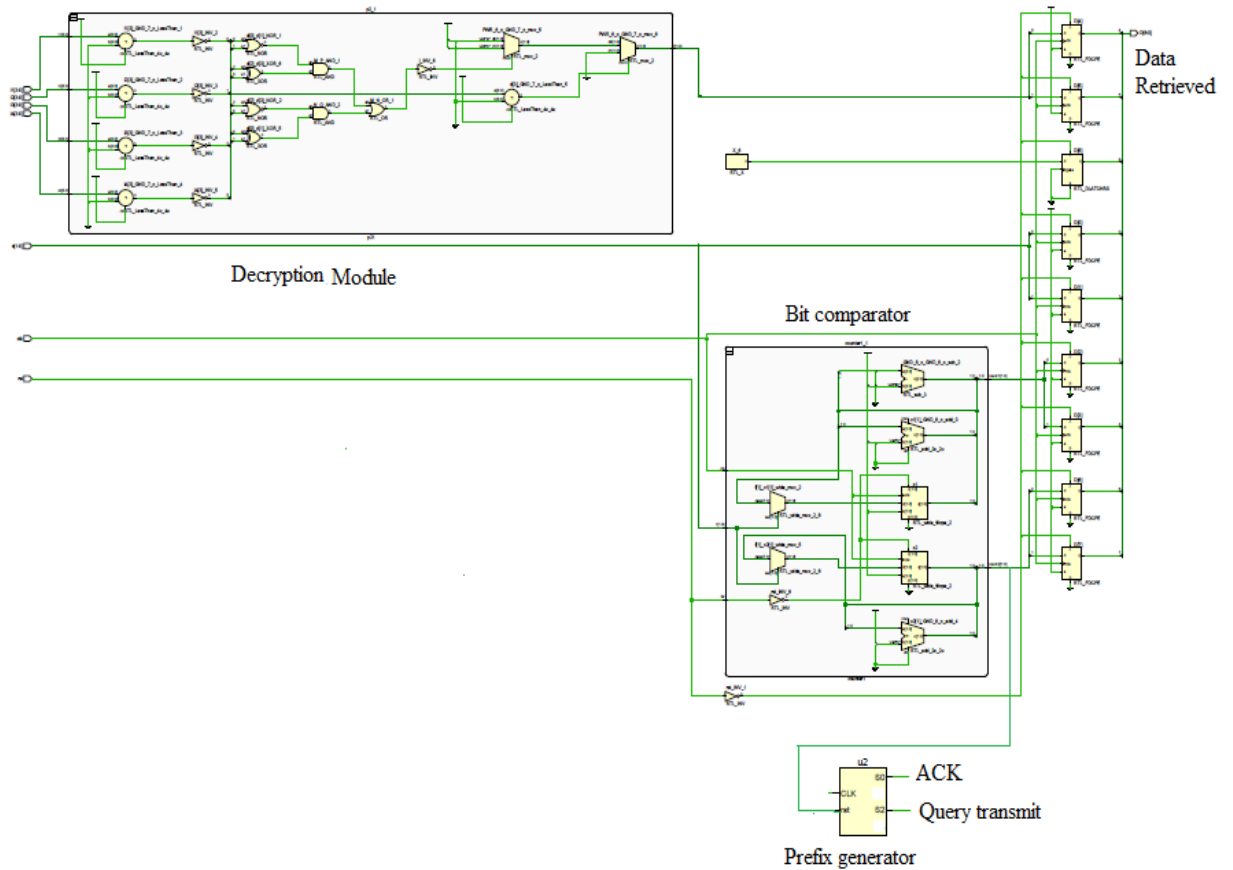


Fig. 4.6 RTL Diagram (reader) for proposed algorithm

Fig. 4.6 shows the RTL diagram of the Reader. The processor consists of three major blocks as shown in Fig 4.5, named as Decryption module, Bit comparator module and prefix generator module. The Decryption module is provided with the same encryption key and PCA rules as the encryption module of the tag has.

A comparative study of hardware requirement of different anti-collision algorithm on VLSI platform is described in Table 4.3.

Table 4.3: Comparative study with different anti-collision algorithms [ID of 8 bit]

Parameters	Binary Tree algorithm		ABS Algorithm Reader + Tag Processor		Proposed LUT based anti collision algorithm		Proposed Query tree algorithm	
	with single priority	without priority	with single priority	without priority	with single priority	without priority	with single priority	without priority
No. of slices of F/F	8	10	20	24	4	6	8	12
No. of 4-input LUTs	13	20	14	22	20	28	16	20
No. of IOs	34	19	42	40	32	18	22	16
Registers	8	10	22	26	4	6	8	12
Comparators	1	1	6	6	4	4	4	4
Xor gates	8	1	8	2	4	1	4	1
Delay('ns')	7.218	6.541	4.920	4.700	6.785	6.209	6.012	5.970
Dynamic Power dissipation	25 mw	22 mw	51 mw	48.4 mw	20.8 mw	19.97 mw	31.6 mw	30.45 mw

Hardware implementation of the anti-collision protocol with priority feature and added data security is the most significant work in the RFID research area. Low power solution with high speed processor and simple circuitry is the outcome of this work. The comparative study with other implemented protocols clarifies a brief overview of hardware requirements, power consumption, and circuit delay. The Query tree is one of the best anti-collision algorithms and also used in high security EPC Gen2 protocol. The proposed PCA rule based security included in the query tree algorithm enhances the data security significantly. Integrated technology with optimized silicon area and low power dissipation improves the performance of the reader and tag. In this case, the proposed design is

reconfigurable and technology independent, which makes it suitable for easy implementation and reconfigure design matrices.

4.4 EPC Gen protocol and its Implementation in VHDL:

For the UHF RFID system, the Electronic Product Code (EPC) Global Inc. has proposed the EPC Class 1 Gen1 and EPC Class 1 Gen2 protocols, and it is ratified as International standard anti-collision protocol [100- 103].

4.4.1 EPC Gen-2 Protocol:

The ‘Electronic Product Code’ (EPC) numbering system is considered as to enhance and finally replace traditional bar codes. EPC assigns a globally unique number to every object equipped with a radio frequency identification chip (RFID tag). This EPC is serving as an identifier for the physical object carrying the tag, which can be detected, identified, and tracked by an interrogator [98- 103]. Moving from the barcode system to RFID tags containing an EPC was motivated in order to save costs, high speed detection, and simplicity of operation if security is not concerned. The implementation of a global system to store and access information about countless products at least cost motivated the enhanced future of marketing and business area. The EPC of an RFID tag has to be regarded as highly sensitive information be it in private or in business environments where product and raw material flows constitute valuable market information.

EPC Gen-2 protocol is the advanced version of the EPC Gen-1 protocol and global standard. According to this protocol, at first Reader uses a command ‘SELECT’ and selects some of the tags among the tag population; Then the Reader transmits a command ‘QUERY’ - containing the Q-parameter to specify the frame size (equal to $L=2^Q-1$). According to the Q-algorithm; after receiving the query command, each selected tag chooses a random number (RN) within the range (0 to 2^Q-1) and store within its memory as its Slot Number (SN). The tag which has chosen its slot number ‘zero’ should respond to the reader and transmits a 16 bit number ‘RN16’. Upon receiving the ‘RN16’ from the responding tag, Reader transmits an acknowledgement ‘ACK’ containing the same ‘RN16’. The tag receives the ‘ACK’ and compares ‘RN16’, if it matches with its own ‘RN16, it broadcasts the information or backscatter its EPC and goes to the sleep mode and do not respond again. The Reader then

issues 'QUERYREP' and 'QUERYADJUST' command to initiate another slot in order to identify the remaining tags to be detected within the readers' range. Each tag should subtract '1' from its slot number or adjust the 'Q' value and pick a new slot number [98- 106].

There are three possible types of slots; empty slot, Collided slot, and the successful slot; tags are asked to choose slot number SN within the range $0 \leq SN \leq (2^2-1)$. But, if no tag is chosen, SN = 0, then the slot will be an empty and no tag will reply. When more than one tag choose SN = 0, more than one tag to respond and it results a collided slot. The Reader modifies its Q value and asks the tags to choose new SN. Successful slot, when there is only one tag to respond and exchange information with SN = 0 and generates the 16 bit number RN16 and transmit [98- 104].

RFID tags will respond only to the Reader of type with anti-collision protocol, without disturbing the overall communication network. Upon receiving power from the EM wave transmitted by the reader, the tags power up and waits for commands from the reader. Tags update their states and reply according to the commands received. These logical operations are implemented in the tag module. Tag module satisfies the backscattering model in physical layer. The backscattering power from the tag is a function of incident signal power and backscatter ratio, is shown in equation 1[4.5].

$$P_{bs} = P_R * G * e * \eta \quad (1)$$

Where 'G' is the antenna gain of the tag, 'e' is the polarization efficiency; 'η' is the backscatter ratio, which is a function of the modulation index (m) and type of modulation. All tag antennas are considered to be isotropic in nature.

4.4.2 Key points of EPC Gen-2 tags:

- Tags must be able to communicate in the frequency between 860 MHz to 960 MHz
- Tags must be able to understand different modulation schemes such as: DSB-ASK, SSB-ASK and PR-ASK. The Reader will determine which modulation scheme to be used.
- Tags must be able to transmit at several speeds or data rates. The Reader will determine what speed to use.
- Gen-2 tags support EPC's up to 256 bits long, whereas Gen-1 tags supports EPC code up to 96 bits long.

- Gen-2 includes a method to support ‘dense-interrogator channelized signaling’ which is an attempt to reduce interference between EPC readers.
- Gen-2 tags have the ability to generate random numbers. The Reader will inform the tags the range in which it should generate a random number by issuing a query command and a Q value. The range will be 0 to (2^Q-1) . If it often gets back no response to its queries, it will automatically reduce the Q value. If it gets more than one tag responding, it will increase the Q value, thereby increasing the range of numbers that can be generated by the tags [98-106].

4.4.3 Q-Algorithm:

The global standard EPC Gen2 protocol uses the Q-algorithm which represents the important transmission control strategy in the communication system. The value of Q in Q algorithm changes according to the collided slot and empty slot to achieve the successful slot, i.e. improves the success rate of an inventory round of the mentioned protocol to detect a tag within the range.

Q-algorithm:

Step1. Select $Q = 4.0$

Step2. Start inventory round

Step3. If tag response = ‘0’ then

$$Q = Q - 1; [Q = Q \text{ if } Q = '0']$$

Else go to Step5

Step4. Go to Step2

Step5. If tag response > ‘1’ then

$$Q = Q + 1; [Q = Q \text{ if } Q = '15']$$

Else go to Step7

Step6. Go to Step2

Step7. If tag response = ‘1’ then

Q remains unchanged

The tag is detected successfully

Step8. Go to Step2 for next inventory round

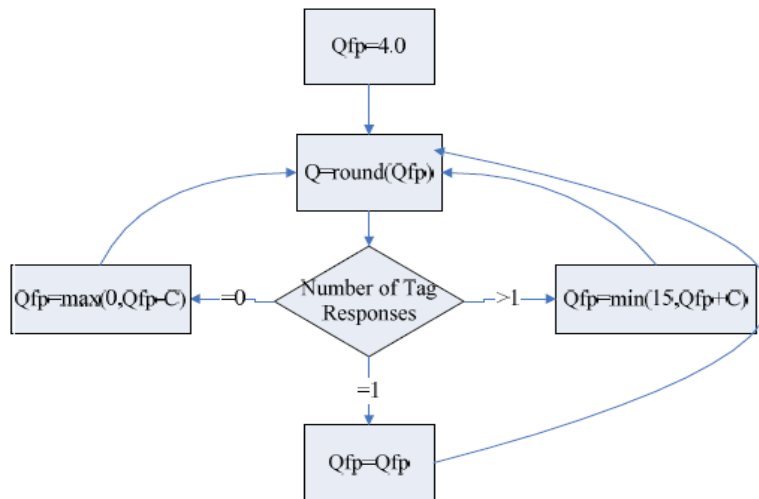


Fig. 4.7 Q-Algorithm

The Q-algorithm started with a standard value of $Q = 4$; it is chosen as a floating value rather than fixed at 4.

- The Reader considers the current Q value and transmits.
- If there is zero response, it is an empty slot of the inventory round and Q sets its value as $Q = Q - 1$ (value of Q remains unchanged if $Q = 0$);
- If more than one tag responds, it results collision and Q is modified its value as $Q = Q + 1$ (value of Q remains unchanged if $Q = 15$).
- Finally, when only one tag responds to the Reader's query, for the successful slot, the tag is detected successfully; Q remains unchanged and next inventory round started.

The Reader transmits different commands for each case to the tags to instruct them for the next operation, according to the algorithm for EPC Gen2 protocol, like 'Query', 'Queryrep' and 'Queryadjust' [100- 104].

4.4.4 Components of EPC Gen module:

A Designer can define four steps to develop the EPC module, like code (EPC) generation, authenticity check, data security provider, and Information service Provider.

i. EPC generation:

The EPC generation module is designed to provide a unique numbering system to the individual unit of products. As RFID has a growing market demand, designer focus on the interchangeability and compatibility to encourage the interoperability of product

identification. In 2006, Class1 Gen2 has been approved as ISO 18000, being a part of ISO/IEC 18000-6 standard. RFID tags-readers compliant to such standard are compatible across companies and industries. Such tag can store important information like manufacturer's code, product type, unique serial number, etc. More commonly used EPC tags in industries are 96 bit since their data capacity is sufficient for almost all applications. Using this combination, about 80,000 trillion unique numbers can be generated, and 268 million companies can register with the EPC, whereas each company can be provided with 68 billion unique serial numbers for each product [99- 103].

Header 8 bits	Manufacturer 28 bits	Product Type 24 bits	Unique serial no. of product 36 bits
--------------------------------	---------------------------------------	---------------------------------------	---

Fig. 4.8 A Data structure of 96 bit EPC Class1 Gen2 tag

A Data structure of 96 bit EPC Class1 Gen2 tag is shown in Fig. 4.8, in which four basic data elements are a header, a code for identification of the manufacturer, a code to represent product type or object class and the unique serial number. This information is generated electronically using a number generating system in such a way that when once the manufacturer assigns and generates the code, the entire logistics network navigates by the product can be visualized by recording all the transactions in a supply chain management.

ii. Product Authenticity Check:

Electronic Product Code or EPC Global class-I Generation-I and Generation-II are popular and globally accepted standard specification which enables the use of password protection for accessing the data stored in the memory of an RFID tag. The use of password gives one of the ultimate securities for the RFID system. But usually in most of the applications, EPC code data are not encrypted, rather covered by more pseudo-random number or data to protect the tag from malicious access. A hybrid cryptographic approach is used in some important areas to encrypt the tag information as it is a costly process. Cover coding of password and kill password are very common approach for EPC data security, but for authenticity check, the encrypted RFID tag has been generated and attached with the product so that only authenticated reader can access the information stored within the tag. The encrypted data is decrypted and the stored data is normalized according to a standard format for globalized identification system. Once the product is within the tracking chain, the

information is captured and registered into the local database EPCIS, the EPC information server. The EPCIS embeds the information about the product and customer can obtain the EPC of a scanned product remotely from the EPCIS in order to check the authenticity of the product. Any type of RFID device can be used to display on a real time basis, not only the product details but location record like where the item was produced and when and where the item was distributed, the route through the item had moved, etc. It is very useful to track an item efficiently and detect fake case or missing case immediately by customer and service provider.

iii. Introduction of Cryptography in EPC:

EPC Gen2 tags are commonly used for item level trace and track, product authentication, it lacks data security. However, in few important cases, to cope with data security threats, a cryptographic approach was adopted to protect information stored within tags.

- a) Jigsaw encoding scheme—this scheme was first adopted in EPC transforming the 96 bit code into a pseudo EPC which is difficult to decrypt.
- b) Hash function based scheme—it is used to lock the pseudo EPC for integrity verification, i.e. to detect whether the tag is authenticated or cloned by hackers. The hash function consists of 32 bit cyclic redundancy code to form a ‘key’ and used as the PIN value of the RFID tag. To decrypt the pseudo EPC, an authentic reader is required, which should have the key to unlock the hash function. These locking and unlocking processes ensure the integrity of the product information.

iv. Information service Provider:

The EPC is registered in the local EPCIS server. To access the information stored in the EPC-Global network about a given EPC, one need to locate the EPCIS server first and then send a query to the Object Naming Service (ONS) and request access to the EPC. ONS is a sub-system of the Domain Name System. This is to fulfill the purpose to encode the EPC into a syntactically correct domain name to use the existing DNS infrastructure in the world of internet. It returns with the location of EPCIS where the item details are available.

4.4.5. Design & Implementation of EPC GEN-2 Protocol:

This chapter presents the implementation of the EPC Gen-2 protocol in VHDL. EPC Gen-2 is a standard to resolve the collision of tags occurred in the UHF RFID. The design is targeting the Xilinx FPGA device, this leads to a real time environment verification of the system. VLSI Design of protocol is performed to achieve high speed, minimum hardware, and enhanced system efficiency with the secured data transfer. It has high level syntax and supports extensive optimizations. The hardware system development using VHDL gains satisfactory results and provides significant reference to FPGA synthesis in structural models. The key factor that influences the system performance is exposed. The Numerical evaluation according to the Q-algorithm is verified for its protocol.

Hardware description language VHDL has been used to design the proposed processor and the design have been simulated to check the algorithm using Xilinx 14.3 ISE simulator to get the desired output and to make sure that the sequence of operations is correct. VHDL simulation provides the verification of the hardware organization and operation at the structural level, whether the selected bit widths for internal and external signals are sufficient for achieving a low precision to speed up the system efficiency and to reduce the implementation complexity. The step by step process by the test bench simulation results are described in this article. The test bench timings are in 'ns' range and clock frequency in RF range.

4.4.5.1 Standard Data Frame of EPC tag & proposed data frame:

The format of a standard data frame of EPC tag is described in Fig. 4.9. The standard EPC class 1 Gen II tag data frame contains kill password, access password, EPC (product code), TID (tag ID) and extra data space for the user.

Kill password(4)	Access password	EPC	TID	User memory(optional)
---------------------	--------------------	-----	-----	--------------------------

Fig. 4.9: Standard data frame of tag

EPC is 64 bits in length, including 16 bit PC, 16-bit EPC and CRC-16. Frame size may be up to 496 bits. The Manufacturer can choose the frame size as per the requirement of the product to be coded and the requirement of the security of the product code. Because secured data transmission is the basic importance of RFID system.

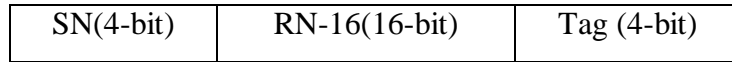


Fig. 4.10: Proposed data frame of tag

In this design, a data frame of 24 bit has been proposed for simplicity as shown in Fig. 4.10. Tags of Gen2 protocol have a random bit generator which generates slot number ‘SN’ and the 15-bit random number ‘RN-16’. For experimental purpose, a format of initial tag ID which will communicate with the reader first containing the SN (slot number, RN16 and tag); if and only if SN='0000' then the RN16 will be generated and transmitted. If SN is not equal to '0' then it receives a command from the reader end and adjusts the SN value.

Slot number generator is a normal counter and number generator (range of $0-2^{Q-1}$). The designer can select the value of 'Q'. In this case, $Q = 4$; So, SN will generate a value within the range of 0-15. If SN = '0' then the random number generator generates a random number within 0-255 and transmits. If the tag receives the same RN16 with ACK signal, it transmits the ID and other necessary information to the reader as the trusted communication has been established, then the tag moves into the sleep mode. According to the design, initially Reader starts an inventory round with $Q = 4$. The modified Q is represented as Q_f . After successful identification of a tag, reader broadcast an ACK signal and decrease its Q_f by '1' automatically up to $Q = '1'$. But, if no tag responds or more than one tag responds, then Q_f increases by '1' automatically until $Q = '15'$.

4.4.5.2 Operational Block Diagram of EPC tag ID generator and reader processor:

The operational block diagram of EPC Reader processor and flow chart of reader operation are described in Fig. 4.11 & Fig. 4.12 respectively.

- a) *Reader operation:* Interrogator or reader, in this protocol manages the tag population using the three basic operations:

- i. *Select*- The process by which an interrogator selects a tag population for inventory and access.
- ii. *Inventory*- The process by which an interrogator identifies a tag. An interrogator begins an inventory round by transmitting a ‘Query’ command with $Q=4$ and ask the tags to activate their slot counter and choose a slot number ‘SN’; $[0 \leq SN \leq 15]$; if any tag choose $SN = 0$ it request the ‘RN16’ and send an acknowledgement signal ‘ACK’ containing same ‘RN16’; otherwise if $SN \neq 0$ then transmit ‘Query rep’ command which ask the tag to reduce SN by ‘1’ and modifies Q decreasing by ‘1’; if more than one tag replies, reader transmit ‘Query adjust’ command and modifies Q increasing by ‘1’; Request the identified tag for information, like PC, EPC, CRC-16 etc.
- iii. *Access*- The process by which an interrogator transacts with the individual tags.

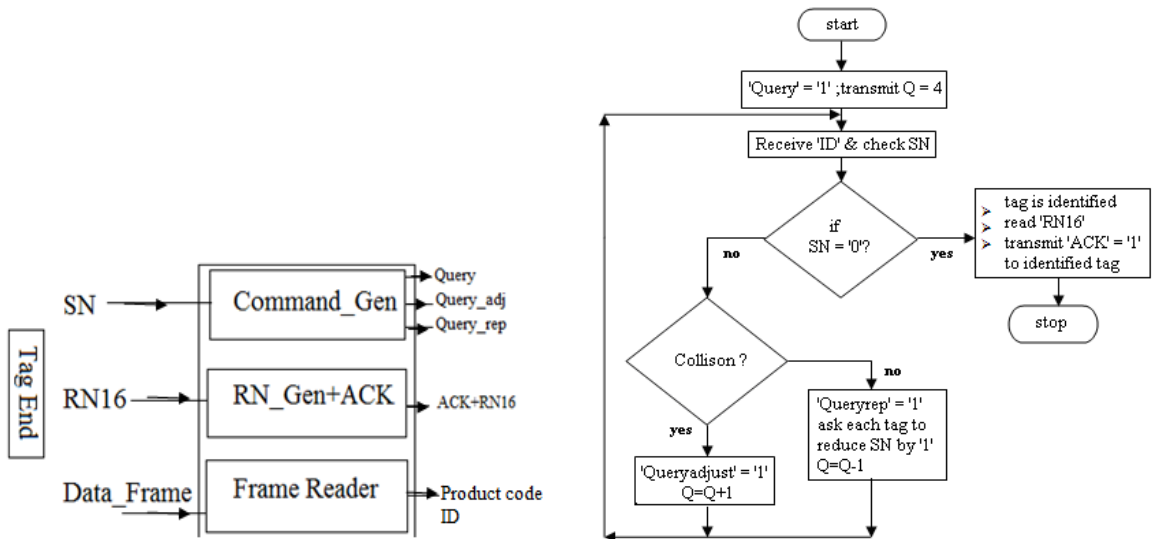


Fig. 4.11: Block diagram of reader processor Fig. 4.12: Flow chart of Reader Operation

b) *Tag Operation:*

- The tag shall implement a Slot counter. Upon receiving a ‘Query’ or ‘Query adjust’ command tag shall preload into its slot counter a value ‘SN’ between 0 and $(2Q-1)$. When $Q=4$, the range is 0-15; a ‘Query’ specifies $Q=4$; a ‘Query adjust’ may modify Q from the prior Q value.
- If a tag selects its slot number $SN=0$, it is in the reply state. Otherwise, it decreases SN by ‘1’;

- The tag shall implement a random number generator. The 16-bit number ‘RN16’ is generated.
- The tag backscatter the number ‘RN16’;
- If the interrogator acknowledges the tag with an ‘ACK’ signal containing same ‘RN16’, the identified tag transmits the important information, i.e. EPC.
- The tag turns itself into sleep mode and ceases to respond.

In Fig. 4.13 & 4.14, the operational block diagram of EPC Tag and flow chart of tag operation are described respectively.

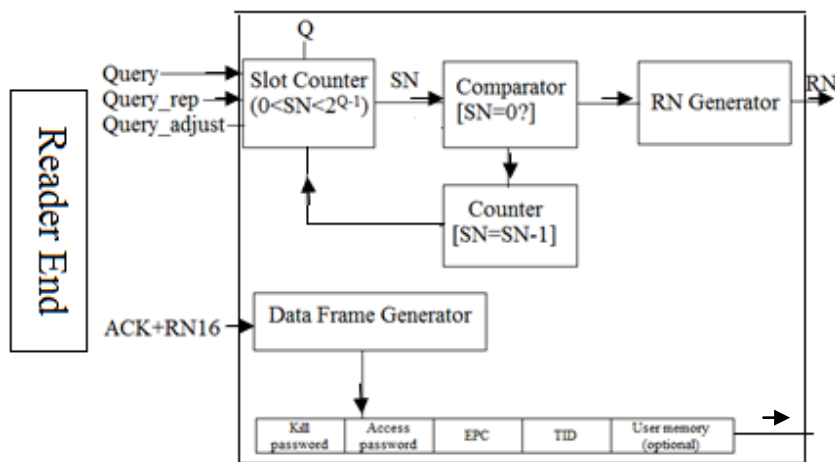


Fig. 4.13: Block diagram of tag

Tags of Gen2 protocol have random bit generator which generates slot number ‘SN’ and the 15-bit random number ‘RN-16’. For experimental purpose, we have designed a format of initial tag ID which will communicate with the reader first containing the SN (slot number, RN16 and tag); if and only if SN=’0’ then the RN16 will be generated and transmitted. After receiving ‘ACK’ the 2-bit tag will be ‘01’ which in turn gives a signal to the tag to transmit the information stored in it.

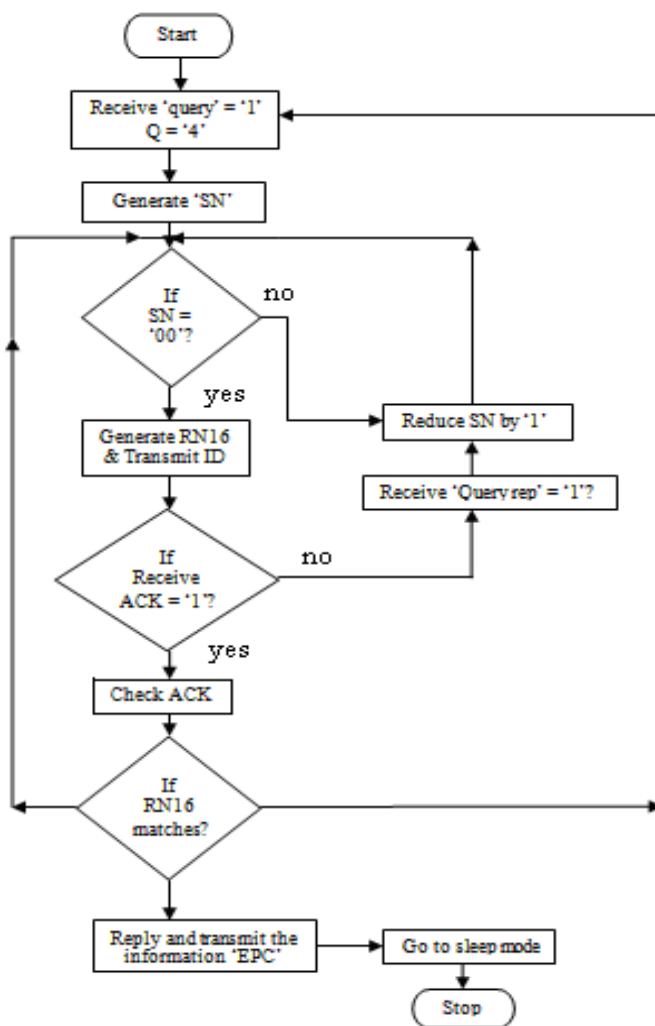


Fig.4.14: Flow chart of Tag operation

4.4.6 Test bench Simulation results:

VHDL coding is used to describe a system at the behavioral level so that the system can be simulated to check the algorithm used and to make sure that the sequence of operations is correct [1- 5]. The HDL simulation provides the verification of the hardware organization and operation at structural level, whether the selected bit widths for internal and external signals are sufficient for achieving a low precision to speed up the system efficiency and reduce the implementation complexity [2- 4]. The step by step process by the test bench simulation results are described here. Xilinx 9.2 ISE simulator is used to get the desired output. The test bench timings are in 'ns' range and clock frequency of RF range. Test bench simulation of designed module is followed by the synthesis process which results the RTL

schematic diagram of the processor along with a study of device utilization, circuit delay, component requirements and static power consumed by the circuit during simulation. We can modify the design as per requirements with no time. The Synthesizable module may be easily implemented on the reconfigurable FPGA development board.

Firstly, consider the Reader module, which transmit commands and query according to the tag response.

a) *Reader module:* According to the design, initially Reader starts an inventory round with $Q = 4$. The modified Q is represented as Q_f . after successful identification of a tag, reader broadcast an ACK signal and decrease its Q_f by '1' automatically up to $Q = '1'$. But, if no tag responds or more than one tag responds, then Q_f increases by '1' automatically until $Q = '15'$. Input 'I' can be observed and its first 4 bit describes the slot number 'SN'. When $SN = '0000'$ the tag is identified by reader and send an ACK signal with $ACK_{16} = '1'$ and ACK_{15-0} as 'RN16' read from I17-2. When tag is identified $Q_f = Q-1=3$ and otherwise $Q_f = Q+1=5$. From Fig.4.12, we can study the output waveform. Input terminals are 'rst', 'clk', I and Q which has fixed value of '4'. We have verified the result for different cases.

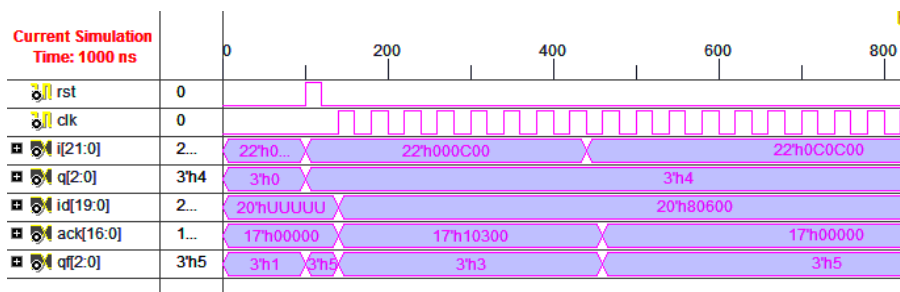


Fig. 4.12: Test bench simulation of reader processor module

b) *Tag Module:* Now, at the Tag end, we will observe the operational performance of our design. As it receives 'Query' signal with $Q = '4'$ it activates its Random bit Generator unit and generate the Slot number 'SN' and the 15 bit number 'RN-16'. Upon receiving a response from the reader end it decides whether it will transmit 'RN-16' or reduce the slot number.

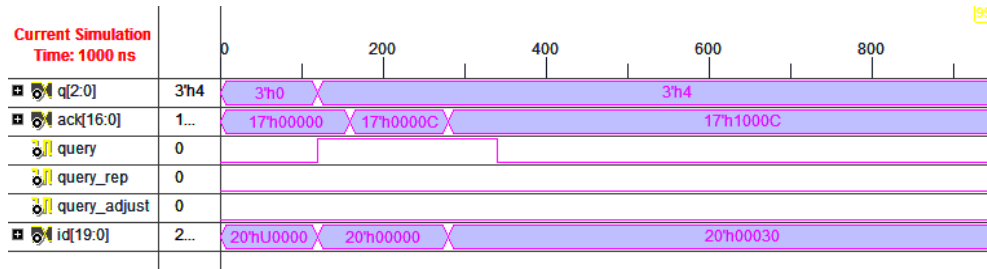


Fig. 4.13: Simulated output of tag

From Fig. 4.13, it is observed that the output of the tag processor after the test bench simulation. If Q='4' and 'query' signal is high ('1') then if 'ACK' signal is there (ACK is received only if SN='0'), the tag will transmit its ID, otherwise it does not transmit RN-16.

4.4.7 RTL Schematic diagrams for Reader processor and EPC Tag:

In Fig. 4.14 and Fig. 4.15, the RTL schematic diagram of the implemented design has been shown. Xilinx Plan-ahead tools have been used to implement the modules of processor and to achieve the elaborate design.

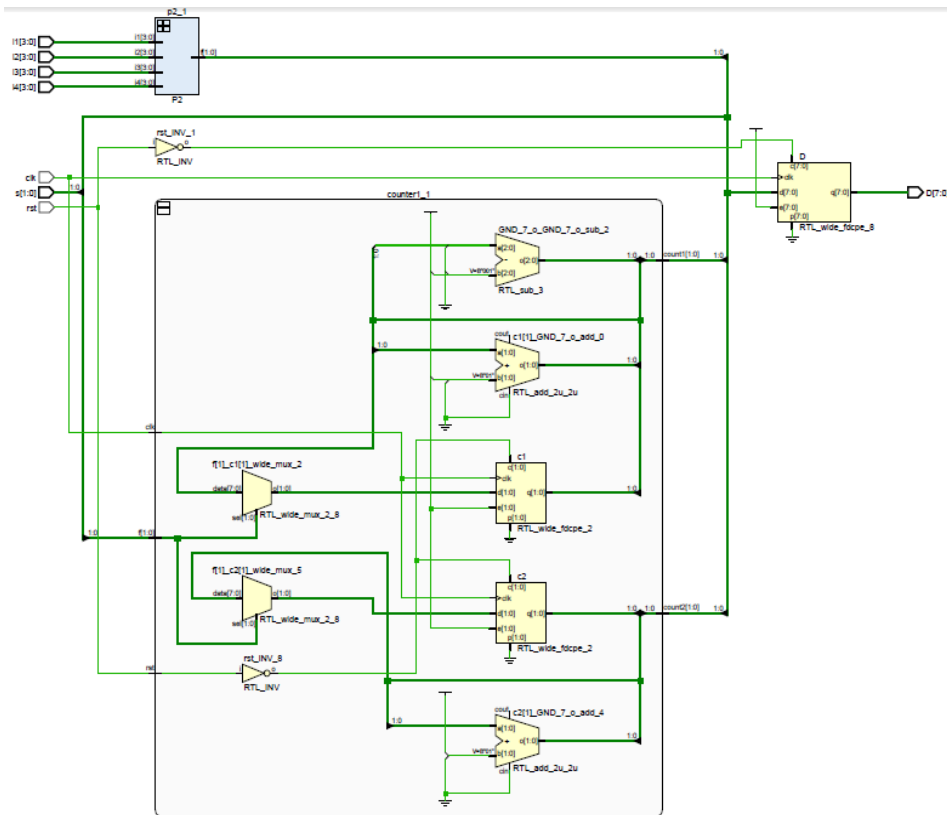


Fig. 4.14: RTL schematic diagram of tag

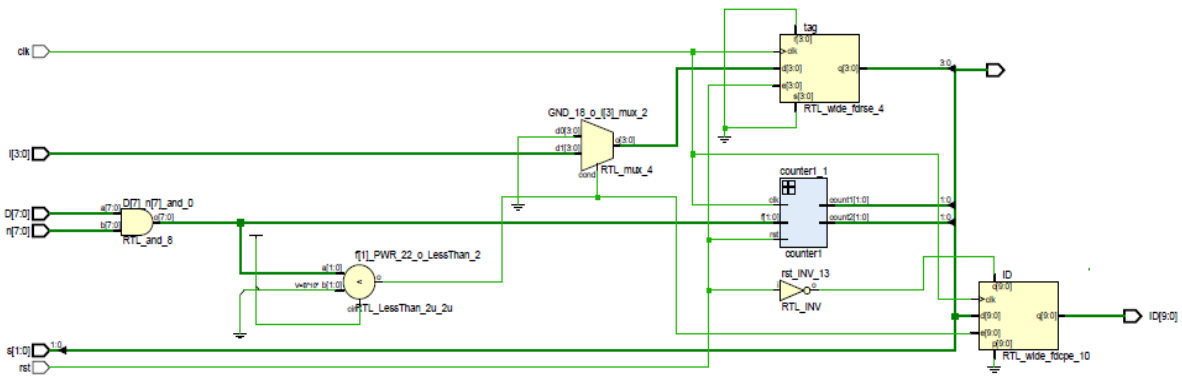


Fig. 4.15: RTL schematic diagram of reader processor

Timing calculation:

1. The Reader send 'query' - wait for 20 ns;
2. Receive 'SN' – check whether 'SN'='0'; if '0' then reads RN16 - transmit ACK – wait for 20 ns;
3. Receive EPC- start new inventory round by sending 'query' again.
4. Else if SN≠'0' the transmit 'Query rep' command - wait for 20 ns;
5. If no response; do not receive any SN then adjusts 'Q' -- start new inventory round by sending 'query' again;

Tag simulation time is 6.229 ns ~ 7 ns to 10 ns;

The Reader simulation time is 10.621 ns+ 7.629 ns (delay) ~ (11 ns + 8 ns) ~ 19 ns ~ 20 ns;

Decoding time for EPC taken by the reader is ~ 10 ns;

The total time taken is ~ 80 ns to identify the tag and decode the EPC. In real world application the timings may vary drastically, but yet the total time for the protocol reduces greatly, it is no doubt because of high speed VLSI implementation of the protocol. We have considered only the simulation time, other delays are neglected. If a complete cycle of identification takes only a few nanoseconds, it is obvious that no. of tags detected in a certain period will be increased.

4.4.8 Synthesis report:

For synthesis, Xilinx 14.3 ISE simulator is used for the simulation process of the processor. The static power consumption for the simulation is only 20 mW, but in case of practical design, designer may choose different suitable low voltages to reduce power consumption. The time scale is set in 'ns' range and simulation is performed for 1000 ns duration. The processor can be modified in accordance with the design constraints and requirements and can be implemented on easily reconfigurable FPGA. The following

discussion explains the device and component requirement for the synthesis of the simulated design, and the combinational path delay of the circuit also.

Table 4.4: Device utilization & HDL Synthesis Report:

<i>Reader module</i>				<i>Tag module</i>			
Advanced HDL Synthesis Report		Device utilization summary		Advanced HDL Synthesis Report		Device utilization summary	
3-bit Adders/Subtractors	1	Number of Slices	13	Registers Flip-Flops	16	Number of Slices	4
Registers: Flip-Flops	22	Number of 4 input LUTs	22	1-bit latch	20	Number of 4 input LUTs	7
4-bit comparator less equal	1	Number of bonded IOBs	67	4-bit latch	1	Number of bonded IOBs	48
Counter	2	IOB Flip Flops	38	Counter	2		
XOR Gate	1			XOR Gate			
Maximum output required time after clock	10.621ns			16-bit comparator less equal	1	IOB Flip Flops	17
Maximum combinational path delay	7.629ns			3-bit comparator less equal	1		
Total memory usage	160584 kilobytes			Max. o/p reqd. time after clock	6.229ns		
				Total memory usage	161160 kilobytes		
Max power consumption(mW)	20.04			Max power consumption(mW)	17.82		

From Table 4.4, we observe the device utilization, and other information for the implemented EPC gen2 reader and tag circuit. The circuit delay is in the order of few nanoseconds whereas the maximum power consumption is 20.04 mW for reader and 17.82 mW for the tag. FPGA based reader and tag has the design flexibility and adaptive feature to modify the processor any time. It is a low power, high speed processor implementation to achieve advanced architecture.

4.5 Efficiency Calculation of EPC Gen 2 Protocols:

The efficiency of protocol depends on the no. of identified tags or successful slots against the no. of query sent or time slot used. The probability of choosing ‘SN’= ‘0’ by a single tag at any time among the range specified by any tag can be calculated using basic probability formula. If more than one tag chooses ‘0’, then the collision occurs, reader confused and can’t identify and transmit ‘query adjust’ command which increases Q by ‘1’ and tags wait for next inventory round.

If the number of tags remaining to be identified for an inventory round is ‘n’ of this protocol, after a ‘query’ command the probability that ‘m’ tags will reply can be calculated according to the Binomial distribution as

$$p_b(m) = \binom{n}{m} \left(\frac{1}{2Q}\right)^m \left(1 - \frac{1}{2Q}\right)^{n-m}$$

According to this distribution theory, the probabilities that a query command results in idle (no tag replies), success (exactly one tag replies) or collision (more than one tag reply) can be calculated respectively as:

$$P_b^{idle} = \left(1 - \frac{1}{2Q}\right)^n ; \quad P_b^{success} = \frac{n}{2Q} \left(1 - \frac{1}{2Q}\right)^{n-1} ; \quad P_b^{collision} = 1 - P_b^{idle} - P_b^{success}$$

To maximize the probability that a query command results in success, that is to maximize the value of $P_b^{success}$.

If a general probability function $P_b(n, x)$ is defined as $P_b(n, x) = nx(1-x)^{n-1}$ where $0 < x < 1$.

For a given value of n, if we wish to maximize $P(n, x)$, we have to find suitable value of x. Differentiating the $P(n, x)$ w.r.t. x, we get,

$$dP_b(n, x)/dx = n(1-x)^{n-1} - n(n-1)x(1-x)^{n-2} = n(1-x)^{n-2}(1-nx)$$

Let, $dP_b(n, x)/dx = 0$, since $0 < x < 1$, we get $x = \frac{1}{n}$.

So, it is found that when $x = \frac{1}{n}$; the value of P (n, x) is maximized. Regarding the EPC Gen-2 protocol, $x = \frac{n}{2^Q}$; We can find that when $n = 2^Q$, or the number of tags equals to the frame size, the value of $P_b^{success}$ maximized.

$$\text{System efficiency} = \frac{\text{successful slot number}}{\text{Frame size}}$$

It is proved that highest efficiency can be obtained if the frame size (total number of slots in a frame) is equal to the number of tags provided. We have used Matlab simulation tool to plot the graphs for probability of successful slots, ' $P_b^{success}$ ' for different 'Q' values (standard values are taken as Q=3, 4 and 5) vs. tag population, 'n'. In Fig.4.16 we plot for tag population $n \leq 40$; and in Fig. 4.17 we plot for $n \leq 100$; the two figures shows that $P_b^{success}$ is maximum for Q = 3 and $n = 8$ (2^3); Q = 4 and $n = 16$; Q = 5 and $n = 2^5 = 32$. We also observed in Fig. 4.16, with increasing tag population, $P_b^{success}$ decreases. To increase the success rate Reader must adopt a modified Q value. With increasing tag population Q value should increase.

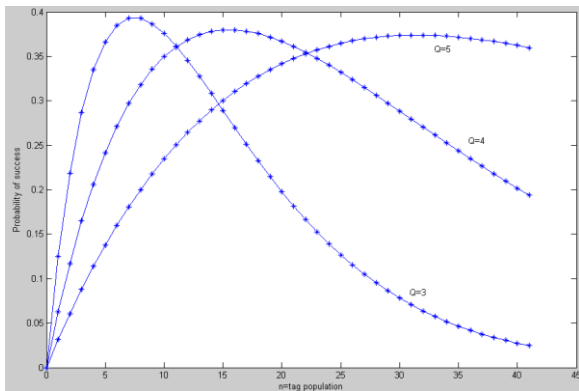


Fig. 4.16: Probability of success vs. tag population ($0 \leq n \leq 40$)

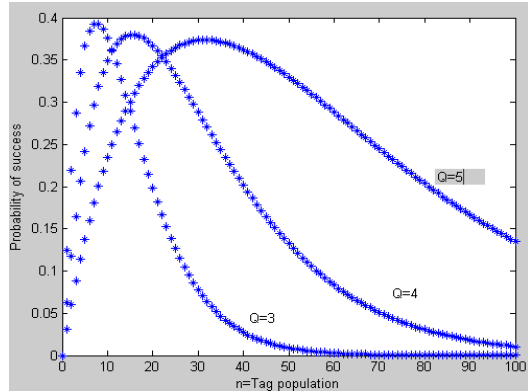


Fig. 4.17: Probability of success vs. tag population ($0 \leq n \leq 100$)

If a tag population of 8 is considered, for Q = 3; ($n = 8$), $\max P_b^{success} = 0.399$; $P_b^{idle} = 0.343$ and $P_b^{collision} = 0.2639$. In this design, a tag takes approximately 80 ns to go to the sleep mode after identified by the reader. Q will be changed for the remaining tags to be identified. In that instance, time duration required is at least 100ns before starting the next inventory round with different/same Q value.

The probability that the number of tags can be decoded within 10 sec interval

$$= \frac{1}{8} * 10 * 100 * 10^{-9}$$

$$= 1.25 * 10^6 = 1,250,000$$

The maximum probability of success can be achieved for $Q_{\max} = 15$; ($n = 2^{15} = 32,768$);

From Matlab simulation, $P_b^{\text{success}} = 0.127052$

Number of tags identified = $1,250,000 * 0.127052 = 1,58,815$;

The time duration utilized to decode the identified tags is equal to about 1.5 seconds which is only 1.5% of the total time. It highlights the very fast identification and processing of tags by the Reader designed by VHDL code which in turn express the enhanced system efficiency.

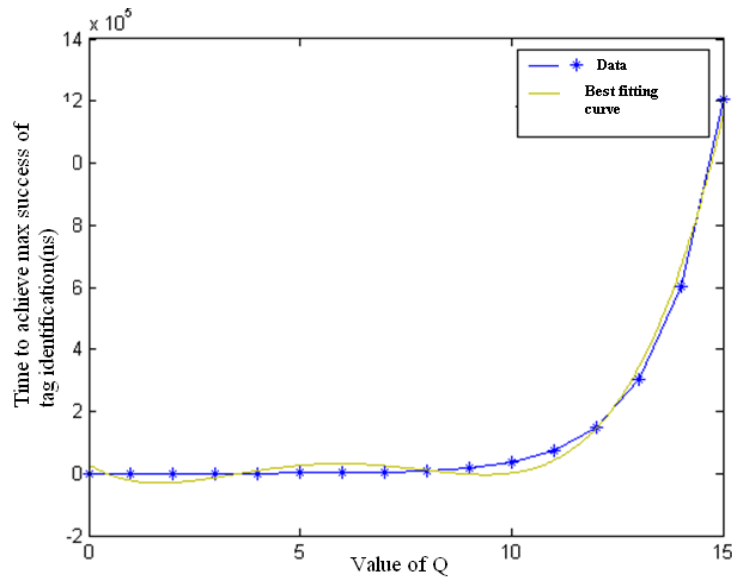


Fig. 4.18: The timing (ns) according to the Q value to achieve the max. Success

The developed model has been simulated for different Q values to achieve the maximum success for tag identification. The time taken by the system has been plotted in Fig.4.18 using Matlab 6.5, where it is observed that when the Q value increases, the time requirement to obtain maximum success increases abruptly. The equation for the best fitting curve to follow the obtained curve is as:

$$\text{Time, } T = 2.2 \cdot 10^2 \cdot Q^4 - 4.9 \cdot 10^3 \cdot Q^3 + 3.6 \cdot 10^4 \cdot Q^2 - 8.2 \cdot 10^4 \cdot Q + 2.8 \cdot 10^4$$

This behavior is not desirable, so the Q value should be maintained within low range value of $0 \leq Q \leq 7$ to obtain maximum efficiency. So, if the no. of tag selection by the Reader using command ‘select’ from a tag population increases, efficiency decreases. From this observation, it is also obvious that Reader should select a considerable portion of tag population to maintain the efficiency curve suitably.

CHAPTER 5

FPGA BASED IMPLEMENTATION OF A DATA SECURITY SCHEME SUITABLE FOR RFID SYSTEM

Chapter 5: FPGA based Implementation of a data security scheme suitable for RFID system

5.1 Introduction:

Secured data transfer is one of the most important criteria of any RFID system and it will also be the responsibility of the system to prevent any unauthorized access to important or personal data or information stored in the RFID tag. Users of RFID tag will need to ensure the security of any personal data or information stored on the tag. In the world of computing, it is very essential to ensure the security and the privacy safeguards into the architecture of an RFID system. The vital communication between tags and readers occurs in the air via RF communication. This connection enables the powerful capabilities of RFID, but it also leaves the window open to several key threats, like unauthorized access to tags, Rogue & clone tags and Side channel attacks.

The Electronic Product Code (EPC) Global class-I Generation-I and Generation-II are popular and globally accepted standard specifications which enable the use of password for accessing the memory of an RFID tag. It gives one of the ultimate securities for the RFID system, but these are not immune to ‘hacking’ [119]. It is possible to know the details of personal data if anybody has the knowledge of EPC references [120]. Under the EPC Generation 2 protocol, there are several common and known factors that act as potential roadblocks to more ubiquitous deployments at the consumer level. Important data or personal information, especially sensitive personal data need an adequate level of encryption to safeguard the data [74].

Hence, we have pointed out the shortcomings of EPC Gen 2 after detailed study about the protocol, from which we get motivated to propose a data security scheme to RFID technology, based on programmable cellular automata rules.

The shortcomings of EPC Gen2 we find are:

- No data encryption – Data (EPC code) is not encrypted and is covered by means of a pseudo-random number transmitted by the tag. Hence, this code can be determined easily by side-channel attack.
- No password protection -Passwords are also not encrypted and is covered with numbers.
- Lack of tag and reader authentication—this introduces the risk of cloned tags and unauthorized readers to recover the data stored in an RFID tag.

So, it is very clear, that the level of security in EPC Gen 2 is not sufficient to meet the original criteria of data security. The alternative scheme, Cryptography cannot be recommended because of its excessive computational overhead and data insecurity on decryption. It also needs a very high level processor to compute the process, which may affect the speed and the cost of the system [121]. Any other suggested method like ‘kill command’ can switch off the tag to such a state that it will be permanently unreadable or unable to respond to interrogation. The ‘clipped tag’ involves temporary removal of its antenna which should not be adopted for all purposes [119, 120]. Presently, the new US passport system is using the RF Shielding, which prevents data to be read unless the shield is being opened [120]. Looking at the rapid development and maturity of RFID system to be deployed in various fields of importance, like defense, warfield, tracking of suspicious element etc, it is an important issue to give security to the database stored in the RFID tag. Data controllers will have to consider the logistics of compliance with the Data Protection Act 1998 before adopting the technology [120].

Data transmission or exchange of data is one of the most important tasks of wireless communication system. Sometimes hackers may hack the data and may alter it or steal information. Radio Frequency Identification technology (RFID) systems, consisting of a reader, tags and middleware have assumed increasing importance in the present age of universal electronic connectivity, of viruses and hackers of electronic eavesdropping and electronic fraud. RFID technology finds a wide range of individuals and organizations like hospitals and patients, retailers and customers, manufacturers and distributors throughout the supply chain, RFID-enabled self-checkouts, contactless payment systems using credit and debit cards with embedded RFID tags, payment systems based on finger scans or other

biometrics to realize substantial efficiencies and productivity gains. All these applications are sure to boost the appeal of RFID in upcoming applications provided the cost of tags reduce and the concerns about basic privacy and security of RFID systems are properly addressed. When a reader interrogates a tag, it cannot only identify the tag, but can also read all the information stored within it. It is necessary to block the access by unwanted readers else, this infringement of privacy becomes a serious problem and hence, authorization of the reader is very important. Thus, security and privacy risks must be carefully addressed (mitigated) through operational, management and technical controls to extract the benefits of the technology [119- 121].

5.2 Literature Review:

In the modern age of wireless data communication, and enormous integrity in information technology, has placed the issue of data security to a challenging level. As the RFID tag store range, hackers can easily hack the data permitting the unauthorized scanning of tags [119, 120]. It may cause adverse effects to the whole RFID system. So, ensuring high security to consumers of the RFID tag and reader is a responsibility of the designers. In some of the cases, where data security has lowest priority and cost is the greater issue, this scheme is not suitable. Encryption of information stored within the tag is typically used to establish some trust between the reader and tag. But in an RFID system, tags have only a few hundred of logic gates whereas most of the encryption scheme requires several hundred / thousands of gates. Most of the onboard encryption operation requires high computational overhead, increasing the gate counts and cost of the tags [121]. AES algorithm is developed as lightweight encryption protocol, which has weak points and can be broken [122]. DST or digital signature transponder algorithm protecting the speed pass has also been broken by scientists [123].

From the study of several literatures, we find proposed application of CA in various fields [124- 129]. The structure of Programmable Cellular Automata can be employed in considerable saving of hardware compared to any existing schemes. The programmability feature of PCA has given more flexibility in VLSI design of this system. For higher processing speed, hardwired implementation of enciphering and deciphering schemes is very useful and demanding too. [130- 135] PCA chips configured with 90 & 150 rules have been

designed, fabricated and tested by S. Nandi et.al. [133]. for building the prototype cryptosystem, PCA plays a major role. In the area of VLSI design and implementation of such data security scheme, PCA has excellent advantages of its simple, modular, regular and cascadable structure. A Tri-valued programmable cellular automata has been proposed and implemented based on Ternary Optical Computer by Jun-Jie Peng et. al.[136]. The TPCA has three advantages over other automata, which is the high programmability, the parallelism of computing and the tri-valued logic implementation. But it is quite complex having high computational speed.

The architectural design and VLSI hardware implementation of cellular automata block and a security system for image processing has described by R.-J. Chen et.al in their article using 2-D Von Neumann CA structure [135,137]. In order to maintain high throughput, the conventional AES cryptography engine includes high complexity. But in an RFID system, the throughput requirement is low. Thus, Adam S.W.Man et.al. focus on the reduction of the complexity in their paper to design the AES architecture for an RFID system and an 8-bit AES encryption and decryption architecture is adopted in their developed system [138].

P. Dasgupta et.al. have described the Programmable Cellular Automata rules in their article ‘Theory and application of non-group cellular automata for message authentication’ [124]. A cellular automaton consists of several identical cells or nodes which are finite state automata (FSA) governed by simple rules, like 90’s rule, 60’s rule, 150’s rule etc. Rules 90 and 150 are important. Rule 90 is the sum modulo 2 of the states of the nearest two neighbors. Rule 150 is the sum modulo 2 of the states of the nearest two neighbors and the state of the cell itself. Both rules 90 and 150 are linear. The cellular automaton is synchronized, i.e., at each time-step, each cell evolves a global update function applied uniformly over all the cells and updates its state according to some set of automation rules. The next state of each cell depends on the present state of the neighbor cells. This update function takes the cell's present state and the states of the cells in its interaction neighborhood. The cells evolve in discrete time steps according to some deterministic rule that depends only on local neighbors. The cell itself may be included in its own neighborhood. A cellular automaton can be of any dimension and can be either cyclic or acyclic. Moreover, PCAs are suitable for hardware implementation since they are very simple, regular, locally interconnected and modular. [127,131].

The structure of the Programmable cellular Automata is very simple, where we find 4-bit PCA resembling a 4-bit parallel in parallel out 4-bit register consists of four D-Flip-Flops and four XOR gates connected in such a way that each state is determined by the two neighboring states [131- 132]. Several research works are going on implementation of cellular automata using different automata rules to meet different types of security needs. Most of them are used for the cryptographic security purpose [33]. D.Das used rules 51,195 & 153 for his proposed parallel AES Encryption Algorithm in his article [122] and P.Angheliesue used rules 51,60 & 102 in his article to design a block cipher cryptosystem and applied for the data encryption of yahoo messenger conversation [134].

M.Mohsen et.al. have described the development of the processor for an image encryption and decryption using cellular automata in their article. R.-J. Chen et.al have described the architecture design and VLSI hardware implementation of cellular automata block. He has developed a security system for image processing and in his article using 2-D Von Neumann CA structure [135,137]. In case of RFID system, the proposed data authentication system has used the 90 and 150 rule for data authentication. A novel code generator for RFID tag and reader using rules 90 & 150 has been proposed in this paper in order to encrypt the tag ID and to provide security for the data/information.

From the research works of different authors, it is found several security scheme using cellular automata rules. A detailed study and review of these schemes reveal that for RFID data security, the proposed security scheme using PCA is very effective with low hardware requirement and high speed. It is a low power and cost effective also due to its low computational overhead with respect to other schemes.

A detailed report of related works has been reflected in Table 5.1.

Table 5.1: Comparison table with other works

Authors name	Rules applied	Application field	Speed & power dissip.	Hardware
Petre Anghelescu	51,60,102	Crypto system	Not mentioned	Not available
Debasis Das	51, 195, 153	AES Encryption	1.44ms (256 bits)	Not available
P. Dasgupta	90, 150	Message authentication	Not mentioned	Not available
R.-J. Chen	2-D Von Neumann CA	Image security	180ms/3Mb& 27.74 mW (256 bits) Working-Freq. 100 MHz	Area reqt. 15.68 mm ²
M.Mohsen,	2-D Von Neumann CA	Image security	0.786ms&516.61mW (256bits)Work.freq.176MHz	1184 slices

5.3 Different Data Security schemes:

Three matrices define data security in an RFID system:

- The controlled access to the data, which indicates that only the authorized reader can read and write information on the tag.
- The control over access to the system, which allow only authorized entities to configure and add to the system. All devices on the system must be authentic and trustworthy.
- Confidence and trust in the system, i.e. users share a general perception that the system is safe and secure.

Now, every communication system has its own level of data security. Not every type of data merits the highest level of security because enhancing levels of security leads to introduce extra cost and technological complexity, and RFID case is not an exception. It is very critical and challenging to balance security threats against security costs. As it is a globally accepted and widespread technology in various important fields, RFID must achieve an appropriate level of confidence, security and trust. Consumers want to ensure that their personal information isn't misused, vital information doesn't leak out and that RFID tags are used responsibly. Manufacturers also want to use RFID technology to increase efficiency, serve consumers better, and gain a competitive advantage. So, RFID systems need to ensure the reliability and security of their systems, as well as their usefulness and competitiveness.

Some existing Security schemes are as follows:

5.3.1 Smart Tag Approach for data security for RFID:

In this scheme, a cryptographic function and a ROM are embedded within each RFID tag. An RFID tag changes its output every time using a cryptographic function, public key encryption, common key encryption or hash function on it.

i. Hash function based Scheme:

It is a very important cryptographic function to provide high-level data security but need a high computational overhead. Hence, the cost of this type of security is high. Hash functions are considered to be less suitable for RFID implementation. The design of many collision-resistant hash functions uses a block cipher with a large block length optimizing the software performance, but makes it inefficient to implement under constrained-memory settings. In this scheme, the reader has a key 'k' for each tag, and each tag has a complex function named as Hash function $h = H(k)$, stored into its memory, is called meta-ID. When a tag receives a request from a reader for ID access, it sends the meta-ID in response. The reader sends key k, which is related to the meta-ID received from the tag. The tag then calculates the hash function from the received key k and checks the relation of $h = H(k)$ with meta-ID stored in the tag memory. If the two ID matches with each other, then the tag responds with its own ID to the reader only. However, the scheme is still susceptible as the meta-ID is fixed. Hence, to overcome this, the meta-ID is required to be modified periodically.

ii. Public key encryption based scheme:

This scheme uses a public key function for encryption of data. This scheme also provides a very good information protection. But this is an expensive scheme due to its complex computational function and requires a comparatively large memory size which is not suitable for low cost RFID chip. Most common symmetric key encryption scheme is AES encryption and ECC scheme is the most used asymmetric key encryption. Both are costly due to their circuit complexity and computational overhead.

iii. Common key encryption based scheme:

A common key encryption based scheme uses a common key for the encryption process. Here, the common key encryption function, a ROM and a pseudorandom number generator are embedded within each RFID tag. Computational overhead is less than that for Public key encryption scheme, but the computational load of the server is high enough.

5.3.2 Rewritable Tag Approach for data security:

In a Rewritable RFID Tag, a nonvolatile RAM is embedded within the tag. The ID of the RFID tag is stored in the RAM and the server can rewrite the ID according to requirement. The tag does not need cryptographic function, the cost of an RFID tag is low, but the running cost of the system is high because the server has to update the tag's ID periodically. The reader uses a public key to decrypt the data and re-encrypt it. The server uses a private key to extract the information from it.

5.3.3 Physical Blocking Approach for data security:

The physical blocking approach for data security prevents an adversary from accessing RFID tags physically. The EPC global standard uses kill command, which disables functionality of the tag. PIN protection is given to this type of kill commands without which the tag cannot be activated. In the clipped tags, user can physically separate the chip from its antenna to avoid unwanted access. But the physical blocking of tag for data security has a problem that a user cannot use the RFID service properly. In this scheme, even a regular service reader cannot access the RFID tag.

5.3.4 Block cipher based cryptography:

To achieve highly efficient hardware optimizations under constrained memory conditions, Block ciphers are suitable for RFID implementations. In this field, substantial work has been done that validates the suitability of AES for RFID tags and full implementations of AES require only 3300–3400 GE.

5.3.5 Pseudo-random number generators for RFID data security:

Pseudo-random number generators can be structured using block ciphers in counter mode, or stream ciphers and independently using other technologies. This type of security provides flexible trade-off opportunities between security and efficiency requirements. Pseudo-random number generators are flexible primitives and thus it has advantages in designing PRNG based security for RFID technology.

5.3.6 Stream cipher based cryptography:

In RFID technology, selection of stream ciphers for data security is difficult due to the lack of standardized choices. Several stream ciphers have been selected on the basis of their performance characteristics in hardware implementations. Considering the resisted cryptanalysis and the good miniaturization characteristics, RFID-suitable stream cipher will be standardized in future applications.

5.3.7 Elliptic curve cryptography (ECC):

Elliptic Curve Cryptography (ECC) is Asymmetric Cryptographic Primitives and it may eventually be used to design high-end, passive tags due to its property of special architectural constructions. It requires a high computational complexity, thus a large memory and cost overhead. Taking price into consideration and the current state of the art in passive tag technology, it appears ECC will not be suitable for RFID data security.

Hardware implementation of the Crypto processor based on these crypto algorithms provides an overview on the performance of these processors in terms of power consumption, silicon area etc, as depicted in Table 5.2 provided here below.

Table 5.2: Comparative study of different crypto-algorithms.

Crypto Algo.	Freq	Power consumption	Si-Area	Delay	Gate count.	CMOS tech
AES	10 MHz	12mW	1.18 mm ²	1000 clk. cycles	3868-4400	0.25μm
DES	500 KHz	5mW (8bit)	0.98 mm ²	-	-	0.25μm
ECC	18 MHz	95mW 173bit	1.31 mm ²	7.56 ms	6300-7800	0.25μm
Hash func.	10 MHz	-	-	-	545 per PUF	0.25μm
TEA Tiny encryption algo.	50 MHz	-	0.21 mm ²	32	-	0.35μm

5.4 VLSI Implementation:

5.4.1 Proposed System:

In this proposed system, the Reader knows the key previously and it also generates the secret code with the same secret code generator. When the tag is identified by the Reader, it receives a data frame containing the Sc and the original ID of 8bit. If the two Sc matches with each other, it transmit a signal ‘ack’. When the tag receives the acknowledgement, (‘ack+Sc’) communication for data transfer is ready. But if the code does not match, the Reader is unable to decode the ID of the identified tag. Thus the tag does not allow reading the data or preventing it from ‘hacking’. The Reader also checks if the tag is of its interest or not otherwise it will skip to read its information saving the time and preventing unwanted gathering of information in the Reader.

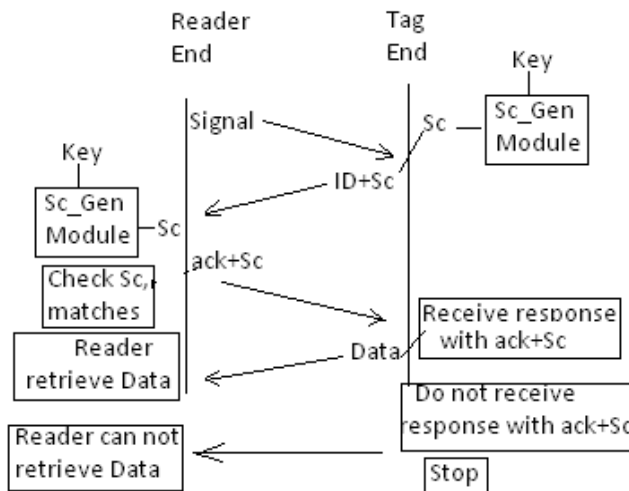


Fig. 5.1: Pictorial description of RFID Data Security System

The excellent performance of proposed Programmable Cellular Automata System, in terms of least time of the software implementation of the scheme is established from the careful studies from different journals [136- 139]. The regular and cascable structure of the cellular automata makes the scheme suitable for VLSI implementation. The processor can achieve very high speed as described in this article. VLSI implementation is performed using VHDL code and Xilinx 14.3 ISE simulation tool. Satisfactory results from the test bench simulation waveforms are obtained and the design has been synthesized to achieve the RTL schematic view of the Reader processor and the tag ID generator module.

In this proposed data authentication system, each tag and the associate Reader will be provided by the same secret key and a special processor to generate the secret code and to decode the generated code using that key. The code will be generated and decoded using the Cellular automata rule from the provided key. The code will be checked by both the Reader and the tag for establishing a trusted communication for secured data transfer. Any unauthorized Reader will not be able to read the data unless the key is available.

5.4.2 Generation of Secret code ‘Sc’ using cellular automation rules:

Rule 90 and rule 150 has been used in this processor design module due to their advantages to implement in VHDL code. So, here is the brief discussion about the rules. In automation rule the next state of cell can be determined if the present state and previous state are known. Table 5.3 shows the chart of these states.

Table 5.3. Rules that update the next state of the cells

Rules	7 111	6 110	5 101	4 100	3 011	2 010	1 001	0 000
90	0	1	0	1	1	0	1	0
150	1	0	0	1	0	1	1	0

The binary number $(01011010)_2$ represents the decimal number 90 and the binary number $(10010110)_2$ represents the decimal number 150. In Fig 5.1 we observe the state transition diagram for programmable cellular automata.

The proposed encryption system has been realized using a combination of two CA. The rules 90 and 150 can be expressed as follows:

$$Sc_i(t + 1) = Sc_{i-1}(t) \text{ XOR } Sc_{i+1}(t) \dots \dots \dots \text{Rule. 90}$$

$$Sc_i(t + 1) = Sc_{i-1}(t) \text{ XOR } Sc_i(t) \text{ XOR } Sc_{i+1}(t) \dots \dots \dots \text{Rule. 150}$$

This CA is used to provide real-time keys for the block cipher in this paper. The operation of CA can be represented by a state-transition graph. Each node of the transition graph represents one of the possible states of the CA. The direct edges of the graph correspond to a

single time step transition of the automata. Fig. 5.3 shows the state transition graph of a 4-bit hybrid null boundary condition CA with rules <90, 150, 90, and 150>.

Suppose we choose key Matrix as $K = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$

Now if the $K_{i0}='0'$ then the entire row will follow the rule 150 and if $K_{i0}='1'$ then it will follow rule 90.

From the chosen key Matrix, 1st and 3rd row will follow rule 90 whereas 2nd and 4th row will follow rule 150.

For rule 90:

- i. Data of 1st column of secret code Matrix Sc will be as $Sc_i = K_i \oplus K_{i+1}$
- ii. Data of 4th column of secret code Matrix Sc will be as $Sc_i = K_{i-1} \oplus K_i$
- iii. Data of other column of secret code Matrix Sc will be as $Sc_i = K_{i-1} \oplus K_i \oplus K_{i+1}$

For rule 150:

- i. Data of 1st column of secret code Matrix Sc will be as $Sc_i = K_{i+1}$
- ii. Data of 4th column of secret code Matrix Sc will be as $Sc_i = K_{i-1}$
- iii. Data of other column of secret code Matrix Sc will be as $Sc_i = K_{i-1} \oplus K_{i+1}$

Following these rules,

The code Matrix for Sc will be as, $Sc = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$

Now if this code Matrix is integrated with the tag ID, only the Reader, who knows the exact Key Matrix, will be able to decode the ID and the data or information stored within the tag. Thus prevents the data hacking by unauthorized Reader.

Fig. 5.2 shows the state transitions diagram of a maximum-length group CA.

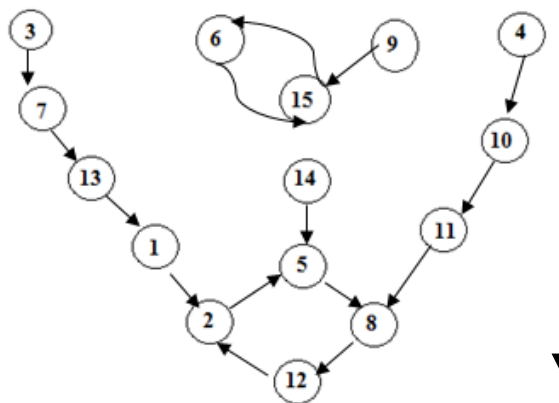


Fig. 5.2 State transition diagram for PCA

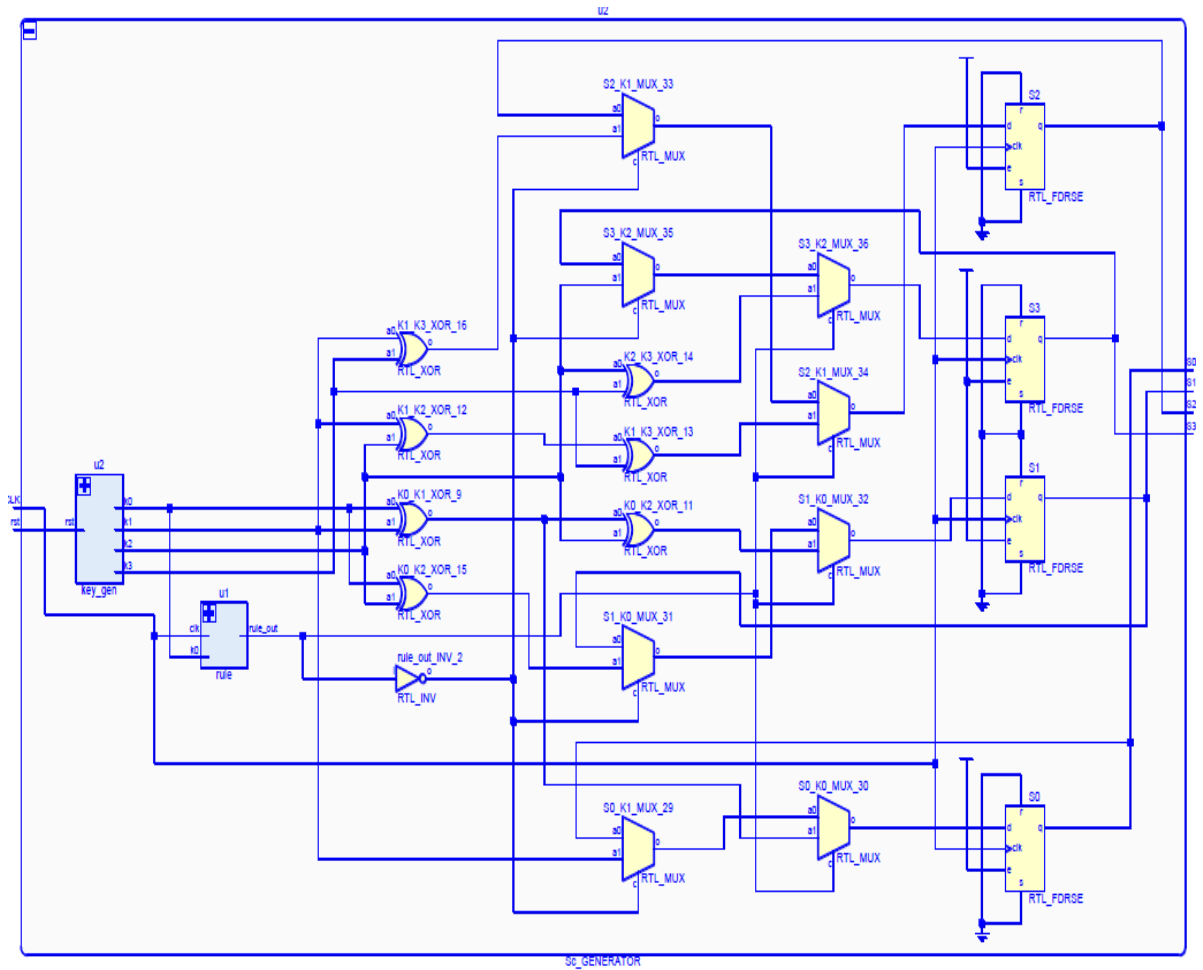


Fig. 5.3 Structure of Secret code generator using Programmable Cellular Automata (PCA)

The implemented structure of the secret code generator is shown in Fig. 5.3, using programmable cellular automata rules. This is the basic block of code generation for both the reader processor and tag ID generator module. In this module, a key generator has been incorporated along with a rule selector. The key generator provides the key matrix as per designers’ choice and the rule selector selects the rule from rule 90 & 150 to be applied accordingly to generate the required code matrix. In Fig.5.3, the RTL schematic diagram of the Secret code generator using Programmable Cellular Automata (PCA) is shown. The XOR operation in the circuit is performed by seven XOR gates. Eight Multiplexers are used to generate the proposed code.

5.4.3 Operation of Tag:

- The tag has its 8-bit unique ID and the secret key matrix
- Generates its own 'Sc' from the secret key matrix
- Receives 'Ack' from the Reader
- Transmits ID+ 'Sc' to check whether the Reader is authenticated or not
- If the Reader is authenticated i.e, is able to decode the data frame and 'Sc', it will transmit 'ack+Sc'
- As the Tag receives this signal 'ack+Sc', it allows the Reader to retrieve data/information stored within it

Else

Skip or do not respond to communication and thus prevent data from unauthorized Reader.

The operational flow chart of the tag is shown in Fig 5.4.

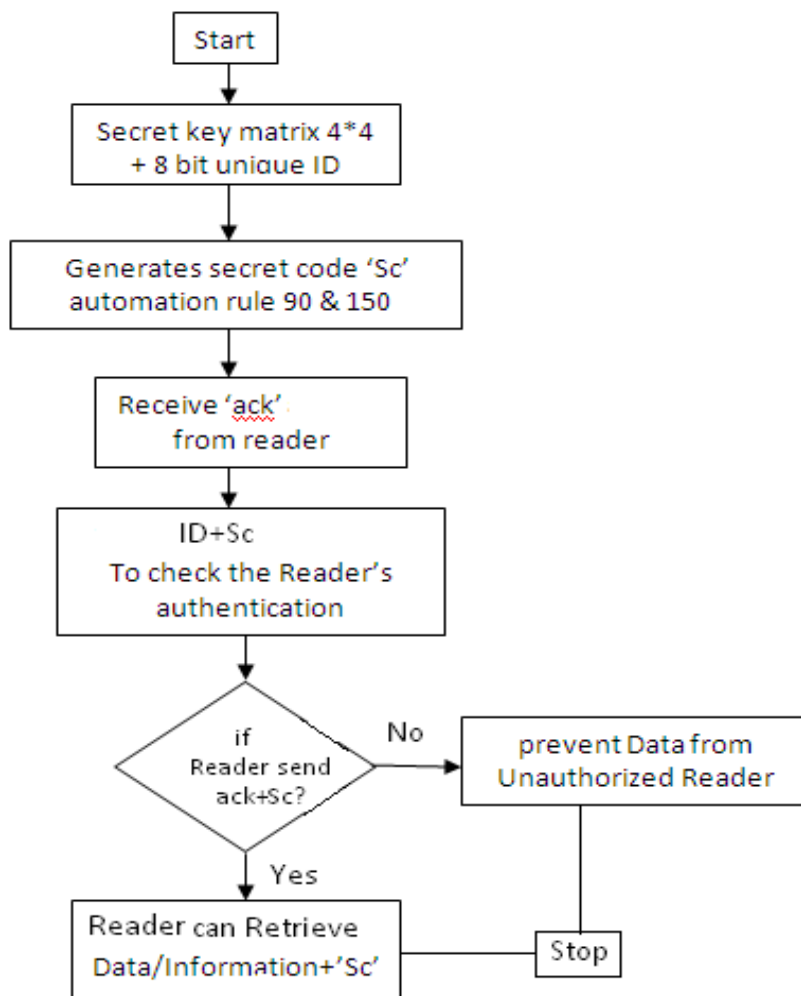


Fig. 5.4. Flow chart for tag operation

5.4.4 Operation of the Reader

- Identifies the tag within its range using an efficient anti-collision algorithm
- The Reader must know the secret key and generates the secret code 'Sc' using that key
- Broadcast a signal 'Ack' along with 'Sc'
- If the Reader receives data from tag, it first decodes the 'Sc'
- If the code matches with its own, Reader will retrieve data from the tag.

Else

Reader will not be able to read the Tag information.

In Fig 5.5, the operational flow chart of the Reader is described.

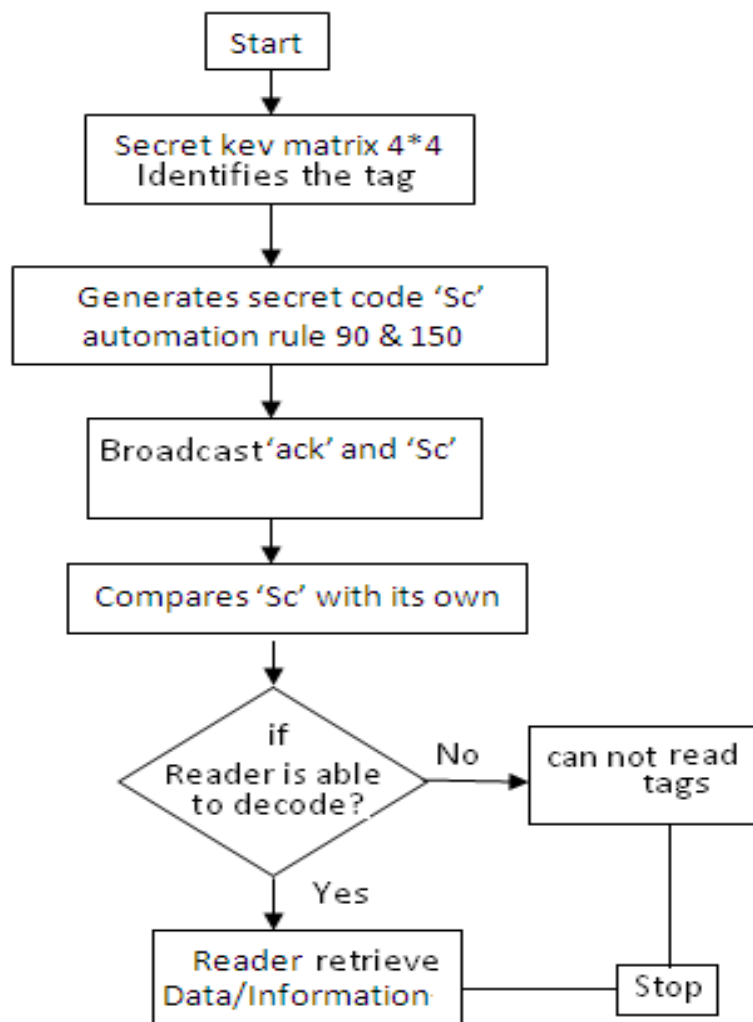


Fig. 5.5 Flow chart of Reader operation

5.5 Simulation Results:

a) Simulation results of tag ID generator:

The secret code generator named as ‘Sc_Generator’ module has been designed, which follows the code generation process using automation rule as described in introduction section shown in Fig.5.3. For simulation purpose, Xilinx 14.3 ISE software simulation tool has been used. The hardware description language with high level syntax, VHDL is used as design code [40, 41]. This same module is used in both tag ID generator and the Reader processor module with same keys.

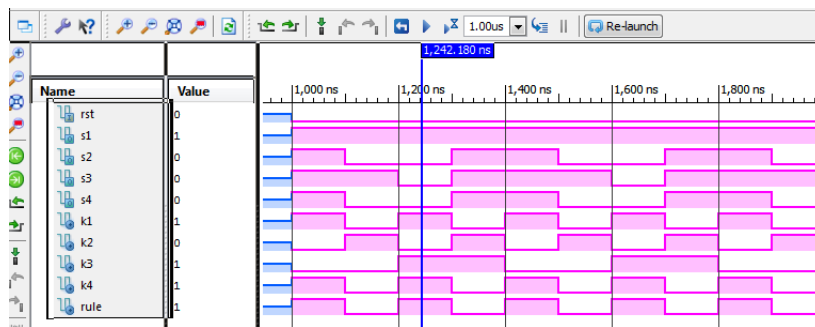


Fig 5.6: Test bench simulation wave form for Sc_Generator

The test bench simulation result of this module is shown in Fig. 5.6. In the test bench, K0,K1,K2 and K3 are the Key Matrix bit and S0,S1,S2 and S3 are the bit for the generated code ‘Sc’. The port ‘RULE’ selects the rule to be used. When RULE=’1’ then rule 90 will be followed and when RULE=’0’ then rule 150 will be followed. Rule gen module selects the port ‘rule’ level ‘0’ or ‘1’. For K=[0 1 1 0], we get Sc=[1 1 1 1],for K=[0 1 0 0], we get Sc=[1 0 1 0] and for K=[1 0 1 1] we get Sc=[1 0 0 0]; which are the desired result. In Fig 5.7, the test bench simulation result for the Tag ID generator is shown.

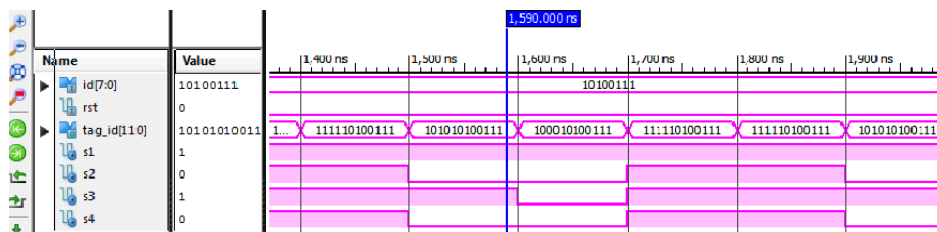


Fig. 5.7 Test bench simulation result for Tag ID generator

The output of the Tag ID generator module is observed in Fig. 5.7. The tag has its tag_id (12 bit) incorporated with Sc (4 bit) and its own unique ID (id of 8 bit). S represents the

generated code from the key matrix. Tag receives signal ‘ack’ and 4 bit for the Sc from Reader end. The Reader can read data/information from the Tag.

b) *Simulation results of Reader processor:*

Tag has its ID incorporated with the ‘Sc’, the code generated from a key matrix using 90&150 cellular automata rule. As the tag and the reader have same key matrix and same Sc code generator module, the reader can easily identify the tag ID, hence the information stored in it is retrievable for the reader. But if an unauthorized reader tries to identify the tag ID, it will not be able to retrieve its original ID from the integrated unique ID until it is provided with the key and the Sc generator module. So it is totally inaccessible for that reader. Thus a high level of data security for the system can be provided.

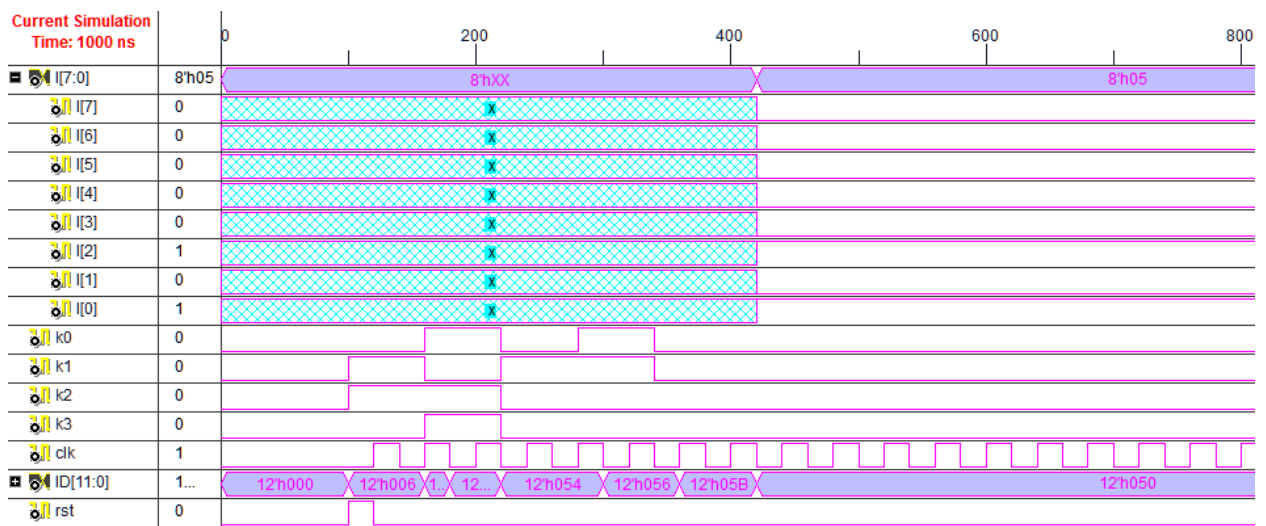


Fig. 5.8: Test bench simulation result for the reader processor.

In Fig. 5.8, ID is the 12 bit data read by the reader as tag ID, where ID(3) to ID(0) represents the ‘Sc’, if the reader has same key and ‘Sc’, the ID of the tag which is represented by rest of the bits[ID(11) to ID(4)] could be retrieved, here it is “0000 0101” (05_h). In Fig.5.8, it is observed, that until the bits are all checked, the reader output ‘I’ is in high impedance state (X) and after checking is complete, reader shows the tag ID as ‘I’ as 05_h.

c) Synthesis Report:

The RTL schematic of the secret code generator, 'Sc_Generator' has shown in Fig 5.9. The elaborate gate level design of this block has shown in Fig. 5.2. The CA module needs 4 D-F/Fs and six XOR gates to perform the code generation. The module follows the adopted rules. The simulation is based on 'ns' timing scale.

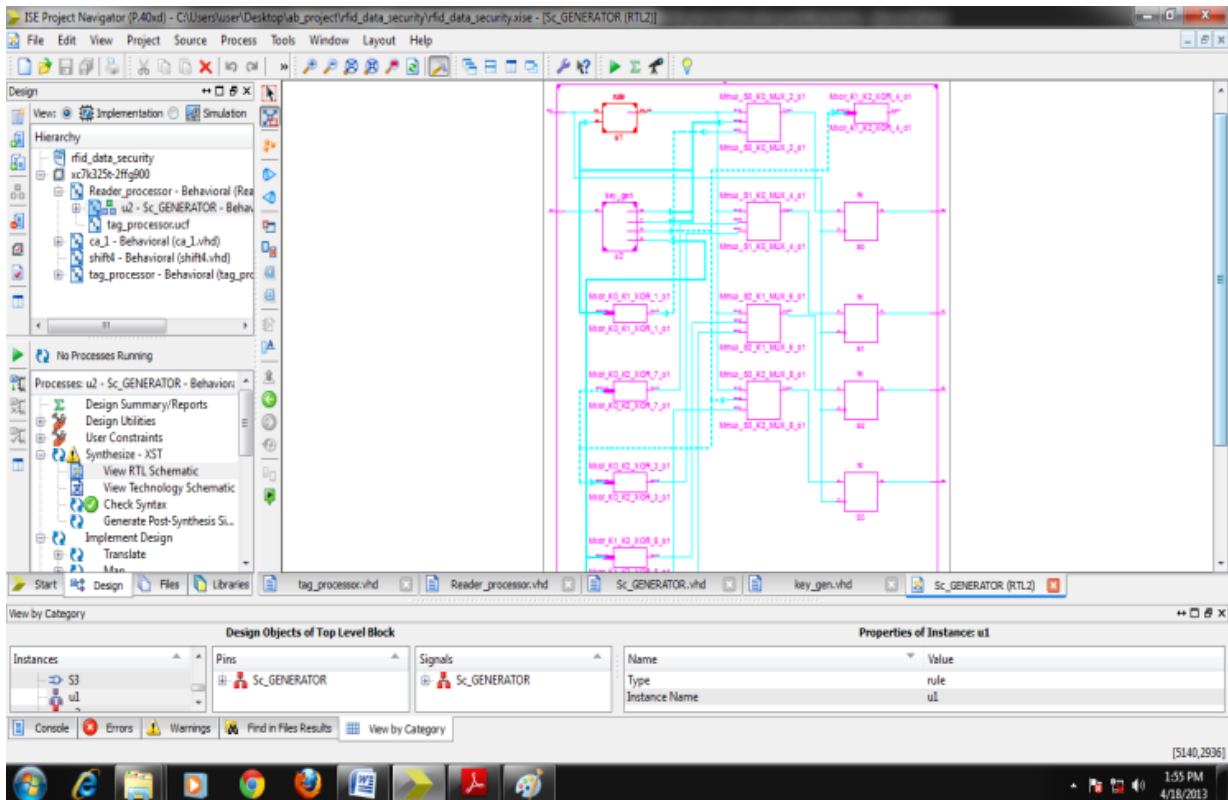


Fig 5.9: RTL schematic view of Sc_Generator (secret code generator)

This 'Sc_Generator' module is used to design the tag ID generator i.e., the module to integrate into the original tag ID with the generated secret code Sc from the Sc_generator module for the Tag. The dataframe for tag will include the 8-bit unique ID and this code. So to retrieve data from this dataframe, the Reader must know the key Matrix to decode the data frame.

Reader_processor Project Status (04/18/2013 - 11:55:40)			
Project File:	rfid_data_security.xise	Parser Errors:	X 2 Errors
Module Name:	Reader_processor	Implementation State:	Synthesized
Target Device:	xc7k325t-2ffg900	• Errors:	
Product Version:	ISE 14.3	• Warnings:	
Design Goal:	Balanced	• Routing Results:	
Design Strategy:	Xilinx Default (unlocked)	• Timing Constraints:	
Environment:	System Settings	• Final Timing Score:	
Reader_processor Project Status (04/18/2013 - 12:04:47)			
Project File:	rfid_data_security.xise	Parser Errors:	X 2 Errors
Module Name:	Reader_processor	Implementation State:	Placed and Routed
Target Device:	xc7k325t-2ffg900	• Errors:	
Product Version:	ISE 14.3	• Warnings:	
Design Goal:	Balanced	• Routing Results:	All Signals Completely Routed
Design Strategy:	Xilinx Default (unlocked)	• Timing Constraints:	All Constraints Met
Environment:	System Settings	• Final Timing Score:	0 (Timing Report)

Fig. 5.10: Report of Synthesized and placed & routed module of RFID data security Reader processor

Fig.5.10 shows the successful report of synthesis and the place & route operation of the reader processor module. The Tag ID generator consists of the sc_generator module to encode its tag ID and the encoded tag ID is transmitted which may be decoded by the RFID reader having the same key matrix and the same Sc_generator module adopting the similar automata rules. The RTL schematic of Tag ID generator is shown in Fig 5.11.

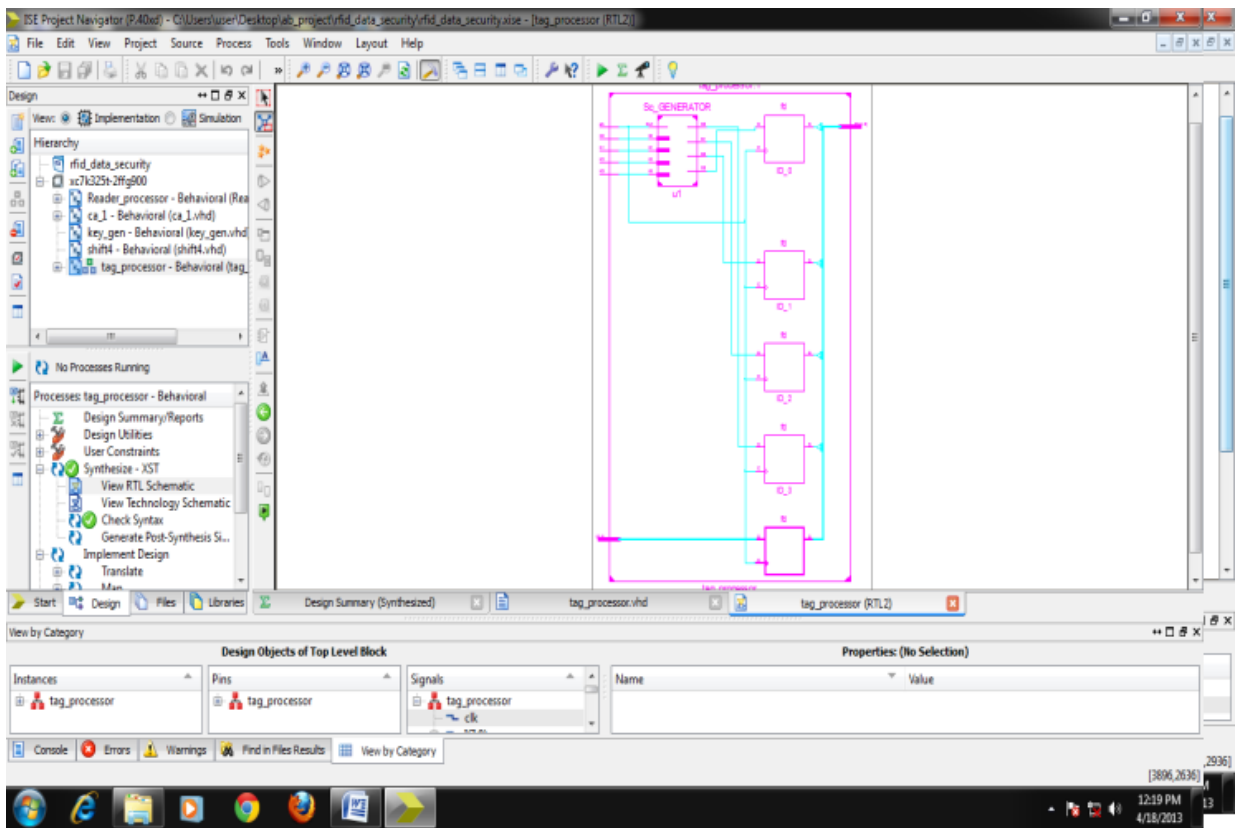


Fig 5.11: RTL schematic for Tag ID generator including Sc_Generator.

The RTL schematic of Tag ID generator is shown in Fig 5.11 which includes the secret code generator module.

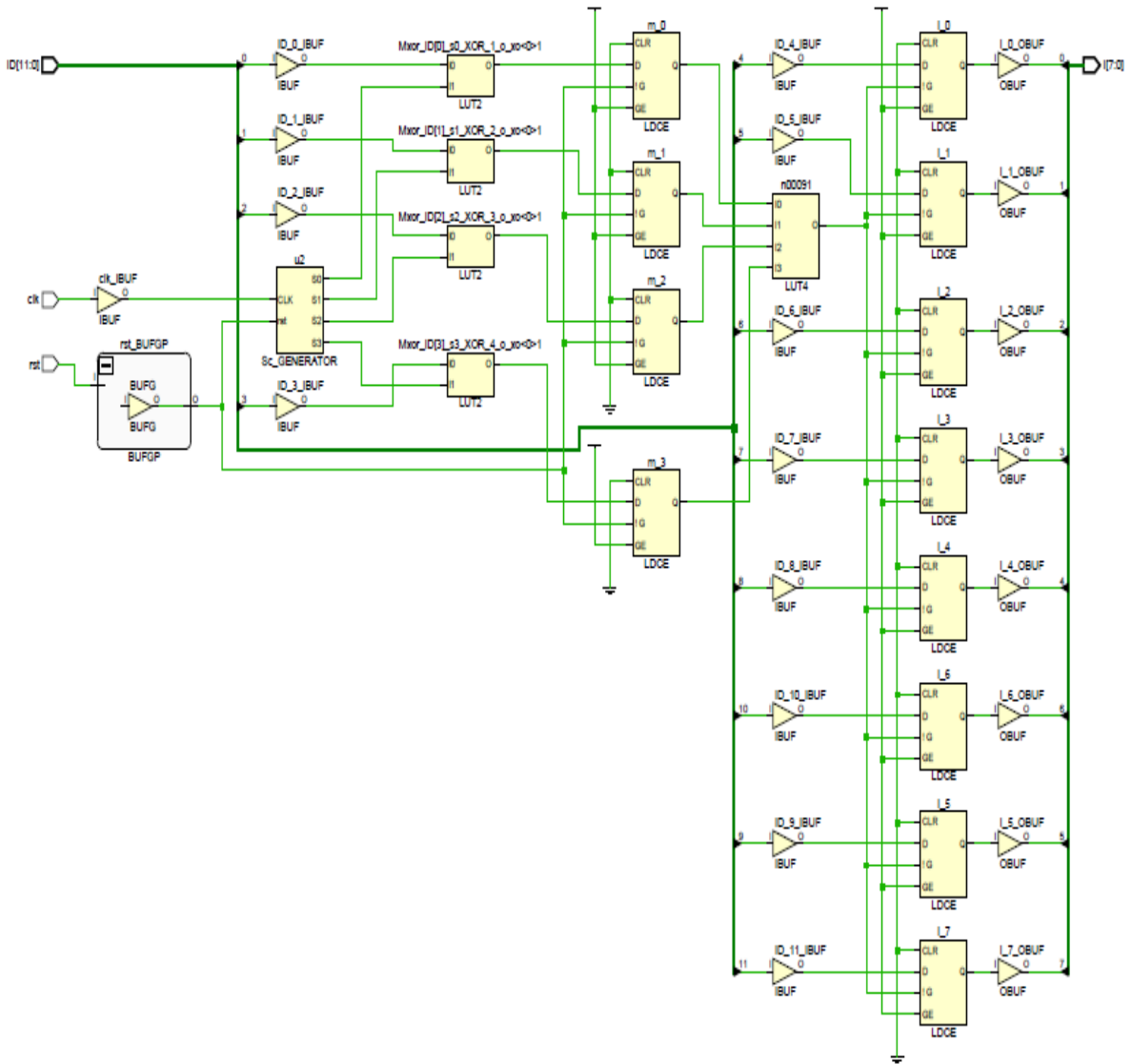


Fig. 5.12: RTL schematic of Reader processor including Sc_generator module. (similar module with same key matrix and same rule of automata)

The RTL schematic view of the Reader processor module has shown in Fig. 5.12. The processor module for reader incorporates the same Sc_gen module having the same key matrix. When the reader interrogates a tag within its range, it can read the coded ID and decode it by the Sc_gen module. It has one comparator and four XOR gates also. The processor takes a fraction of nanoseconds to process the data frame and it draws a very little power for processing.

The device utilization summary is given in the following Table 5.4.

The device used for application Rf_Device is an NCD, version 3.2, device xc7k325t, package ffg900, speed grade -2; Minimum clock period: 0.652ns (Maximum Frequency: 1533.507MHz)]

Table 5.4: Device utilization summary for Sc_Generator; Tag ID generator and Reader Processor

Parameters	<i>Sc_Generator</i>	<i>Tag ID generator</i>	<i>Reader Processor</i>
Multiplexers	8	4	0
Flip-Flops	5	17	5
1-bit xor2	7	7	10
4-bit comparator	0	0	1
1-bit latch	0	0	12
Number of 4 input LUTs	5	5	10
Number of Slice Flip flops	5	9	9
Number of bonded IOBs	9	25	26
IOB Flip Flops	3	8	8
Delay	0.575 ns	0.681 ns	0.795 ns
On-Chip Static Power	-	-	122.13 mW
Quiescent Current	-	-	1.27 mA

From Table 5.4, we observe the on chip static power consumption of the processor for data processing is only 122.13 mW with a quiescent current of 1.27 mA. The processing time after clock is 0.795 ns only. The hardware utilization is only 37% for the reader module and 26% for the tag module. As the PCA based security scheme minimizes the computational overhead unlike other encryption algorithm based security scheme, it is better in respect of circuit complexity, processing speed and power consumption.

CHAPTER 6

LOW POWER VLSI DESIGN FOR LARGE WIRELESS SENSOR NETWORK

Chapter 6: Low power VLSI Design for large Wireless Sensor Network

6.1 Introduction:

The Wireless Sensor Network is a network of spatially distributed autonomous or semi-autonomous sensor nodes to monitor and collect the physical or environmental conditions, like temperature, pressure, etc and to co-operatively forwarding the information to the next node towards the main controller unit. Modern networks are bidirectional, enabled with control over sensor activity. The major applications of WSN are battlefield surveillance, industrial process monitoring and controls, etc. WSN is consists of several hundreds and thousands of sensor nodes and each node has typically three parts: a radio transceiver, a microcontroller and an electronic circuit to interface with the other sensors. The energy source is usually a battery or an embedded form of energy harvesting. Size and cost of nodes largely depends on corresponding constraints like computational speed, memory capacity, communication bandwidth, application area and importance of the field.

In general point of view, sensor nodes must be economical, miniaturize, plentiful, and reliable. The sensor node to become a wireless sensor network must have the capability of sensing, processing, and communication elements [19]. WSN is a new direction for researchers to provide more energy efficient, reliable and low cost system. Prolonging network lifetime for these sensor nodes is a critical issue. Sleep scheduling for sensor network is another important key factor which controls the energy management. In a sensor network, a wake up timer is used which activates the sensor node when it receives a signal and it starts processing. It enters into sleep mode again after processing until it receives next wake up signal [150- 151].

The design and implementation of a sensor node model has been accomplished in this research work, incorporating the data sensing, processing and communication capability for short and long transmission range efficiently. In order to achieve power efficient system, an intelligent sleep scheduling algorithm has been adopted. On the other hand, ASIC VLSI implementation is the most energy efficient preferred solution where need for flexibility is

almost nil after sensor deployment [10,11,19,20]. The available beacon sensor nodes based on microprocessor and microcontroller are unable to incorporate the new developing technology due to technical limitations. Hence to take advantage of new process technologies and geometries to increase economies of scale and throughput has shift the sensor nodes to soft core processors embedded within the FPGA or ASICs.

Modern electronics systems are moving towards the self-adjusting and adaptive circuit architecture that can quickly and efficiently respond to real time changes. Hence, we propose suitable object localization and its boundary estimation algorithm in the next step of this research work. The aim of this algorithm is to integrate the advancement of technology with the sensor networking system. The FPGA based reconfigurable hardware architecture can be easily modified or upgraded to enhance its performance without much effort, time or cost. In the proposed algorithm in this research work, the network structure is used to communicate the corners of the obstacle detected by the nodes. The position and boundary of the obstacle are constructed by the network infrastructures. The Beacons with the ability to reconfigure the routing protocol can broadcast final and appropriate routing information to all other sensing nodes. A processor is designed and implemented in this research work, to enhance the processing ability of the beacon and guide it to take proper decision. The fast processor reduced the delay to a fraction of a second. The nodes are distributed in a random manner. If some nodes do not respond due to some environmental cause, yet, the proposed technique can give an overview of the obstacle, if any, at a glance, without delay.

Enabling multi-hopping and employing an appropriate routing algorithm the nodes are able to send data in a sensor network. But they don't have information about their position. So, in real world applications, a high degree of autonomy and self-organization is required for proper functioning of the Wireless Sensor Network [146- 151]. Routing and navigation of WSN operation are hindered by various forms, like mountains, high rise building, big trees, rocks, etc. If the location and size of these obstacles can be obtained in advance, preventative action can be taken to ensure that the functionality of the WSN is preserved causing no attenuation or delay [144, 145].

In the network topology, the nodes are randomly distributed throughout the area and a small number of special nodes, called beacons are placed in a regular manner, so that they control the total area by reconstructing the routing information. This specialized network

node or beacons know their exact position by means of Global positioning system (GPS). They also have some information about themselves like identity, transmission range, etc. This information is broadcasted by each beacon to other nodes in the form of a message. The other nodes calculate their position details and transmit with a low transmission range to neighbor nodes. In this case, the position is determined in the probabilistic way using region code determination [144].

A Typical Wireless Sensor Network Topology is shown in Fig.6.1. Where 'A' is the node sensing an 'event' and deploy multi-hop process to transmit the information to the next neighbor node as per routing algorithm.

Information/Data is transmitted through

$A \rightarrow B \rightarrow C \rightarrow D \rightarrow E \rightarrow \text{Sink} \rightarrow \text{Internet \& Satellite}$ and User through Controller or Task manager node.

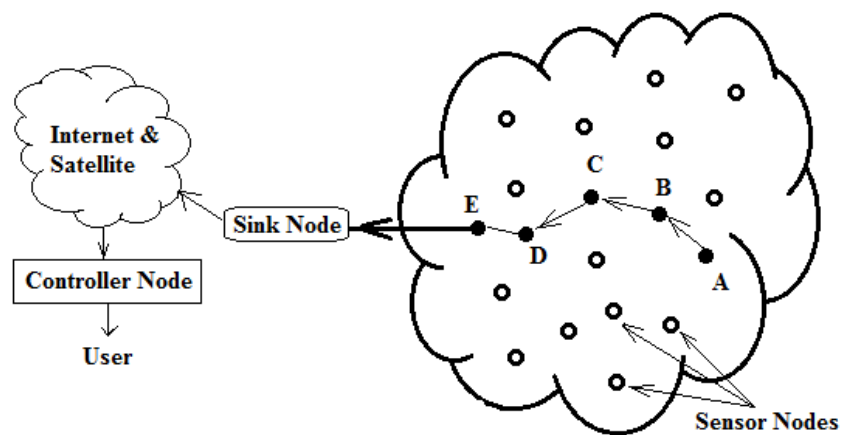


Fig. 6.1 A Typical Wireless Sensor Network Topology

The pivotal function of WSN is to confirm the position of the event, where it occurs and the position of the obstacle which causes disturbance on proper delivery of data packets [6- 10]. Without position information of obstacle within the network region, WSN cannot work properly. In large forest area or in the area with small rocks where manual tracing is not possible, the proposed designed system is useful to detect the object which causes disturbance in the network system and configure its boundary almost accurate. The deployment of large scale sensor networks is prevented because of lack of effective protocol support, network spectrum capacity limit, energy consumption, node size and cost. An integrated hardware and protocol suite capable of supporting 1000+ nodes flexible to adjust different requirements

and suitable for inexpensive very large scale integrated (VLSI) circuit implementation is required to realize these sensor network goals [19,20].

Appropriate Sleep scheduling of sensor nodes without harming the network functionality is an accepted and interesting method to reduce energy consumption of dense wireless sensor networks. Energy efficiency is a primary goal for most of the WSN [21-22]. The major sources of energy waste are collision, overhearing, idle listening, etc. These can be minimized choosing an efficient routing and periodic listen and sleep. If nothing is sensed, nodes are in idle mode. Many measurements have shown that idle listening consumes 50-100% of the energy required [23,24]. Pico-net is an architecture designed for low power WSN where sensor nodes are put into periodic sleep for energy conservation. In these schemes, neighboring nodes are synchronized and broadcast its address before it starts listening. This property has been employed for the functioning of the proposed sensor network.

6.2 Literature Review:

In some recent research articles, we find the research works for developing low power sensor nodes for a large wireless sensor network. In the work of Gu and Stankovic, a radio triggered hardware had been used to wake-up a sleeping node. The hardware is energized with the signal received from the transmitter and a significant level of power can be saved. But in this system, the range must be very low and applicable to limited nodes [7].Liang et. al. developed a low power sensor node in their research work using wake-up radio ATA5283 fabricated by ATMEL. The working frequency is about 125 kHz only in the year of 2008[8]. In recent years technology has been developed and more advanced sensor nodes are implemented [146,11,19,20].

Van Der Doom et.al. has developed a sensor node consists of wake-up timer circuit in order to have a power saving approach. They have presented their work with 868MHz frequency of timer circuit and used a microcontroller PIC12F683 to detect the wake-up signal. Another microcontroller ATMEGA128 has been used as node processor which becomes activated in its low power mode receiving the wake-up signal [9]. Renyan Zhou et.al. presented VLSI design of single chip processor architecture of sensor node using 8051 microcontroller. The system clock frequency is about 16 MHz and power dissipation of the

order of 60mW [10]. Aki Happonen et. al. explained the power optimization for a single chip sensor node using a reference design OKI's ML7051 for ARM 7TDMI processor [11].

To capture significant events, monitor the surrounding environment, and to interpret the physical space information with sensors are useful and demanding in several application fields such as disaster management, surveillance, home/power automation, automatic and e-healthcare systems etc. Despite their success, current IEEE 802.15.4 based wireless sensor networks (WSN) have a lifetime measured in weeks or months, which is not suitable for long-lived applications requiring unobtrusive sensing. The radio frequency identification (RFID) technology, recently in advanced stage and enhanced by computational RFID tags with integrated sensors. Recent RFID technology has a number of key aspects like small form factor, zero-power backscatter communication, and standardized identification of tags which make it a promising candidate to complement the existing WSN system.

The integration of communication, computation, sensing/actuation, and storage functionalities in UHF RFID tags have made it more popular among researchers, practitioners, commercial and industrial users/manufacturers. The tag, compatible with the Gen2 protocol, is fully programmable and exhibits a maximum operating range of 12 m. The continuous advancement of technology and requirement of high speed network have provoked the scientists and researchers towards more extensive research on object localization algorithm for large Wireless sensor network. Sensor nodes around the obstacle can detect a coverage hole because there is no neighbor in the direction of the obstacle. To determine the distance of the obstacles from the vehicle a Fuzzy Inference System has been used so that the vehicle could decide whether an obstacle is present in the travelling path or it has to change its direction of travel. In the article of J. Byrne et.al find a Visual Threat Awareness (VISTA) system which detects passive stereo-based obstacles for (UAVs) [12].

In the field of automatic navigation systems, obstacle localization and its avoidance is a well-studied subject. Q. Li, et.al has described the Distributed Object Localization algorithm or DOL algorithm in their article [13]. The success of this algorithm depends upon each sensor being able to sense the presence of obstacles within the network. Wang et al. also proposed a distributed algorithm for boundary recognition in sensor networks using only the communication graph but the algorithm exploits a special structure of the shortest path trees to detect nodes on the boundaries. This scheme is performed without considering the location information, angular information, or distance information thus it may involve a large number

of control messages and collisions. A distributed obstacle localization algorithm was proposed and developed by F. Reichenbach et.al. based on the shadow effects caused by the obstacles. This scheme locates obstacles using only the radio transmissions between the deployed sensor nodes and has no requirement for additional hardware devices [14]. In this scheme, a special deployment of four beacons at the four corners of the sensing field is used. Each beacon having the ability to communicate with all of the sensor nodes in the sensing area is a requirement to obtain a satisfactory performance of the scheme. The sensor nodes are uniformly distributed throughout the sensing field. Statistical methods were used for boundary recognition in wireless sensor networks.

C.Y. Wong et.al has proposed another obstacle avoidance system for a robotic vehicle in which ultrasonic sensors were used to detect obstacles in the vehicle path [15]. Most of the obstacle detection schemes are designed for automatic navigation applications and assumed the use of onboard hardware such as radar, laser, infrared, sonar, cameras, etc. to detect nearby obstacles. The Topological Hole Detection (THD) scheme developed by Funke, is based on an analogy of ripples, created by a stone dropped into a pool, which break on rocks protruding above the pool surface and the obstacles in the sensing field are represented by the rocks, and global beacons are represented by the dropped stones [16].

In the proposed scheme, the global beacons communicate with the entire network with beacon messages and each non-beacon node or sensor node can calculate its hop-distance from each beacon node. The sensor nodes with the same hop-distance from a specialized beacon node are considered to lie on the same contour and the contours are broken at the boundaries of the obstacle in the network field. The Topological Hole Detection scheme relies upon the deployment of multiple and well-spaced beacons within the sensing field, and this increases the deployment cost. In their article, Fekete et al. has proposed the restricted stress centrality as the metric to classify the boundary nodes where the restricted stress centrality of a node is defined as the number of the shortest paths containing this node within a given distance. Thus, to define a good threshold is the most important issue for such methods [17,18].

VLSI design is applicable for almost all types of electronic circuits and systems. It has penetrated several fields and find new applications for new area almost every day. In this respect, VLSI design is a solution to fabricate any system very cost effectively and without

degradation of system performance. Design can be sent to market with minimum requirements and additional features can be added without any change in physical device or system. The research articles by Mark Hempstead et.al. provide a survey of ultra low power processors specifically designed for WSN applications that have begun to emerge from research labs, which require detailed understanding of tradeoffs between application space, architecture, and circuit techniques to implement these low-power systems. The tradeoff between communication and computation places a higher burden on energy-efficient computation [19]. Existing all sensor networks are generally designed with off-the-shelf microcontrollers, such as the TIMSP430 or Atmel ATmega 128L. These processors are typically designed for low-power operation across a range of embedded applications, but these controllers, based on monolithic and general-purpose computing engines are not suitable for the event-driven nature of sensor networks. Such processors do support low-power idle states, which made the entire processor disabled and waking it back up on the next interrupt. This behavior limits the use of these modes in interrupt-dominated, event-driven applications such as wireless sensor networking.

Renyan Zhou et. al. proposes an innovative SoC wireless image sensor node architecture. In their work, the 8051 Microcontroller is optimized and enhanced with more extra components such as DMAC. [10]. Chen Liu et. al. proposed a novel approach for object localization in based on RSSI.[145]. But there is a problem of high cost and interference. Marcos Santana Farias et.al. has described the implementation of a subtractive clustering algorithm in hardware [146].

Marcus Vinicius Carvalho Da Silva et.al. has proposed a multi-objective evolutionary-based mapping of an image processing application on a Network-on-chip or NOC based platform [147]. NOC based is considered the next generation of communication infrastructure. Obstacle detection using stereovision is proposed by Huang in his paper in 2005 [148] and Khan et.al. in 2006 [149]. For low power sensor network design, sleep scheduling plays important role. Energy efficient sleep scheduling technique is described by Jiang et.al. for target tracking in 2008 [150]. Another way of power saving in sensor network is described by J. Ansari using Radio-triggered wake-up signals in 2008 [151].

In Table 6.1, an overview of related work has been attempted to focus.

Table 6.1: An overview of related work

Year	Author	Technology used	Working-freq.	Achievement
2004	Gu and Stankovic [7]	Radio triggered H/W to wake-up sensor node	125kHz	Limited range and nodes
2007	Liang et.al.[8]	Low power Sensor node with wake-up radio ATA5283	125kHz	Low power node with Microcontroller
2008	Ansari et.al. [177]	Telos B sensor node with attached wake-up timer	868 MHz	Low power node with Microcontroller
2009	Vander Doom et.al.[9]	Sensor node equipped with a wake-up circuit and PIC ATMEGA128	862 MHz	801 μ W
2010	Renyan Zhou et.al.[10]	Single chip VLSI architecture with 8051	16MHz	60mW 0.18 μ m CMOS technology
2012	Akin Hopponen [11]	Low power sensor node using OKI's ML7051 LA as reference		210 mW in operation and 2.4 μ W in standby.

From the above literature survey, it is obvious that there are some scopes of work for VLSI Designer. As the WSN based solution is used and getting pervasively deployed in various applications, there is a requirement of long life and low cost adaptive sensor nodes as well as high performance processor for Beacon. The features of infield programming, ability to process high data with a reasonably high speed made FPGA based design very effective and suitable for future WSN based applications. So, being motivated with this scope, an adaptive low power FPGA based sensor node and a high performance processor for Beacon architecture is implemented in this work.

6.3 Realization of a Low power Sensor node processor for Wireless Sensor Network and its VLSI Implementation

In a large Wireless Sensor Network, power efficiency of sensor node is one of the most important factors. Long time operating capability with efficient energy management plays very important role for a sensor node. In this work, the sensor intelligence has been merged with a low power processor model. Sensor node within a single chip has been developed and implemented on a high performance FPGA kit. Xilinx ISE 14.3 simulator has been used to design the processor model in VHDL code. An efficient sleep scheduling with a synchronized timer and algorithm to achieve optimum power efficiency has been adopted in this design. Realization up to RTL schematic level has been performed and results power efficiency of almost 90% compared to commercially available microcontroller based sensor node.

6.3.2 Design Metrics:

For a power efficient Wireless Sensor Network, designing of a sensor node faces some challenges like: it requires a quite large memory and large bandwidth. It should have the high computational ability along with relatively low power consumption.

So, to develop a low power sensor node processor module some important design metrics should be adopted. These are as follows:

- To develop protocols to keep it as simple as possible to maintain power consumption.
- In order to minimize the power consumption, size and cost, minimum hardware should be involved in the design. Hence design should be optimized.
- Reduction of circuit complexity to a minimum level is another challenging requirement.
- Sensor node must be cheap; hence data storage also should be a minimum.

To meet all these challenges and requirement, an approach has been attempted here.

6.3.3 Design and Implementation:

6.3.3.1 Functional Details of a sensor node

Fig.6.2 describes an overview of the operational flow chart for a typical sensor node within a wireless sensor network. The centralized control is performed by Beacon, the specialized sensor network station with high communication and processing capability and

own GPS system. When a data packet is to be transmitted from beacon, it first searches the sensor node within its range and check whether the node respond or not. Because, it is usual that a sensor node may be demolished, lost or damaged by any reason. So, before transmission, response is checked. If beacon receives 'ACK' from neighbor node, it transmits the data packet in a specific format shown in Fig.6.3:

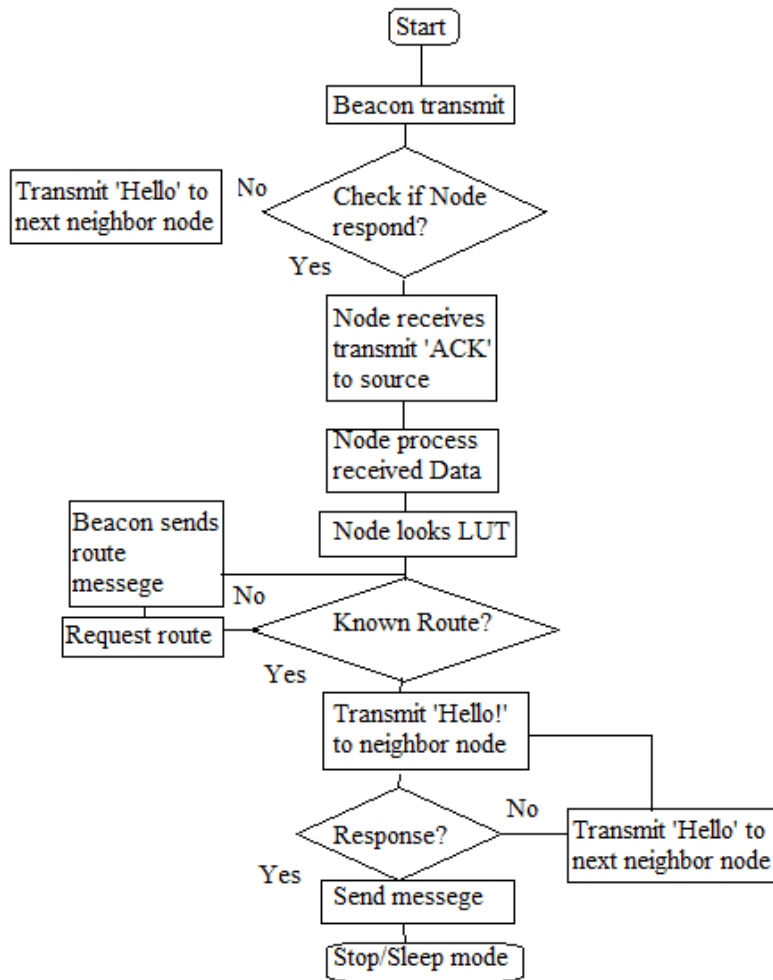


Fig. 6.2: Flow chart for the basic node functions

Source Address Beacon's Identity/ X,Y position	Request ID Counter	Destination Address	Information/ Data packet	End signal
--	-----------------------	------------------------	-----------------------------	---------------

Fig.6.3 Data format transmitted by beacon (24 bit)

Each node maintains a LUT of route information for specific destination. But if for any reason, the path is changed, it sends a request to the beacon to send the new route information or it decides to avoid delay.

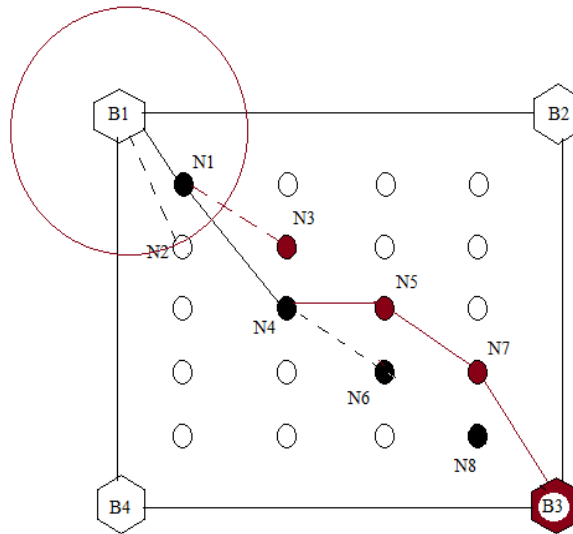


Fig.6.4 A Typical sensor network routing

Fig.6.4 gives an idea about the node deployment and routing path for data packets from source to destination within a sensor network. In the given example, beacon B1 has two sensor nodes (N1 & N2) within its transmission range shown as a circular boundary. It receives response from N1 only if N2 is dead or does not respond. For destination B3, if the node has a LUT of routing information as [N4, N6, N8, B3], and N6 is lost, the modified routing should be transmitted by Beacon as [N4, N5, N7, B3]. So, the node first looks into its LUT for known routing path else send a 'routing request' to the source, B1. Before transmitting the data packet every sensor node transmits a 'Hello' signal to its neighbor node to check whether it is in active mode or not.

6.3.3.2 Sensor Node Functional Diagram

The processor is the controller and the heart of the sensor node. In Fig.6.5 we observe the other important components or architectural details of a typical sensor node. The processor performs several tasks, like: process data and controls the functionality of other components in the sensor node.

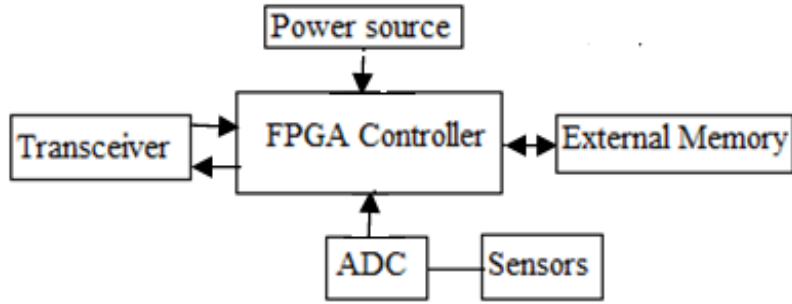


Fig.6.5 Architectural diagram of a typical sensor node

External memory is not necessary for all cases rather on-chip memory serves the purpose very well in most of the usual cases. The sensor nodes consume power for sensing, processing and communication purpose, but power consumption should be extremely low or as less as possible. Currently available sensor nodes are able to renew their energy from solar sources, temperature differences or even vibrations.

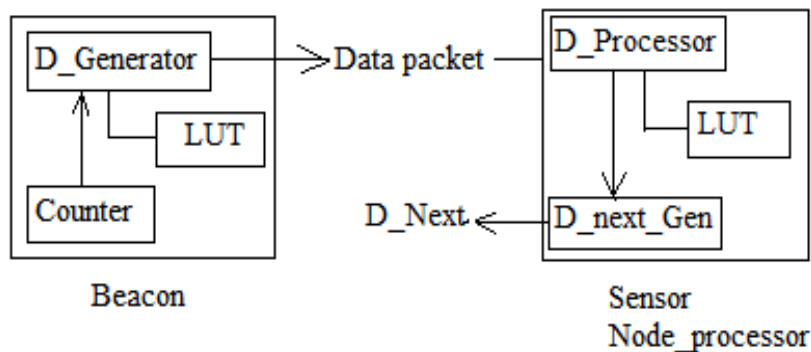


Fig.6.6 Operational Block diagram of a typical sensor network (Beacon & Node)

In Fig.6.6, a simple operational block diagram explains the function of a typical sensor network. Beacon generates a data packet as shown in Fig.6.3 and transmits to the nearest node, In order to generate the data packet, the processor requires a counter and a look-up-table of different parameters like, routing path information or node information within its network zone. On the other hand, each sensor node processor consists of a data processor, a LUT of routing/other node information and a modified data packet generator which keeps the original information unchanged and is transmitted to the next node coming in the routing path.

6.3.4 Hardware Implementation:

Considering the design metrics and challenges for low power sensor node design, a synthesizable model of low power sensor has been designed, implemented and tested in the Xilinx ISE 14.3 environment here. High syntax hardware description language VHDL has been used to design the processor for sensor node. Suitable test bench simulation has been performed using Xilinx simulator. Synthesis and implementation is performed using Plan Ahead tools and obtain the optimized RTL schematic view of the processor. The power and delay analysis reports the performance of the processor. The Advance HDL synthesis report gives the hardware requirement of the optimized design. In order to verify the real time operation of the processor, the design has been downloaded into the high performance Virtex-7 FPGA board Kintex-7.

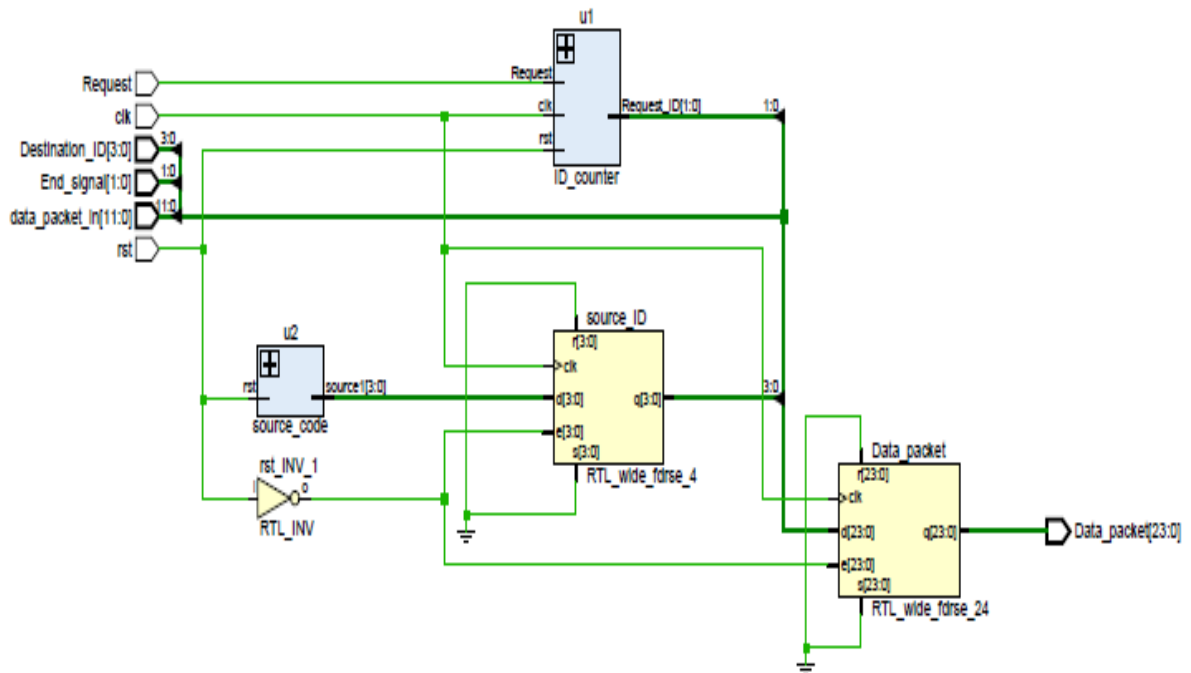


Fig.6.7 RTL schematic view of a typical beacon processor of a sensor network

RTL schematic diagram of the beacon processor is shown in Fig.6.7. ID of source and destination beacon is generated from code_generator block; one request_ID counter and a data assembler block perform the data frame generation from the beacon processor. On the other hand, a sensor node is small enough with the minimum cost processor. The nodal processor first checks the destination and looks at the look-up-table for routing path. If the destination is unknown or routing path is unknown, it sends a 'request' to the source beacon.

Once it gets the information that to which node, it has to send the data packet, it transmits the data packet without any alteration.

In Fig.6.8, RTL schematic of the nodal processor has been shown.

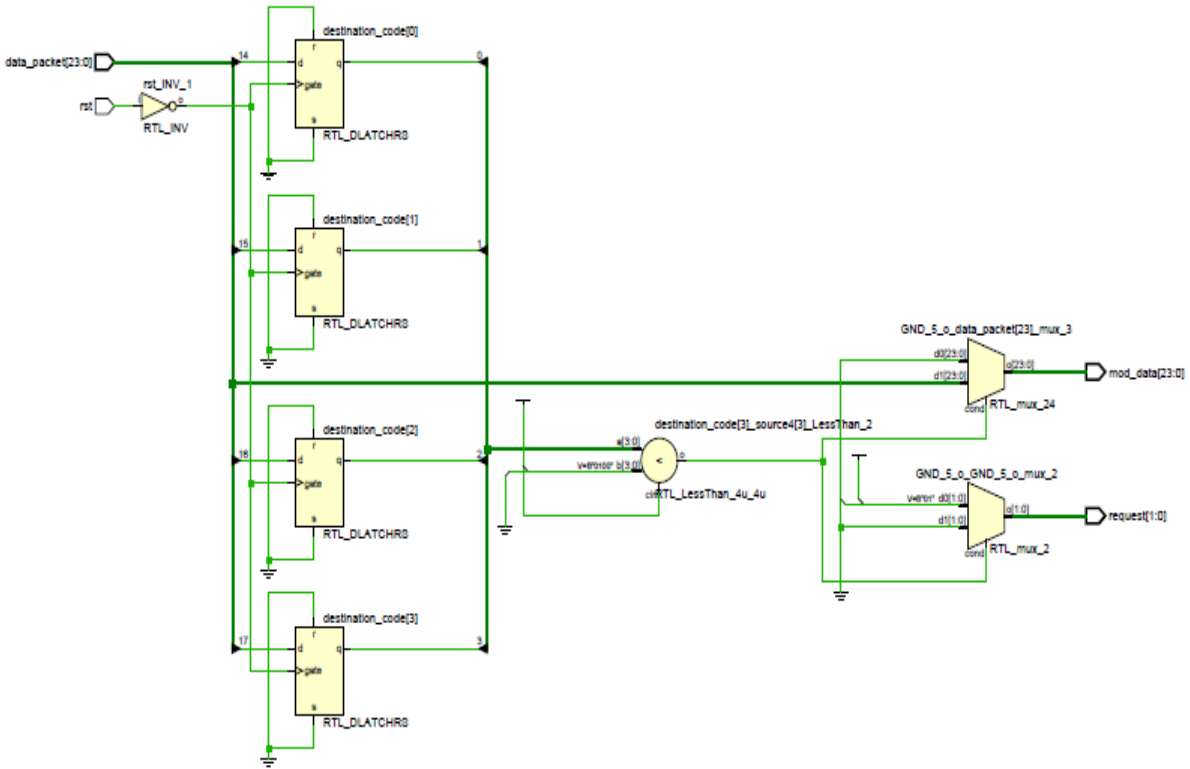


Fig.6.8 RTL schematic view of a typical sensor node processor of a sensor network

The node consists of 11 latches thus 20 IOB Flip-Flops to perform its data frame access and retransmit to the next node. The simulation results of the Beacon and the node processor has been performed using suitable test benches. The test bench used is in 'ns' range. Fig.6.9 & Fig.6.10 shows the test bench simulation result of Beacon processor and node processor respectively.

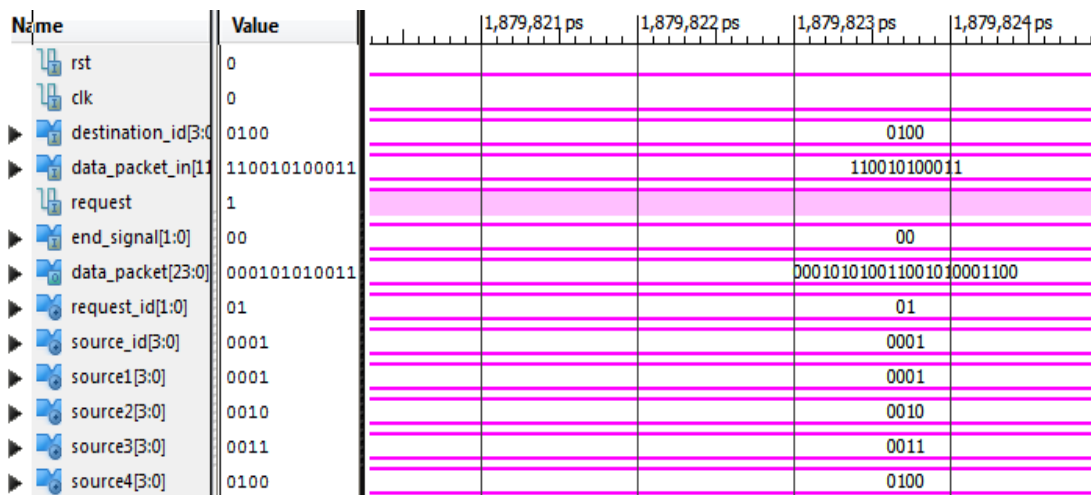


Fig.6.9 Test bench simulation of the beacon processor

From the test bench wave form in Fig.6.9, we observe that data packet of 24 bit has been generated including all the desired information like: source id, destination id, etc. In this particular example, the source is 'source1' and destination is 'source4'. An 'end_signal' of "00" has been provided in order to complete the data packet transmission process. If the route is new, the 'request' port becomes 'high' and transmitted to the Beacon, so that it can provide the routing information to the sensor node. If the destination is known or the node posses the record of previous route, it just works as a buffer and retransmit the data to the next node.

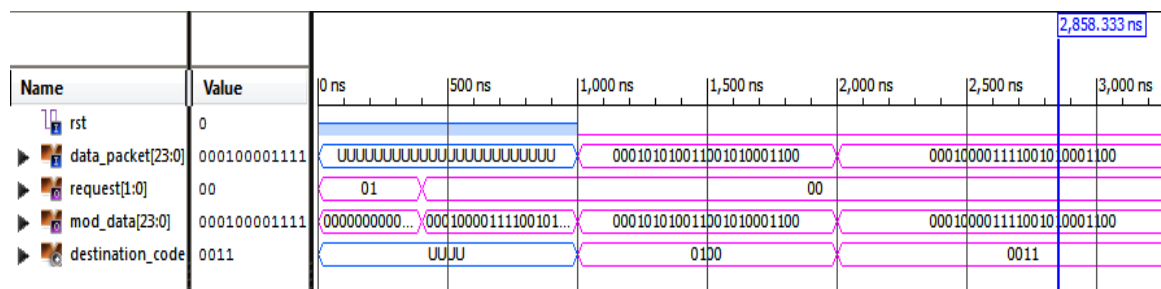


Fig.6.10 Test bench simulation of the sensor node processor

In the test bench simulation waveform of sensor node processor, in Fig.6.10, we observe that if the destination is unknown, request = '01' and transmitted data is 'nil'. But when the destination is known, (here it is source3 and source4) node can identify it in its LUT and transmit the data packet to the next node. The simulation results of sensor node processor and beacon processor assure the effective operation of the processor with appropriate test

bench wave form. Successful Synthesis of any module provides the RTL schematic and technology schematic waveform of the synthesizable module in VHDL code. The Advance HDL synthesis report, device utilization chart and analysis of delay and power are obtained and shown in Table 6.2. Selected Device is Kintex 7 of the series: 7k325tffg900-(speed grade-2)

In Table 6.2, a device utilization report is listed. The circuit processing time delay is in the order of 1.260 ns. On-chip static power consumption by the processor is only 212 μ W with a quiescent current in the order of only 127 μ A. This high speed and low power node processor is suitable for long life sensor network system.

Table 6.2: HDL synthesis/Device utilization summary [Node_Processor]

Parameters	Numbers
1-bit latch	5
4-bit comparator	1
Multiplexer	1
Slice registers	4
Slice LUTs	25
LUT Flip Flop pairs	29
Unique control sets:	2
IOs	51
IOB Flip Flops	20
BUFG/BUFGCTRLs	1
Delay	1.260ns
On-Chip Static Power	212 μ W
Quiescent Current	127 μ A

6.4 Design and VLSI Implementation of Power Efficient Processor for object localization in Large WSN:

The presence of multiple obstacles in the real deployed geographical area may hinder the effective operations of large scale Wireless Sensor Network in terms of significant disturbance in proper routing, increased delay in data transmission and increased energy consumptions. To overcome this problem, a novel pulse mode object localization algorithm and its VLSI implementation for designing the sensor node processor is proposed in this article. The algorithm supports distributed and energy efficient sleep scheduling with periodic synchronization and reconfigure the routing scheme that can be used to extend the lifetime of the sensor network. The algorithm is made power efficient by using pulse mode operation. It is a high performance sensor node processor with an overall power consumption of 0.012mW in active mode with a dynamic current of 1.27mA at the working frequency of 1536MHz. The algorithm is verified using MATLAB for different possible obstacles and percentage error has been calculated for each case. The hardware of this sensor node processor has been realized using ISE 14.3 simulation tools and emulated in Virtex-V prototype Field Programmable Gate Array kit.

6.4.2 Sensor Network as Assumed in this work:

The topology of sensor network assumed for the proposed protocol has been described in Fig.6.11. Here four beacons are working at four corners of almost a rectangular area of interest. It was observed that without obstacles, the network will work properly. But in the presence of an obstacle like large hill as shown in the figure, the visibility of surrounding network changes, in turns radio wave communication may be blocked and thus induce significant problems.

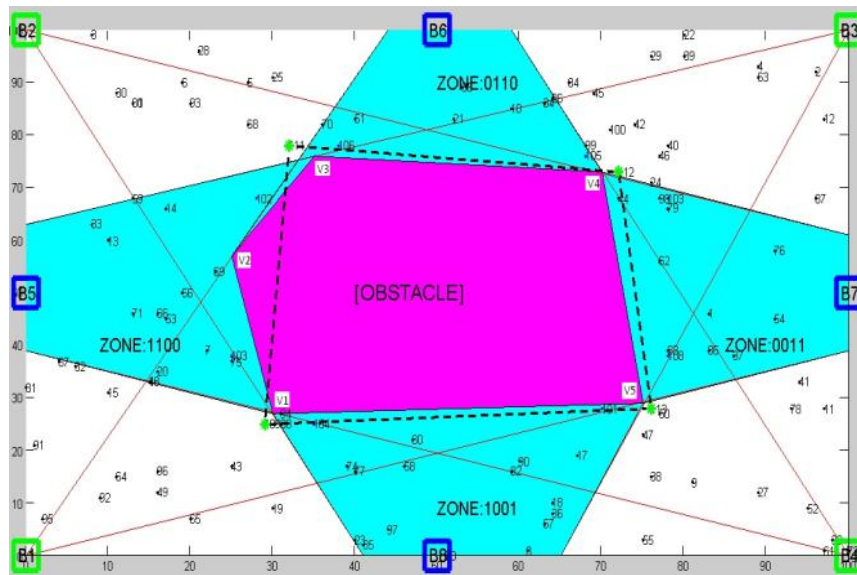


Fig.6.11 Network Topology assumed in this work

In the network topology, the nodes are randomly distributed throughout the area and a small number of special nodes, called beacons are placed in a regular manner, so that they control the total area by reconstructing the routing information. This specialized network nodes or beacons know their exact position by means of Global positioning system (GPS). They also have some information about themselves like identity, transmission range etc. This information is broadcasted by each beacon to other nodes in the form of a message. The other nodes calculate their position details and transmit with low transmission range to neighbor nodes. In this case, position is determined in the probabilistic way using region code determination [143,144].

The region code 'Ci' is a four bit number indicating whether the node is receiving message 'mi' from the four beacons or not. If any of the three region codes intersects it can consider the point as a corner (approximate) of the obstacle, which are named as virtual corner. Using only four nodes it can't process any corner of an obstacle, which is cleared in Fig.6.11. For proper processing of the structure or boundary of an obstacle within the sensor network region, it has considered eight beacons, but all the eight beacons need not to work at a time. To save power, alternate four corner beacons operate at a time using train of pulses to achieve the ultimate goal.

6.4.3 Considerations for the experimental implementation of the proposed algorithm:

- a) Each Beacon consists of the proposed processor, which process the data received from the nodes.
- b) According to the received data, i.e, position of the obstacle, the processor helps the Beacon to reroute the path.
- c) Sensor nodes are randomly distributed throughout the network area, with the help of helicopter or other means and it is assumed that they are static nodes.
- d) Initially, it has considered the object is a static one to establish the network and functioning of sensor nodes and processor.
- e) If any other obstacle like new building arises, the system will automatically reroute its transmission path.
- f) The shadow effect has been considered to detect the obstacle.
- g) Any dynamic obstacle is not considered because it is not a long term obstacle in the network path, but if there is a movement of an obstacle which retains within the network can be detected and each time the beacon will receive new data and reschedule the routing for proper functioning of the network.
- h) The periodic sleep and listen of Beacons and sensor nodes have been introduced, so collision and overhearing can be reduced saving energy. [150]
- i) It is applicable for dense forest where human intervention is almost impossible but signal transmission and establishment of sensor network is required to detect any suspicious object or arms or other.
- j) It is also applicable for large hilly area, abandoned places and areas under monitoring.
- k) Once the network is established and sensor nodes store the information of other neighbor nodes, communication starts without disturbance, but if there is an obstacle, it is immediately detected and beacons reroute the transmission path.
- l) The distance between each sensor node and its neighboring nodes can be obtained using the Received Signal Strength Indicator (RSSI) technique [145].

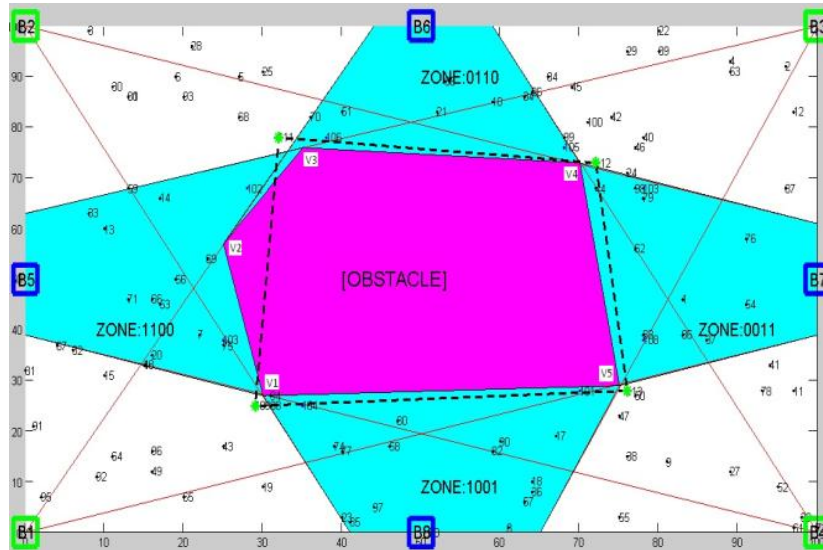


Fig.6.12.Network with image/obstacle; Different region codes, virtual corners and the estimated position of object

In Fig. 6.12, the corners of the object are named as V1, V2, V3, and V4 & V5. It is obvious that each corner is a meeting point of three different regions. Region codes $C_i = \{c_4, c_3, c_2, c_1\}$; for example, the region '0110' gets message from only B2 and B3. Beacons B1 and B4 are in the shadow region, so no message from these two beacons. Now, according to Distributed Object Localization (DOL) algorithm [13,14,15], the nodes transmit a response with C_i , and V_i . If the node is a virtual corner, $V_i = '1'$ otherwise '0'. After receiving responses from all sensor nodes the beacons construct an approximate figure and position of the object, then the rerouting becomes easier and the beacons transmit appropriate routing information.

In the figure, it is observed that the corner V2 is unidentified by the beacons. Similar points can also remain as unidentified which may cause a disturbance to the effective working of the protocol. To overcome such problem of unidentified corner nodes, the proposed algorithm so that the set of beacons become active for certain time duration, i.e.20 sec and go to sleep mode after that i.e.40 sec and process the same steps to locate the corner nodes.

In the proposed system eight beacons at 45° intervals have used as in Fig 1 where B1, B2, B3 and B4 form one set of beacons and B5, B6, B7 and B8 form the other set. After

each interval of 40 sec, one set is active for 20 sec and the other is in sleep mode. So, the pulse mode of operation is adopted which in turn makes it a power saving algorithm. V2 and similar corners can also be identified. In this proposed algorithm, this feature is added with the beacons to achieve an approximate image of the object. In the above figure it is also observed that the estimated image or position of the object as detected by only four beacons, B1, B2, B3 and B4.

6.4.4 Proposed Algorithm:

Based on the discussion, the region code and virtual corner determination are the primary criteria of this Distributed localization algorithm. The sensor network is consisted of many small sensor nodes deployed in an ad hoc fashion. The large number of nodes also has the advantage of using short range multi hop communication instead of long range to conserve energy. All nodes communicate with neighboring nodes first and each node maintains a schedule table and stores the neighbors' location.

Algorithm:

Step1: A set of four beacons B1, B2, B3 and B4 broadcast the relevant parameters like position, transmission range, identity etc. as a data frame, m_i . other set of beacons are inactive during this time until the 'rotate' signal is high.

Step2: All nodes receive ' m_i ' from beacons.

Step3: All nodes calculate their region code ' C_i '

Step4: All nodes transmit ' C_i ' with short transmission range.

Step5: The nodes receive ' C_i ' of neighbor nodes.

Step6: The nodes then calculate whether it is a virtual corner or not and sets a signal ' V_i ' high or low.

Step7: Now the nodes transmit a data frame including the region code ' C_i ', transmission range and ' V_i '.

Step8: Active beacons receive the message from all nodes and determine the localization of the obstacle.

Step9: Active beacons transmit the appropriate routing information.

Step10: Wait for predetermined time period 't'.

Step11: after completing the operation, 'Rotate' signal becomes high and active beacons change their state and become inactive and the other set of beacons (B5, B6, B7 and B8) becomes active for the next time duration,

Step12: Repeat the steps from step1 to step10 again and locate the unidentified corner nodes.

Step13: Construct the object image and approximate position.

Step14: go to step1.

According to our design, beacons have a data frame 'mi' generator block and a data 'N' processor (received feedback from other nodes) to identify the corner nodes and their region code. Other than these two blocks beacons are specialized sensor nodes with special processor. On the other hand, the other sensor nodes have three operational blocks. 'Ci' generator block receives messages from beacons, and generates own region code 'Ci'. The 'N' data generator generates data frame 'N' which consists of 'Ci', low transmission range and 'Vi'. Initially, $V_i=0$, and the 'N' data processor block. Now, the data 'N' data processor receives 'N' from other nodes, process the data to get the 'Ci' of other nodes using which the data 'N' generator sets the value of 'Vi' finally. So the overall process has a timing delay to start functioning properly. After this delay or wait time, beacons get the message from all nodes and finally tune the proper routing information. The most significant feature of the proposed algorithm is its power efficiency.

As the beacons are operating in pulse mode, they remain in sleeping mode for a prolonged period compared to their 'on' period during their total investigation time.

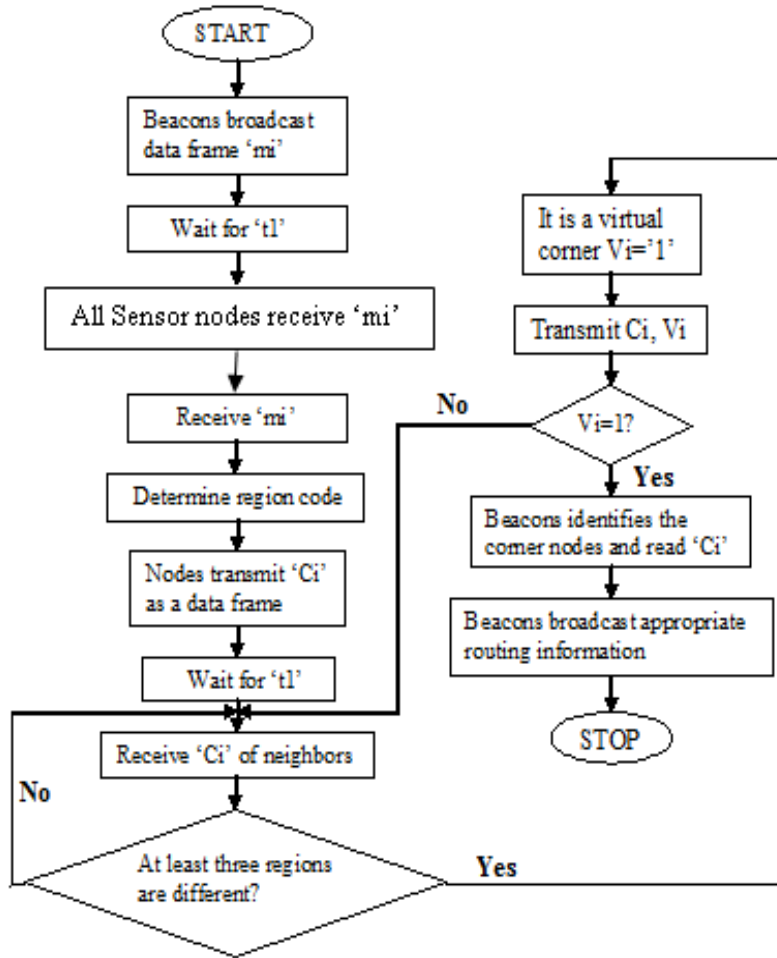


Fig.6.13. Flow chart showing algorithm

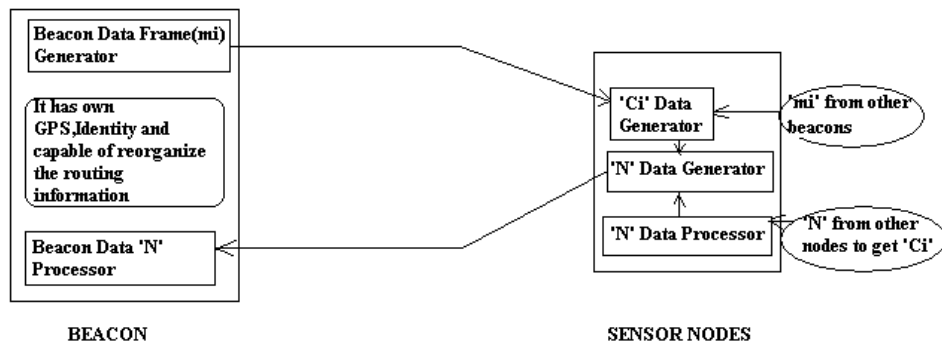


Fig.6.14 Operational block diagram

Fig 6.13 shows the algorithm flow chart and the operational block diagram of the total network shown in Fig 6.14. The operational block diagram describes the basic operation of beacons as well as other sensor nodes.

6.4.5 Designs and Implementation:

The proposed pulse mode object localization algorithm has been simulated in the Matlab environment. According to the topology, B1, B2, B3 and B4 will be activated first to detect the object as shown in Fig.6.15 and in Fig.6.16 it is observed that the area detected by beacons B5, B6, B7 and B8.

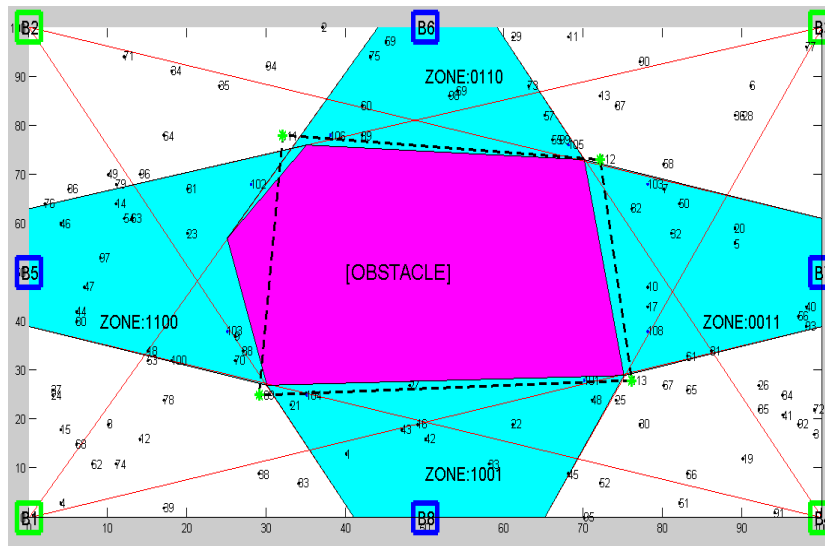


Fig.6.15 Detected obstacle area by B1, B2, B3 and B4

In the first case, Fig.6.15, an area of about 2131.00 sq. units is detected whereas the original area is 2057.50 sq. units. So, the percentage error of area detection is almost negligible (0.0357% only).

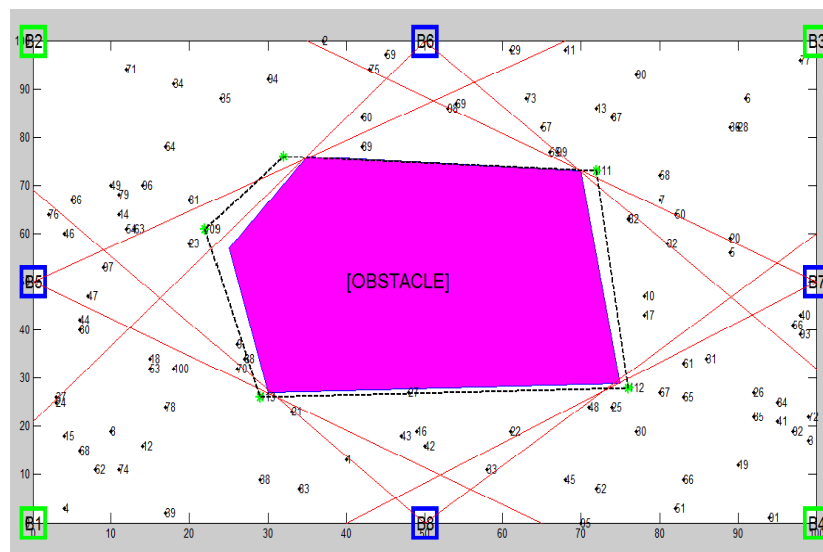


Fig.6.16 Detected obstacle area by B5, B6, B7 and B8

But in that case, one corner of the obstacle has been missed. This problem is solved in the second round of activation, when beacons B5, B6, B7 and B8 are active. In Fig.6.16, it is observed that the missed corner has been detected and coverage area for obstacle is now more than before. Now the obstacle area is about 2293.5 sq. units and error is yet very low (0.1147% only). We have simulated our algorithm for other figures also to verify the detection efficiency.

After satisfied results obtained from MATLAB simulation, hardware level design of the processor is performed for beacon and simulation. Different operational blocks as per required conditions have been designed as shown in Fig 6.14. The designs in VHDL code are simulated using Xilinx9.2 ISE simulation tools. After successful simulation the synthesizable module of the processor is achieved and implemented in the Virtex®-5 FPGA to check the performance of the processor. Virtex®-5 FPGAs use CMOS Configuration Latches (CCLs) to enable configurable interconnects between routing lines and logic cells. The simulated output of each block is described in the form of test bench (ns) simulation.

6.4.5.1. 'N' data generator:

This is one of the operational blocks of sensor node which collects information from neighbor nodes and generates a data frame 'N' of 9 bit and transmit.

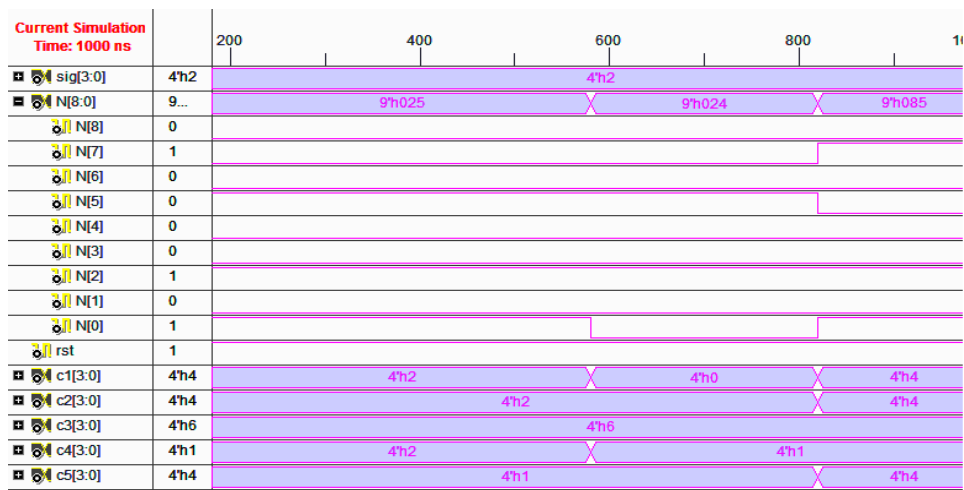


Fig.6.17 Output of the nodal generator

In Fig 6.17, the output of the nodal data generator or 'N' data generator block of the sensor node end is observed. 'N' is a 9-bit data frame, where N(0) refers to the virtual corner

'v', N(1) to N(4) denotes the 4-bit low transmission range and 4-bit region code 'Ci' is referred to the next. When at least three region code 'Ci' are different, it denotes a virtual corner, 'v'=1' otherwise 'v'=0'; So, from the Fig.6.17, it is observed that, N(0) is high, i.e level '1' when at least three Ci are different and the data frame is generated including all information. The structure of the data frame is given in Fig 6.18.

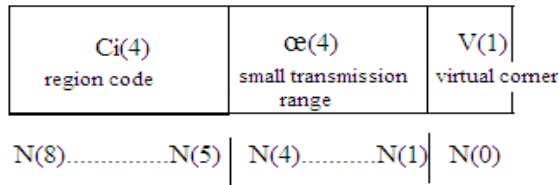


Fig. 6.18 Data frame 'N'

6.4.5.2. Data frame 'N' processor

This is another operational block present in both beacon and sensor node which decodes the information store in the data frame 'N'. In case of beacon, if N(0)=1' then only the region code of sending node is decoded to mark it as a corner node and a reset signal becomes high to enable the beacon to reconfigure the routing protocol. But in case of sensor nodes each time the region code is being read and fed as input to the 'N' data frame generator.

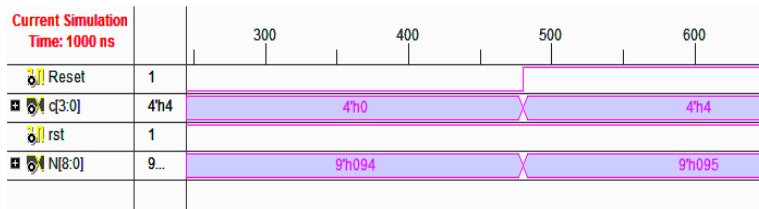


Fig. 6.19 Output of N_processor

When the sensor nodes receive 'N' data frame from other neighbor nodes, it needs to process the data frame to get the information within it so that it can take decision accordingly. Initially 'v'=0', the node decodes the region code of other nodes and modify the N(0) and retransmit the data frame.

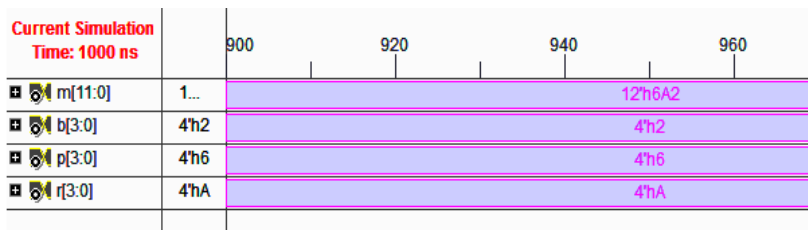


Fig. 6.20 Output of 'mi' generator

6.4.5.3. Beacon data frame ‘mi’ generator

This is the most important data generator block of the beacon. The data frame includes the information like p, the position of the beacon as per GPS; r, the transmission range; Bi, the beacon’s identity. The data frame structure is shown in Fig 6.18. All the information including these, the message ‘m_i’ is generated and transmitted to all nodes from the beacon end. Now it is obvious that all the nodes do not receive the transmitted data frame due to the presence of obstacle. If receiving data is denoted by ‘1’ and not receiving is denoted by ‘0’ we can construct a region code as shown in Fig. 6.18.

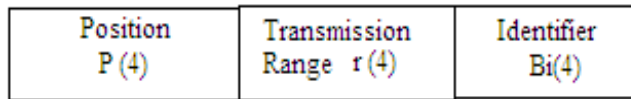


Fig. 6.21 Structure of 12 bit ‘mi’ data frame

6.4.5.4. Region code ‘Ci’ generator

This is one of the data generator blocks of the sensor node. Here, inputs ‘m_i’, received from the beacons. According to the received data, code ‘c’ is generated by this module. ‘c’= “0000” if the node gets no response from any of the four beacons. ‘c’=”0011” if the node get responses from only beacons B3 and B4 and so on. In Fig 6.22, the output of the code ‘c’ generator block is shown. The bits m1, m2, m3 and m4 denote the data frame transmitted by B1, B2, B3 and B4 respectively. When m1 and m3 is receiving, code c = “1010” but when m4 is also received, c = “1011”. After successful simulation of each block for both the beacon and sensor node, the total system is designed working together with required time delay for processing the data frame and different operation.

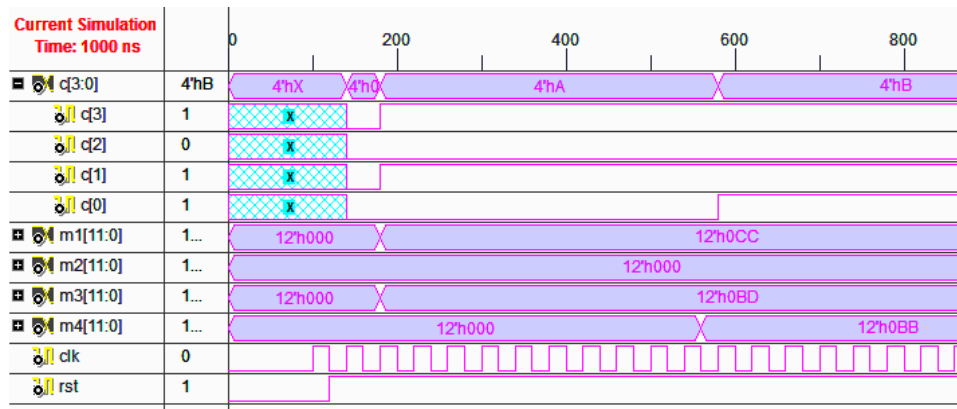


Fig. 6.22 Output of code ‘c’ generator

6.4.6 Efficiency Calculation:

a) *Power efficiency calculation:*

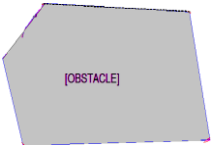
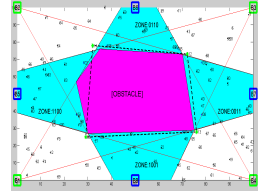
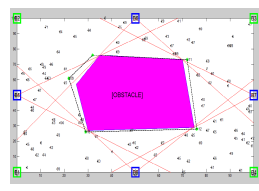
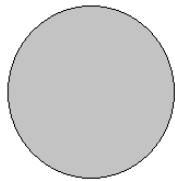
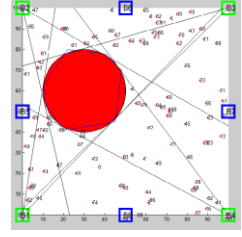
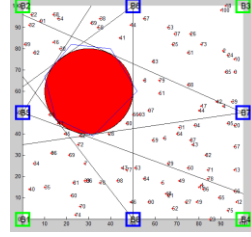
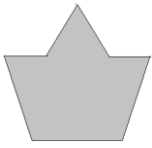
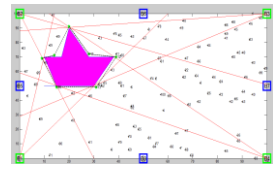
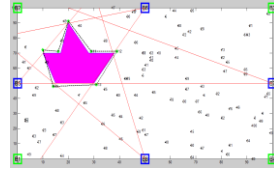
Eight beacons have been used in this system, out of which only four is active at a time. As they have highly directional antenna, a node can be detected within a fraction of a second. From the simulation result, the total processing time for one complete cycle of operation takes about 340 ns after giving wait period, then switch over to another four set of beacons. So, the time taken is $2 \times 340 \text{ ns} = 680 \text{ ns}$ only. Within this time span, the purpose to detect object or to determine its image is fulfilled. Hence, there is no need to use the beacons full time active, and a huge power is saved. Power consumed by a single processor is 0.012mW in active mode with a dynamic current of 1.27mA according to the experimental result. This sleep scheduling of beacons and the FPGA based processor made the proposed system *power efficient*.

A controlling timer has been designed to synchronize the overall process. The 'on time' and 'off time' can be predetermined according to the requirement of the application. For an example, if we keep 20sec 'on' time and 40sec 'off' time, we use only 20sec 'on' time out of 60sec. So, the active state of the beacon is for only $(20/60) \times 100\% = 33.33\%$ of total investigation time. Therefore, power will be saved by almost 66.67%. As per the simulation result, two sets of beacons will be activated for only 680ns. If we adopt only this time limit, the consumption of power will be effectively minimized.

b) *Obstacle area detection efficiency calculation:*

To evaluate the *obstacle area detection efficiency* of the proposed processor, three different figures are taken into consideration. This algorithm is simulated and verified for these three figures and presented the result in the tabulation format in Table 6.3. From Table 6.3, it is observed that the more actual area is achieved considering both set of beacons (more detected virtual corner) each time. More obstacle area detection provides significant reduction in the percentage error, providing enough information to beacon. So, the Beacon may adopt a suitable routing path avoiding undesirable delay. In case of a circular area, it is observed that, the detected area is less than the actual area but it is very little and may be ignored.

Table 6.3: Obstacle area detection efficiency calculation

Figure	First round detection case 1	Second round detection case 2	Percentage error= (Detected area-actual area) / actual area
 <p>Actual area= 2057.50 sq.ft.</p>	 <p>Detected area=2131.00sq.ft.</p>	 <p>Detected area=2293.50sq.ft</p>	<p>Case1: 0.0357%</p> <p>Case2:0.1147%</p>
 <p>Actual area= 1256.63 sq.ft.</p>	 <p>Detected area=1133.00sq.ft</p>	 <p>Detected area=1186.00sq.ft</p>	<p>Case1: 0.056%</p> <p>Case2:0.098%</p>
 <p>Actual area= 540.00 sq.ft.</p>	 <p>Detected area=655.00sq.ft</p>	 <p>Detected area=647.50sq.ft</p>	<p>Case1: 0.213%</p> <p>Case2:0.199%</p>

6.4.7 Synthesis Report:

After successful test bench simulation of the processor, we performed the behavioral synthesis of the design. The behavioral synthesis of a design is the process of generating a register-transfer level (RTL) design from an algorithmic behavioral specification which is written in hardware description language or VHDL code. In particular, the behavioral synthesis process of a design constructs a structural view of the data path and a logical view of the control unit of a circuit. The data path consists of a set of interconnected functional units (arithmetic, logic, memory and registers) and the steering units (multiplexers and busses) while the control unit sends signals to the data path to schedule the appropriate sequence of operations in time.

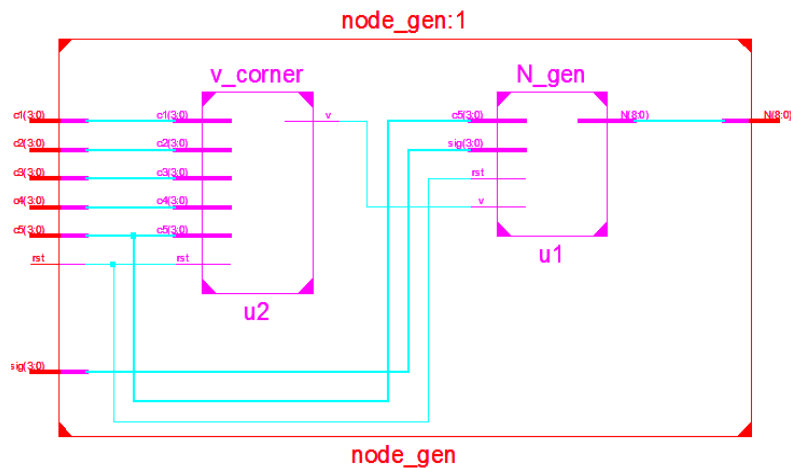


Fig. 6.23 RTL schematic of Node_gen

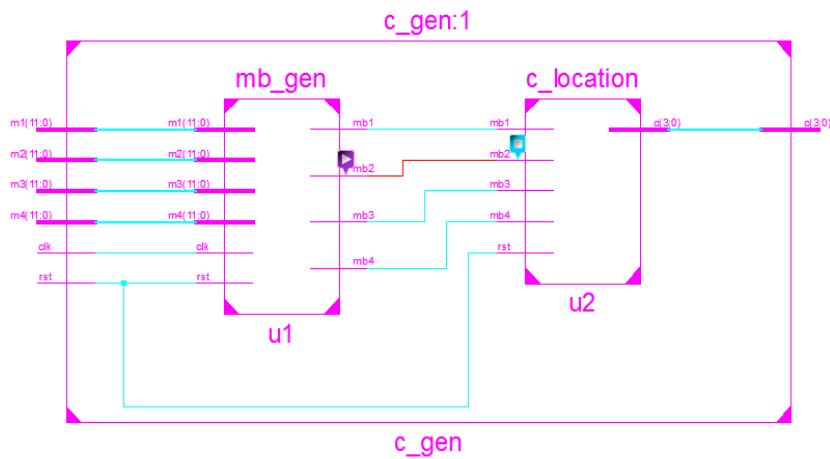


Fig. 6.24 RTL schematic view of code generator

After successful synthesis we obtain the RTL schematics of each block module as well as the final processor block which incorporates all the necessary blocks. Some RTL schematic views are given for reference, i.e. the RTL schematic of nodal data generator shown in Fig. 6.23. This module consists of v_corner and N_gen modules. Similarly, Fig. 6.24 shows the RTL schematic view of code generator.

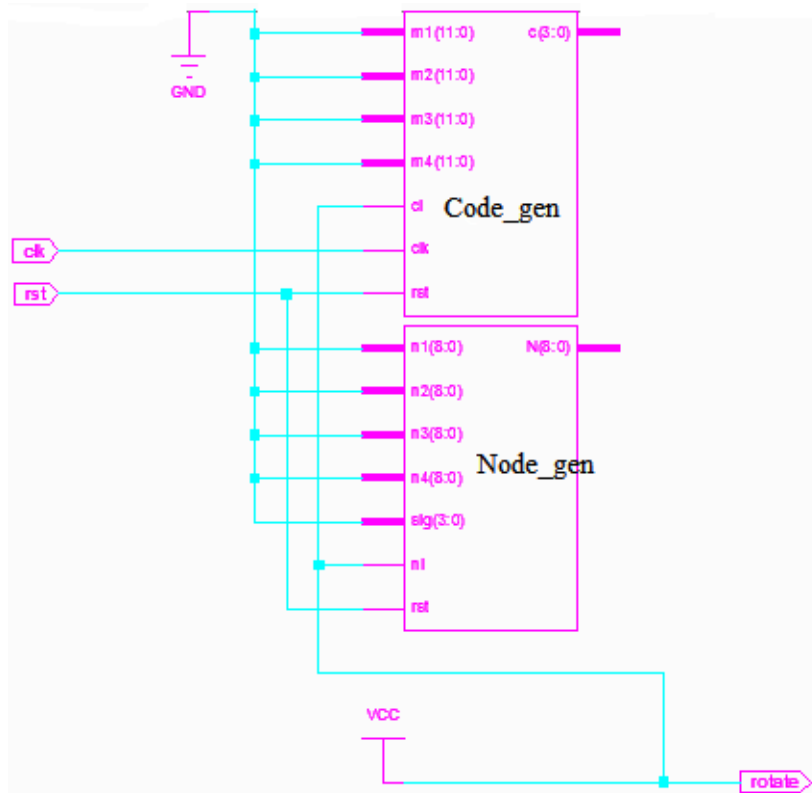


Fig. 6.25 RTL schematic view of the processor including code generator, 'N' data generator with control clock

In the Fig. 6.25 RTL schematic view of the processor including code generator, 'N' data generator with control clock, the complete RTL schematic view of the code generator block which consists of two modules named as 'mb_gen' and 'c_location' is shown. Fig. 6.25 shows the RTL schematic view of the final processor incorporated with the code generator, [Code_gen]; 'N' data generator, [Node_gen] with control clock and virtual corner detector modules.

After successful synthesis of the design, the list of hardware requirements, device utilization chart and delay reports of the processor are depicted in Table 6.4. Some of the modules have been considered in these tables. The working of the processor is verified in real environment using the FPGA Virtex5 kit. The control timer that controls the timing synchronization of operational blocks can be designed with appropriate timing according to the application. Moreover, it operates in pulse mode to make the sensor node processor as a high performance and power efficient system.

The presence of obstacles creates an unwanted detour and/or dead ends, thereby distorting the sensor networks and may lead to deploy complex and costly routing techniques. Radio signal shadowing due to its blockage by obstacles can be efficiently utilized for field segmentation which in turn forms little deflected virtual obstacles. In order to relieve these problems, in the present work a power efficient DOL algorithm based processor has been developed. The VLSI implementation of the proposed processor (aimed towards power efficient DOL algorithm) and its hardware realization have been achieved through Xilinx ISE 14.3 simulation tool and synthesized codes are downloaded into the Virtex-V FPGA kit. The same is subsequently verified using MATLAB environment.

Table 6.4: List of hardware requirements, Device Utilization and Delay Report

Advanced HDL Synthesis Report				Device utilization summary	
Components	node_gen	c_gen	sensor node	Node_Processor	
1-bit latch	37	4	41	Number of Slice Flip Flops	4
4-bit latch	8	-	8	Number of 4 input LUTs	16
4-bit comparator	8	-	8	Number of Slices	10
1-bit xor4	8	-	2	Number of IOs	54
4-bit xor2	8	-	8	IOB Flip Flops	16
Flip-Flops	-	4	4	Number of GCLKs	2
12-bit comparator	-	4	4	Delay	2.357ns
				On-Chip Static Power	0.012mW
				Quiescent Current	1.27mA

From Table 6.4, we observe that the Processing speed of the final node processor is very high (2.357ns) as circuit complexity is negligible due to simple hardware requirements. Power consumption is of the order of 0.012mW with a quiescent current of near about 1.27mA only. Low power consumption is the desired goal for sensor node to enhance its life time and thus provide more the efficient sensor networking system.

CHAPTER 7

CORDIC ALGORITHM BASED VLSI DESIGN FOR WIRELESS COMMUNICATION SYSTEM: DPSK MODEM DESIGN AND IMPLEMENTATION

Chapter 7: CORDIC Algorithm based VLSI Design for Wireless Communication System: DPSK Modem Design and Implementation

7.1 Introduction:

Digitalization of data transmission has opened many windows for researchers to develop and implement more efficient data transmission techniques. Realization of the high speed processor for transmitter and receiver with reduced cost has become possible by the grace of VLSI design and its hardware realization using the programmable gate array or high performance and reconfigurable FPGA. In a communication system, FPGA based system realization has attained much popularity because of its easy implementation and adaptive nature to reconfigure or upgrade the system according to requirement without much effort and time. Differential Phase Shift Keying or DPSK modulation has the magnificent features of limited bandwidth, resistivity against interference, multipath fading and almost constant envelope which are very important for mobile communication systems for providing the output in accordance to the customers/designers' requirements [153- 154]. DPSK modulation is favored in communication system because of its high power efficiency and its capability to support high data rate. This work presents the FPGA implementation of DPSK modulator/demodulator incorporating the CORDIC sine-cosine block as a carrier wave generator.

The CORDIC algorithm provides the opportunity to calculate all the essential functions in a rather simple and elegant way, thereby making it well suited for VLSI implementation as its basic operating unit contains only shift, add and subtract. CORDIC module provides a good foundation for the rapid development of Very Large Scale Integrated circuits. A significant scarcity in FPGA resources makes these algorithms easier to be achieved in hardware, and thus meet the requirements of design engineers [156- 159]. The Designers pay more attention to its advantages, excellent performance and it is popularly used in the computing real-time signal processing of high quality requirements, modern software defined communication systems, image processing and so on [160,161].

A power efficient DPSK modem has been implemented using the CORDIC algorithm in VHDL code. Here, CORDIC algorithms are used to generate the carrier in the modulator and to implement the multiplier in the demodulator. Carrier generator on same chip minimizes the effect of noise significantly. The singlechip implementation provides a low power DPSK modem operating with high frequency which is suitable for wireless communication system. The CORDIC algorithm based DPSK modem is found to be a much efficient system in terms of reduced hardware cost, improved performance and included flexibility. Importance of portable FPGA based device for wireless communication system and system on a single chip is now growing rapidly. In this context, proposed modem provides an efficient alternative over a conventional DPSK modem. Real time verification is performed using the Kintex-7 FPGA board. The performance of the proposed modem has been compared with a normal DPSK modem implemented in SDR kit using Xilinx block and Spartan 6 FPGA.

7.2 *Literature Review:*

Jack E. Volder has implemented the basic intelligent COordinate Rotation DIGital Computer algorithm or CORDIC algorithm for multiplication, division, conversion of binary to decimal and mixed radix number systems. It is basically an iterative algorithm, requiring simple 'shift' and 'addition' operations, for hardware realization of basic elementary functions. CORDIC algorithm in rotation mode is used to calculate the sine and the cosine value of an angle. It is assumed that the desired angle is in radians and is represented in a fixed point format. To calculate the sine or cosine value for an angle θ , the y or x coordinate of a point on a circle corresponding to the desired angle is found. After a sufficient number of iterations, the value is calculated [156- 158].

CORDIC algorithm can be used to calculate different mathematical functions. CORDIC block can be used for many high-speed and real-time applications. It is very preferable choice for the system designer to replace the computational overhead with the CORDIC block in order to enhance the speed and performance of the processor [159- 165]. The important goals in the design of a digital communication system are to provide a reliable communication, i.e., achieve a very low probability of error and the efficient utilization of channel bandwidth.

John Stephen Walther generalized the techniques proposed by Volder in order to compute hyperbolic, exponential, logarithm and square root functions [157,158]. Since CORDIC is used as a building block in various single chip solutions, the critical aspects to be considered are high speed, low power, and low areas. To achieve reasonable overall performance and to speed up the CORDIC by reducing its iteration counts and through its pipelined implementation, several algorithms and architectures have been developed. Enhancing the throughput and reducing the latency of CORDIC module, CORDIC block can be used for many high-speed and real-time applications. It is very preferable choice for the system designer to replace the computational overhead with the CORDIC block in order to enhance the speed and performance of the processor [155- 158].

In 2009, author P.K.Meher et.al. have described the versatilities of CORDIC algorithm in their paper, mentioning the 50 years of the algorithm[159]. A parallel double step CORDIC algorithm is proposed by W.Han et.al. Hardware multipliers are replaced by CORDIC algorithm which uses only adder, subtracter, shift register and a look-up-table, thus reducing the complexity, as well as cost of the hardware[160]. Due to high speed, low cost and simple architecture, FPGA based DSP processor accomplished with CORDIC algorithm is a popular choice. A pipelined CORDIC design on FPGA for a digital sine- co-sine waveforms is realized by E.O.Garcia et.al. Pipeline architectures used in CORDIC algorithm reduce the critical path increasing speed and reduced the power consumption effectively [161].

In this present work, we have used CORDIC algorithm as sine/co-sine wave generator and multiplier in a DPSK Modulator model. The Modem is an indispensable part of a communication system. The intelligent design of modem successfully mitigated the basic problems of communication engineering. Performance improvement and realization cost reduction are essential parameters for modem designers. Modems can be classified by the amount of data they can send in a given time period which is expressed in bits per second. Another way, a modem can also be classified in terms of their symbolic rate 'Baud'. For example, the ITU V22 standard, which can transmit and receive four distinct symbols, transmitted 1,200 bits by sending 600 symbols per second (600 baud) using phase shift keying [166].

In the year 2011, author Z.Zhao presented the design and implementation of the BPSK Modem on FPGA. Author has used software defined radio as the experimental platform. Cordic Algorithm is adopted to realize the arctangent phase detector, which is used in place of traditional multiplier phase detector[162]. Here, in BPSK modulation technique, synchronous carrier is needed to generate the carrier and the demodulator requires the copy of the reference signal. But, in case of DPSK, receiver do not need the copy of such reference signal. So, it is found to implement a DPSK Modem more simple way which is the modified version of BPSK.W. Song et.al. also have their work on BPSK modulator-demodulator design and implementation based on modern DSP technology, in the year 2009.

Software Defined Radio(SDR) is the radio in which the properties of a transmitter and receiver, like carrier frequency, signal bandwidth, modulation, and network access are defined by software. So it is a simple software defined or programmable versatile radio, and also suitable for researchers to experiment on the field of communication. Such work we find in the papers by W.Song et.al, Hiroshi Harada et.al.[163- 165]. In 2011, the Optical Society of America published a paper describing implementation of silicon electro-optic Microring Modulator based DPSK modulator authored by K.Padmaraju et.al.[166]. Their experimental demonstration of DPSK modulator successfully validated with BER measurements at 250 Mbps to show the acceptable power penalty. This is ideal for wave guides.

The Multi-core Processors are continue to scale in size, complexity in the field of wireless mobile communication. Furthermore, lower power dissipation and improved scalability at higher data rates motivating researchers for the development of suitable networks-on-chip. In this point of view, our proposed FPGA based DPSK modulator-demodulator using CORDIC algorithm finds its way of acceptability.

7.3 Different Modulation and Demodulation techniques:

There are three important classes of digital modulation/demodulation techniques used for transmission of digital data or digital communication system:

- Amplitude shift keying or ASK
- Frequency shift keying or FSK and
- Phase shift keying or PSK

Among these three techniques, the PSK modulation technique is commonly used for its simplicity, low cost and easy implementation. It has other prominent features, like good spectral characteristics, high spectrum efficiency, strong anti-interference performance, and faster data transfer rate. In case of PSK, the phase change is used to represent the data signal. There are several PSK modulation techniques for data transmission, like Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK), Differential phase Shift Keying (DPSK) etc [167- 170].

The wireless LAN standard, IEEE 802.11 uses a variety of PSKs depending on the data rate required for the application. For example, DBPSK (Differential BPSK) is used for application with the basic rate 1 Mbit/s and to provide a rate of 2 Mbps, DQPSK is used. QPSK is employed where rate is extended to 5.5 Mbps to 11 Mbps. In case of higher speed, BPSK and QPSK modulation is employed. Because of its simplicity, BPSK is appropriate for low-cost passive transmitters, like RFID standards and many other applications [168,170].

7.3.1 BPSK Modulation/Demodulation:

In BPSK modulation technique, the transmitted signal is a sinusoid of fixed amplitude. It is a simple one-dimensional modulation type. The phase of carrier signal changes abruptly by π radian for every transition of binary sequence. In the demodulator, carrier synchronization is very important to recover the baseband signal. DPSK is the modified form of BPSK which eliminates the need to provide the synchronous carrier required to generate the carrier. DPSK is simpler to implement than ordinary PSK since there is no need for the demodulator to have a copy of the reference signal. For BPSK and QPSK, there is uncertainty of phase due to some effect in the communications channel through which the signal passes [168,169]. PSK has a lower probability of error and better performance than FSK. DPSK is comparatively easy, suitable and less error methods [167,168,169]. So, in this article the implementation of DPSK modulator has been performed.

7.3.2 DPSK Modulation/Demodulation:

The Differential phase shift keying technique is facilitated by encoding the binary stream of data using differential code before modulation. According to this modulation technique, there is a probability of bit error. The bit error is due to the fact that DPSK uses only the reference of previous bit. Since this method depends on the difference between successive phases of bit stream, it is termed as differential phase-shift keying (DPSK). DPSK can be significantly simpler to implement than ordinary PSK since there is no need for the demodulator to have a copy of the reference signal to determine the exact phase of the received signal. Differential phase shift keying (DPSK) is a simplest form of phase modulation that conveys data by changing the phase of the carrier wave. For BPSK and QPSK, there is an uncertainty of phase due to some effect in the communications channel through which the signal passes. This problem can be resolved by using the data to change according to the phase [167,168,169]. In the demodulation process again 1-bit delay is used to generate the original binary message. In DPSK, or differentially encoded BPSK, a binary '1' may be transmitted by adding 180° to the current phase and a binary '0' by adding 0° to the current phase. Another variant of DPSK is Symmetric Differential Phase Shift keying, SDPSK, where encoding would be $+90^\circ$ for a '1' and -90° for a '0'.

7.3.3 QPSK Modulation/ Demodulation:

QPSK is sometimes known as 'quadriphase PSK or 4-PSK'. The mathematical analysis of QPSK shows that it can be used to double the data rate of BPSK system, maintaining the same bandwidth of the signal or vice versa. But, QPSK transmitter and receiver are more complicated than that of BPSK [167,168,169]. A QPSK signal is generated by two BPSK signal and to distinguish two signals, two orthogonal carrier signals are used. In the demodulator section, the received signal is multiplied by the carrier frequency. FIR filter is used to recover the transmitted signal. The carrier frequency must be the same as in transmitter. Thus it implies complexity in QPSK modulator/demodulator design and implementation process.

7.4 Cordic Algorithm:

CORDIC is an iteration algorithm of arithmetic calculations. The basic operation performed by this algorithm is a series of addition, subtraction using shift register and look-up-tables. Traditional analog calculator of trigonometric functions, polynomial expansion costs higher and can not meet the speed and accuracy requirements of modern age. Because of its basic operating unit being only 'shift', 'add' and 'subtract', CORDIC module laid a good foundation for the rapid development of Very Large Scale Integrated circuits and solve this problem. These algorithm can be easily implemented into low cost hardware [170-174].

To determine the sine or cosine for an angle θ , the y or x coordinate of a point on the unit circle corresponding to the desired angle must be found. Using CORDIC, we would start with the vector V_0 .

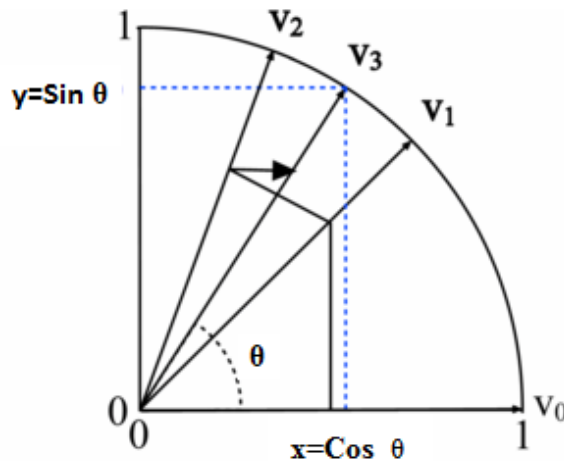


Fig.7.1 CORDIC vector rotation

In the first iteration, this vector is rotated 45° counter-clockwise to get the vector V_1 . Successive iterations rotate the vector in one or the other direction by size-decreasing steps, until the desired angle has been achieved. After a sufficient number of iterations, the vector's angle will be close to the wanted angle θ . For most ordinary purposes, 40 iterations ($n = 40$) are sufficient to obtain the correct result up to the 10th decimal place[171- 176].

In the iterative implementation of cordic algorithm, the generator takes several clock cycles to build a single output. But using pipeline, converts iterations into pipeline phase. Each pipeline stage takes exactly one cycle to complete.

7.5 Proposed DPSK modem module:

7.5.1 Functional Block Diagram:

The functional block diagram of the proposed DPSK modem using CORDIC block is shown in Fig.7.2. The modem includes four basic functional blocks.

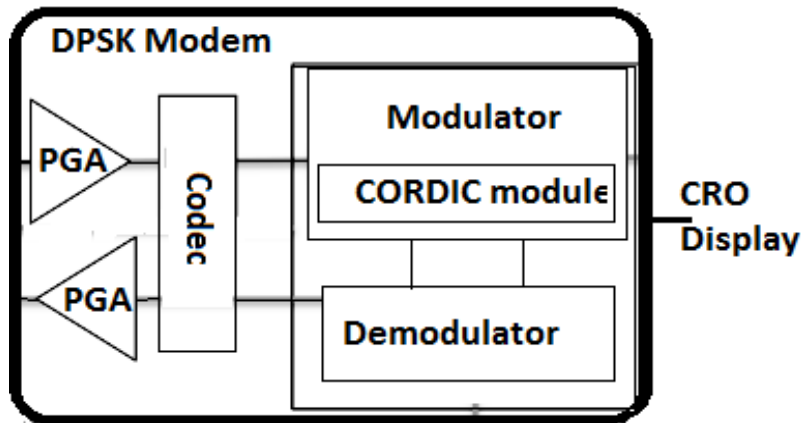


Fig.7.2 Functional Block diagram of DPSK Modem

- DPSK modulator block: The modulator modulates the digital information to be transmitted. The *CORDIC block* acts as the carrier wave generator.
- DPSK demodulator block: The demodulator demodulates the received signal to extract the digital information.
- Codec module block: This is the basic Coder/Decoder block which performs both analog-to-digital conversion (ADC) and digital-to-analog conversion.
- PGA block: It is the programmable gain amplifier module.

DPSK Modulator:

The proposed DPSK modulator is versatile and has sufficient programming facility. Its functionality can be improved or modified according to the requirement. It is also easy to upgrade the system anytime. The use of CORDIC block for wave generation by integrating sequence bit generator has improved the speed of the system. It also reduces the requirement of hardware.

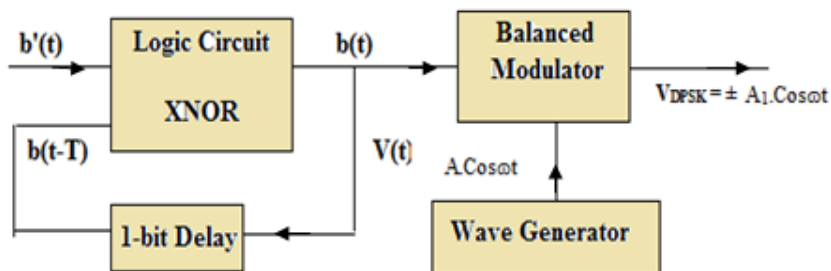


Fig.7.3. DPSK Modulator Block diagram

In Fig.7.3 the block diagram of the DPSK modulator is shown. Where $V_{DPSK} = \pm A_1.Cos\omega t$. According to the modulation technique, $b'(t)$ is the bit stream to be transmitted and supplied to the modulator input which is also a multiplier block using CORDIC algorithm and XNOR Logic circuit block where $b(t)$ is the auxiliary bit message generated from the Logic circuit output.

Cordic module block:

CORDIC algorithm in rotational mode is implemented here to calculate the sine and cosine of an angle. It is assumed that the desired angle is given in radians and is represented in a fixed point format. To determine the sine or cosine for an angle θ , the y or x coordinate of a point on the unit circle corresponding to the desired angle has been found. The CORDIC algorithm requires one shift-add/sub operation for each bit of accuracy [174- 176]. A CORDIC core has been implemented using a single shift-add/sub stage and feeding back the output as shown in Fig.7.4.

An iterative CORDIC block with N bit width, required N clock cycles to accomplish the operation. To obtain sine and cosine values of a given angle z_0 , the structure takes the value of (x_0, y_0) as $(1, 0)$ in the first clock cycle. The control signal for the input registers is provided by a state-machine designed for the purpose. To get an N bit precise output, the structure requires iterating at least N times. Hence, it requires a minimum of N clock cycles to produce the required output. The frequency of the wave depends on the system clock frequency. In this case the frequency of generated sine/co-sine wave is about 1.33 MHz, whereas the maximum clock frequency available is 276.60MHz.

In Fig. 7.4(a), the CORDIC module is shown which has been implemented in this work as the basic building block and Fig. 7.4(b) shows the pipeline array of the CORDIC modules.

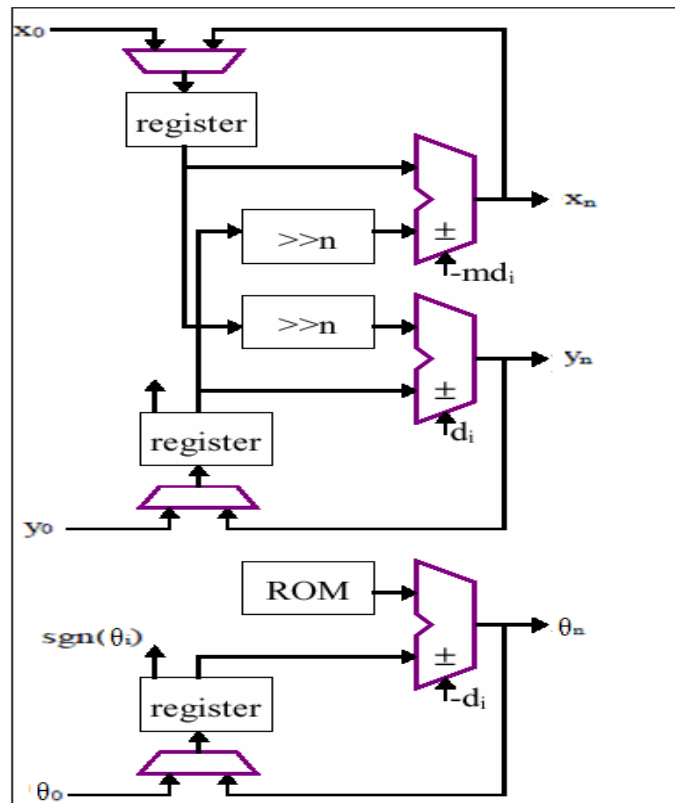


Fig.7.4(a). Basic CORDIC module block diagram

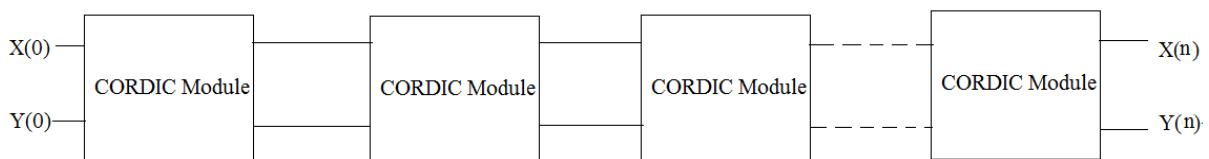


Fig.7.4(b). Pipeline array of CORDIC Modules

In the realization of hardware, this pipeline architecture is used to get the desired 8 bit output of sine-co-sine waveforms. Each module consists of one ROM, three Registers and three Adder/Subtracters.

DPSK Demodulator:

The demodulator block in Fig.7.5 consists of a synchronous detector, a delay circuit and a matched low pass filter to retrieve the desired or original message $b'(t)$. In demodulation of DPSK signal, carrier wave generator is not required because the received modulated signal itself is a carrier, $\pm A_1 \cdot \cos\omega t$. Instead of carrier generator, a delay circuit, T_d of 1-bit delay of received signal is used to retrieve the data stream. The synchronous detector or multiplier has been used to multiply the received signal and the 1-bit delayed signal. In this case a CORDIC multiplier is used to serve the purpose. If both are of the same polarity, multiplier output will be $A_1^2 \cdot \cos^2\omega t$ and output pulse will be positive and can be detected as bit '1' whereas if the two signals are of opposite polarity, output of multiplier will be $-A_1^2 \cdot \cos^2\omega t$. This negative amplitude or significantly less positive pulse will be detected as bit '0'.

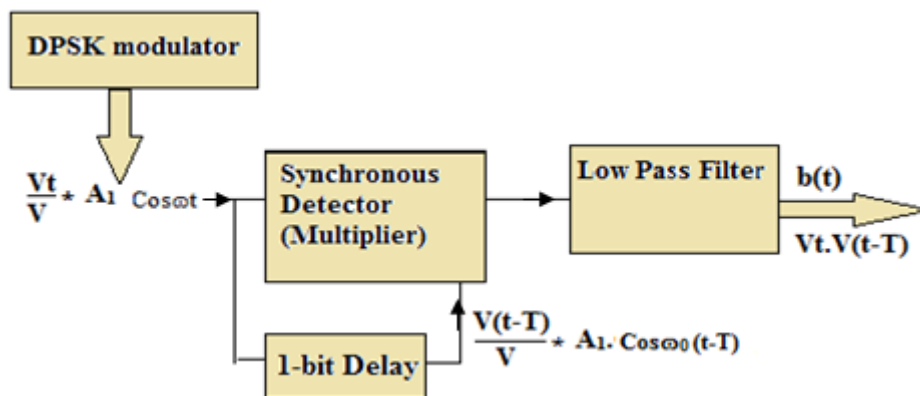


Fig. 7.5 DPSK Demodulator Block diagram

DPSK modulated signal is fed as input to the demodulator section to observe the desired output recovered from it. Every modem includes four basic functional blocks including modulator, demodulator. The other two blocks are CODEC (Coder/Decoder) and PGA (programmable gain amplifier), whereas CODEC block is used to convert analog to digital and digital to analog conversion, gain amplifier serves the general amplifier. In this proposed architecture, as the modulated signal is used directly to verify the operating accuracy of the design, we consider design of only modulator and demodulator block. To verify the performance of onchip carrier generation and modulation using the CORDIC module is another purpose of our design. So that the module can be tested for real time application.

7.6 Implementation of proposed DPSK modem module:

Each block of a DPSK modem [modulator/demodulator/CORDIC module] has been implemented using VHDL code and Xilinx ISE 14.3 simulator tool.

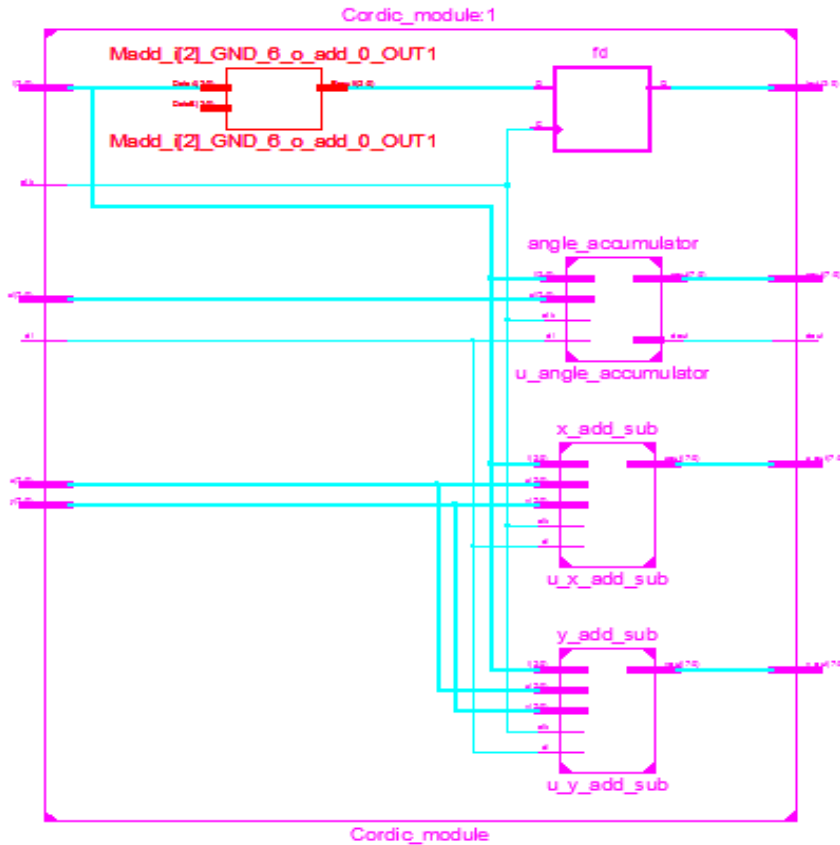


Fig. 7.6 Implemented CORDIC Block RTL schematic

Blocks have been realized using suitable test-bench simulation and synthesizable module of each block is shown in the following figures. The RTL schematic views of the CORDIC block and DPSK modulator are shown in Fig. 7.6 and Fig. 7.7 respectively. In this view, a bit_gen block and a wave_generator block (sine cosine) are present. The CORDIC multiplier block multiplies the $A \cdot \cos \omega t$ with the generated bit stream. An expanded view is given in Fig.7.8. An arithmetic block DSP48E1 has been used to perform the modulation operation.

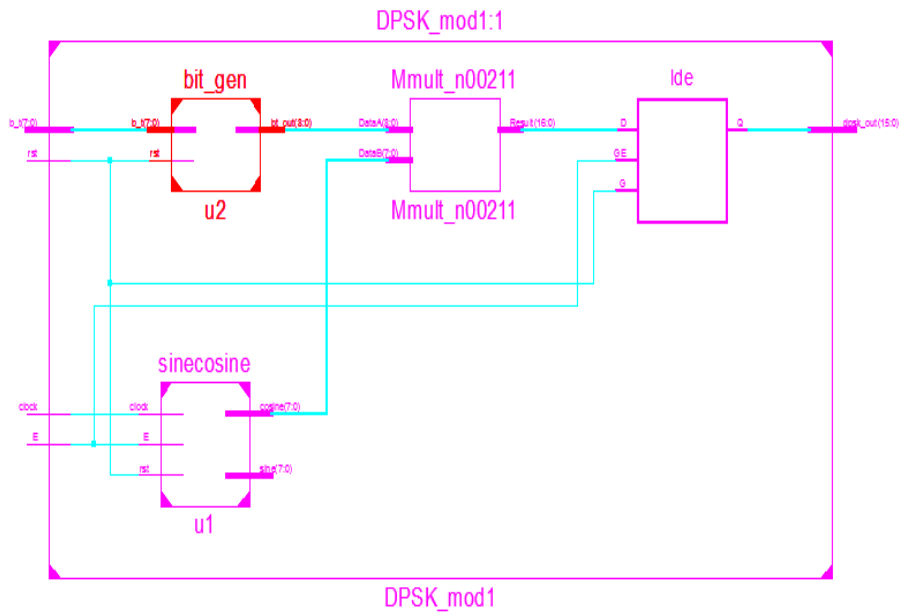


Fig.7.7 RTL schematic view of the Implemented DPSK modulator

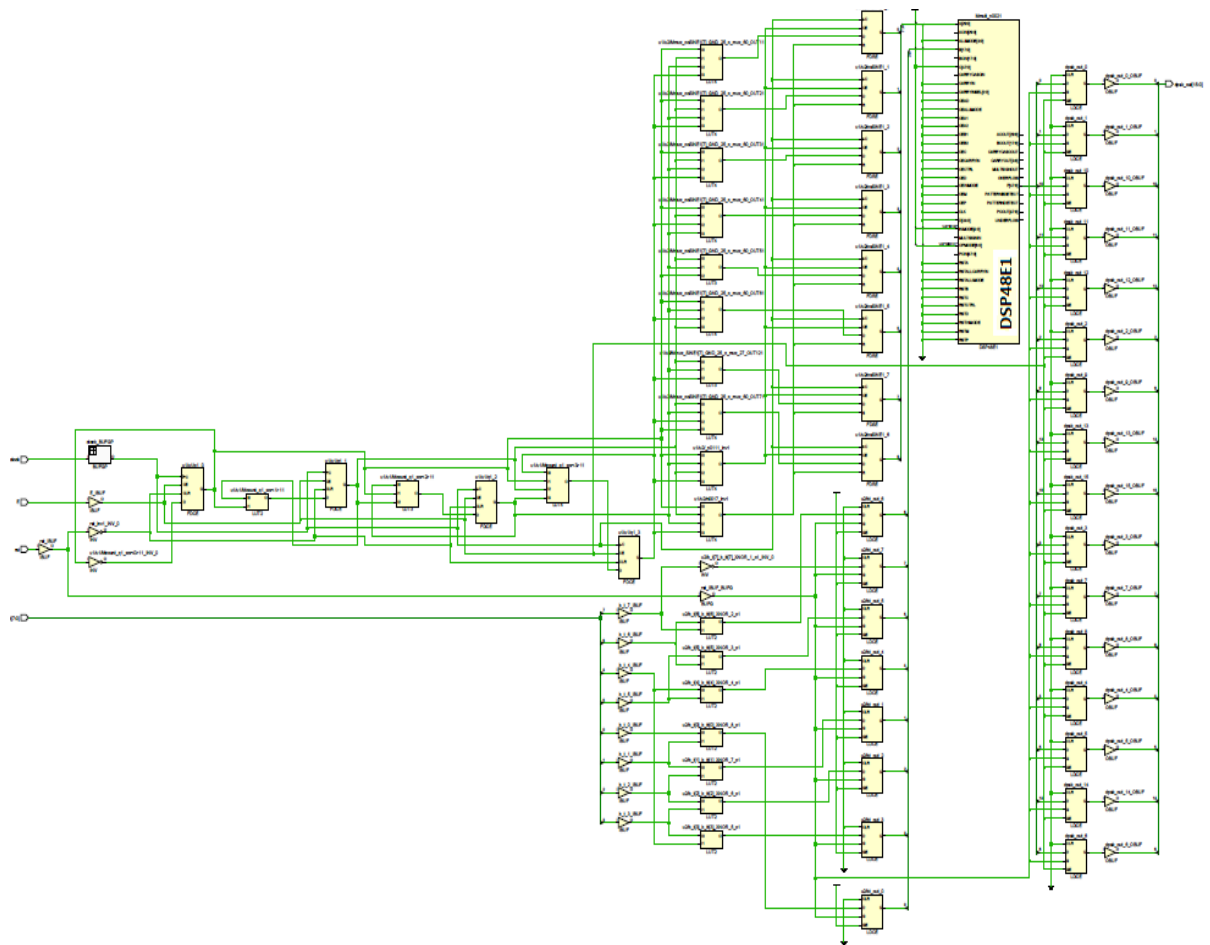


Fig.7.8 Expanded RTL view of the DPSK modulator using Plan Ahead 14.3

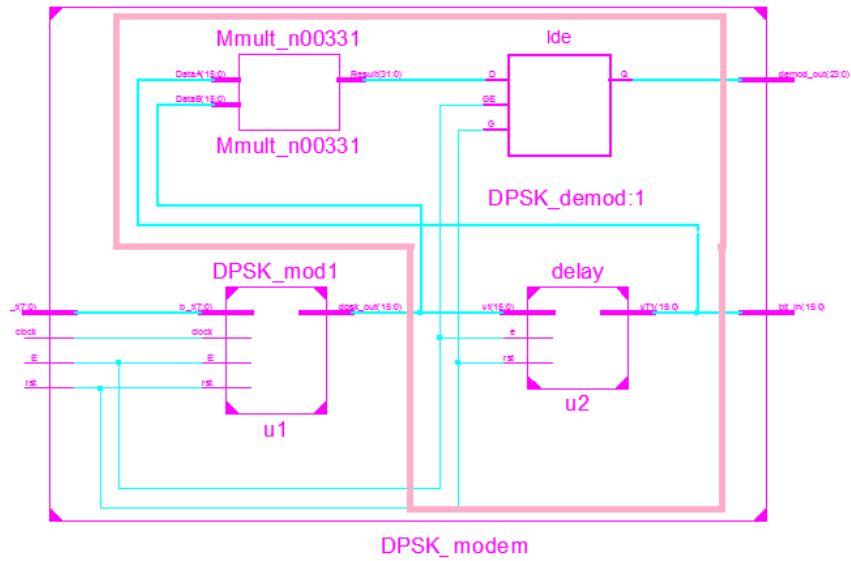


Fig. 7.9 RTL schematic view of the DPSK modem

The RTL schematic view of the modem is shown in Fig.7.9. The modem module consists of modulator and demodulator sections within the single block. The expanded view of the DPSK modem using Plan Ahead 14.3 is shown in Fig. 7.10.

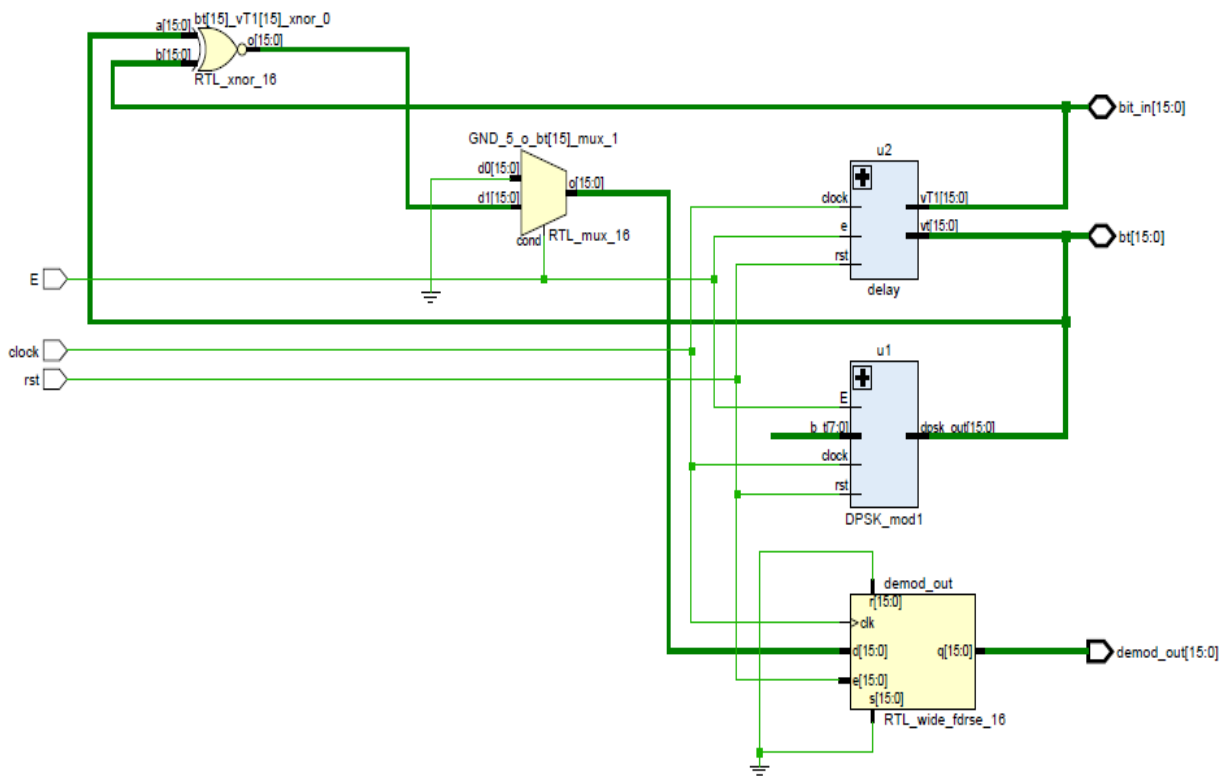


Fig.7.10 Expanded RTL view of the DPSK modem using Plan Ahead 14.3

The DPSK modem has been designed and simulated using Xilinx ISE 14.3 simulation tool and implemented on Kintex-7 FPGA board. Kintex™-7 FPGA board provides a comprehensive, high-performance development and demonstration platform. Introduction of 28nm FPGAs in Kintex-7, confirm it as a very high speed FPGA suitable for portable module for wireless communication system. It is highly integrated and has high speed connectivity with superior bandwidth.

It has 8 Block RAMs configured within to build a 32 bit words memory. Incorporated CORDIC module has enhanced the speed and performance of the design. Reduction of complexity of the electronic circuits and the number of passive elements such as resistors, capacitor etc. reduces the size of the implemented modem device. The area requirement is also small and the VLSI architecture reduces the power consumption or dissipation to a minimum level.

7.7 Simulation Results:

Each block is simulated with suitable testbenches to get the desired result output. These test bench simulation results are shown in Figs. 7.11, 7.12 and 7.13.

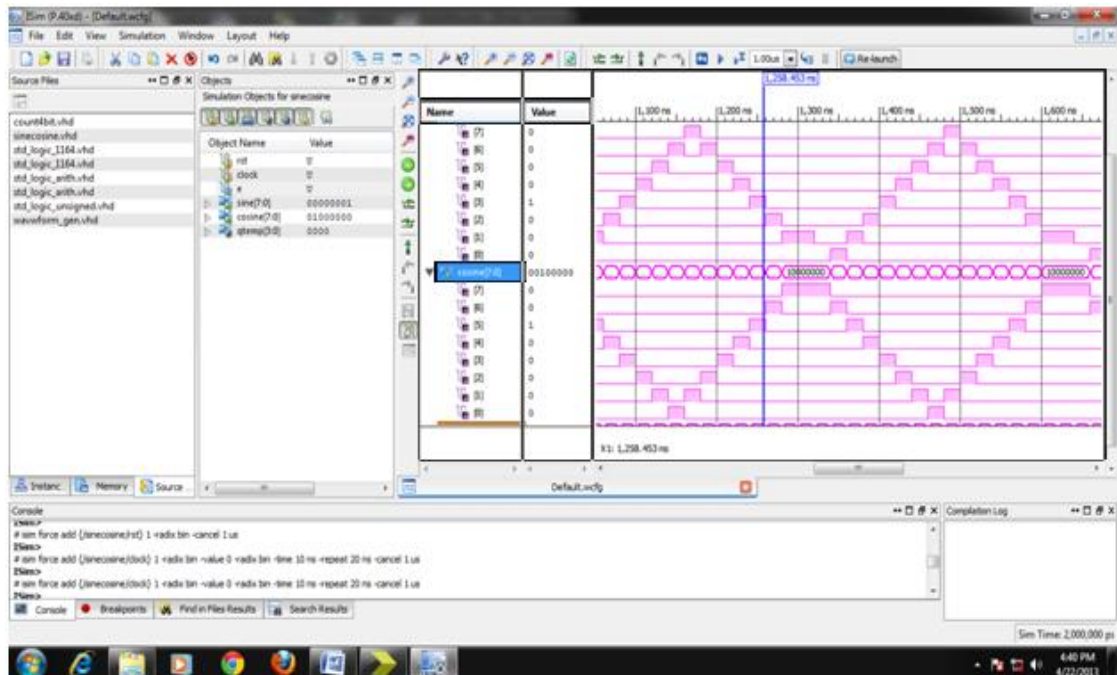


Fig. 7.11 Sinewave & Co-Sinewave generation

It can be observed from Fig. 7.11, that the sine and co-sine waves have been generated using CORDIC sine_cosine_wave_generator as bit stream which represents the approximate digital values of the angles. The generation of sine and co-sine wave using look-up-table of predetermined stored values is shown. Thus the signal generated is digitalized and gives approximate values of the signal, but due to minor error, it can be avoided. This waveform has been used as carrier frequency in the modulator block to modulate the input bit stream and resultant output is produced in Fig 7.12.

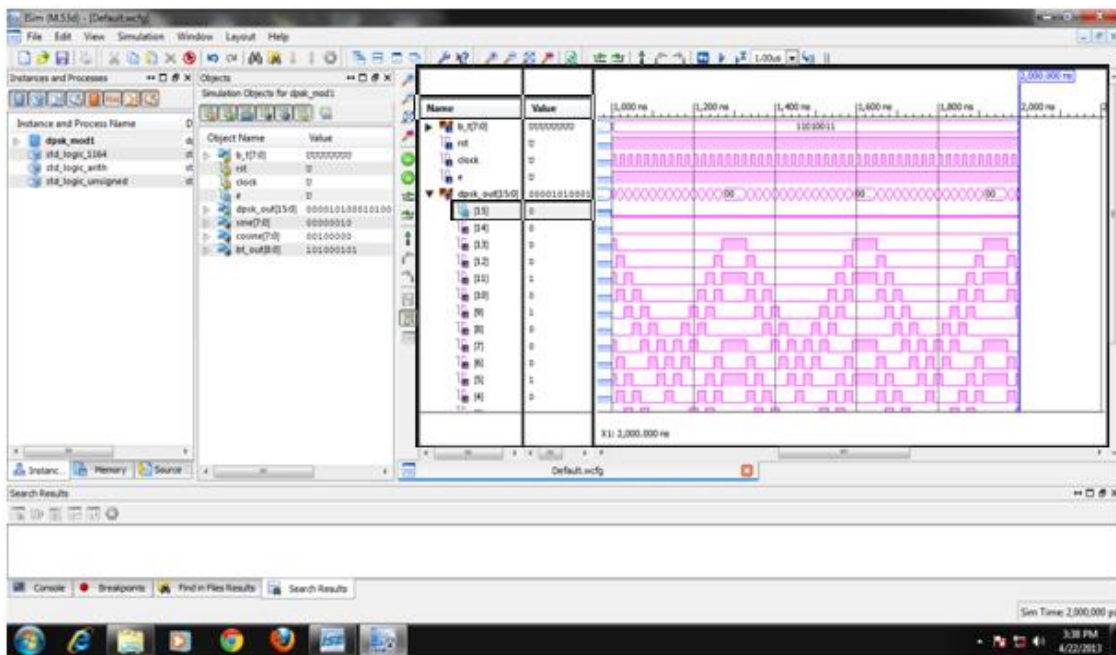


Fig. 7.12 DPSK Modulator output result

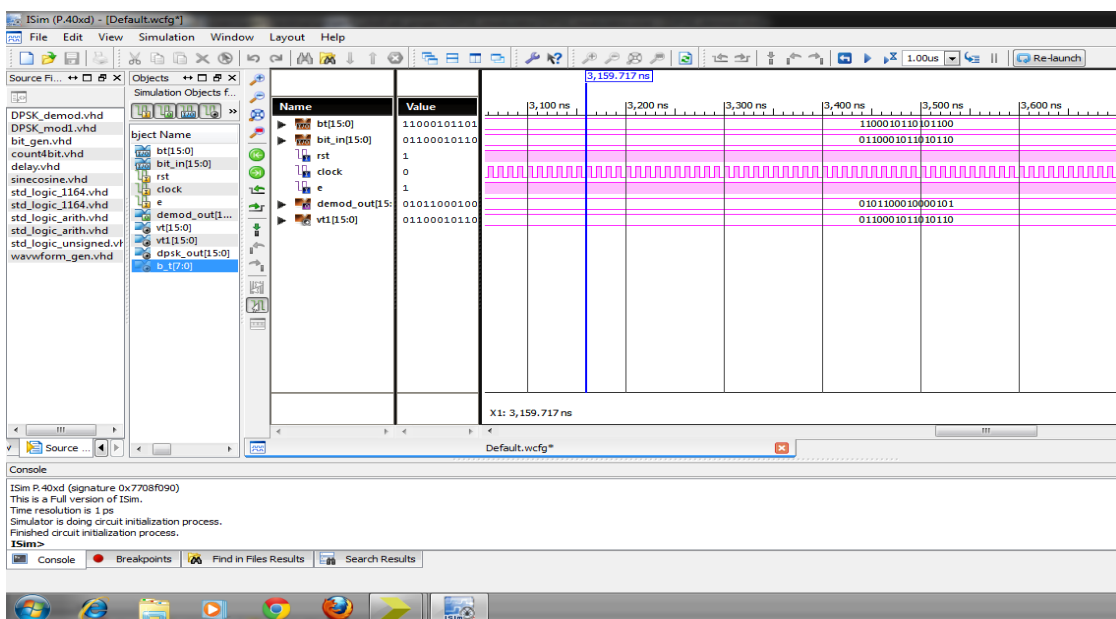


Fig.7.13 DPSK demodulator output result

In Fig.7.13 the test-bench output result of the DPSK demodulator is shown. In order to verify the functionality of the DPSK modulator, our design is also implemented on Software Defined Radio (SDR). SDR technology is based on programmable hardware modules (FPGA Devices).

An SDR (Software Defined Radio) is a device for radio communication in which the properties of carrier frequency, modulation type, signal bandwidth all are defined by software. SDR is a general-purpose device in which the same radio tuner and processors are used to implement modulation/demodulation at many frequencies. The idea is to get the hardware problems into software problems. This advantage has made the equipment more versatile, user friendly, adaptive and cost-effective. Here, in this research work, design and implementation of DPSK modulator and demodulator based on SDR ideology is performed.

In mobile communication technology, DPSK modulation generally uses modem chips, or ASIC to implement, but those chips don't have programming skills and thus its functionality cannot be changed or improved easily in the product development process. Hence, those chips are not suitable in the cases where parameters change frequently and functionality needs to be changed or improved. The FPGA based device for communication system is easy to implement and the pipeline architecture made it simple to upgrade. This is a very practical and effective approach to implement the FPGA based DPSK modulator and demodulator.

The SDR trainer (ViSDR-01), which is based on Spartan-6 DSP FPGA devices, is used here. The SDR experimental board consists of a high speed ADC & DAC for digital up / down conversion, reconfigurable board, a 2.4 GHz RF Up / Down converter board and antenna all with PC interfacing features. This flexible programmable hardware is suitable for implementation of various functions of a radio system like Modulation, Demodulation, Line coding, etc. The ViSDR-01 product fully supports the library of Xilinx system Generator blocks in MATLAB, which are used in this work. The block model is shown in Fig. 7.11 and the simulated result in Fig 7.14.

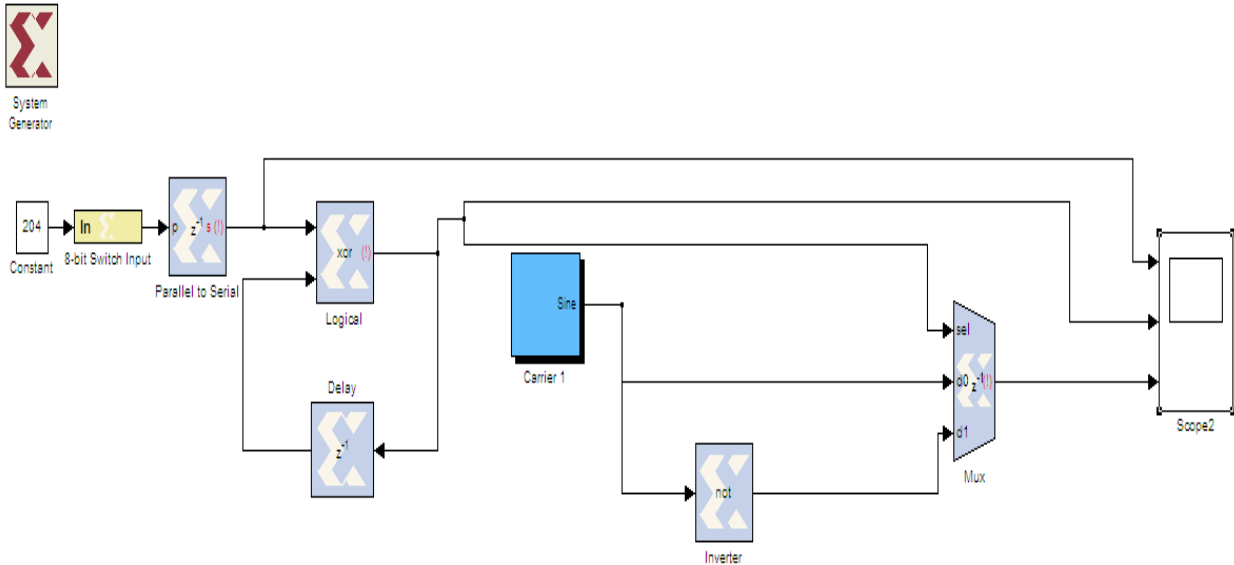


Fig. 7.14 The DPSK modulator design using Simulink, Matlab10 (Xilinx block on SDR)

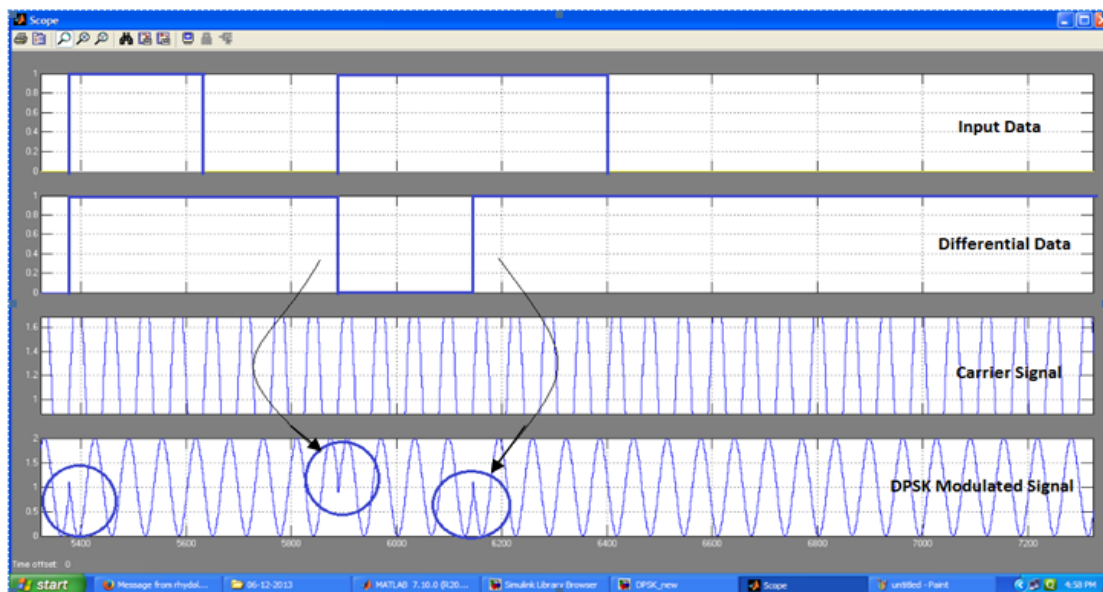


Fig. 7.15 DPSK Modulator output result in Simulink model

The DPSK modulator of the Simulink model using Xilinx block is shown in Fig. 7.14. Differential Phase shift occurs as we observe in the circled figure on the modulated waveform in Fig. 7.15. The simulated results can be verified in hardware output. We have verified only the modulator section on SDR. Similarly, the complete modem section also can be verified which we have avoided here because of the brevity of the paper. After successful synthesis of our proposed DPSK modem, we obtained the advanced synthesis report and device utilization

chart. We have used high performance FPGA (Device: 7k325tffg900-2) in order to verify the functionality of the processor. Introduction of 28nm FPGAs in Kintex-7, conform it as a very high speed FPGA and used for new generation module for wireless communication system and very much suitable for portable module. It is highly integrated and has high speed connectivity with superior bandwidth.

Table 7.1: Advanced HDL Synthesis Report

Parameters	DPSK Modulator	CORDIC Block	DPSK Modem
RAM	-	1	4
Adder/ Subtractor	-	4	16
Registers/Flip Flop	16	27	45
Multiplexers	23	2	32
Counters	1	-	2
Comparators	15	-	30
Xors	8	-	16

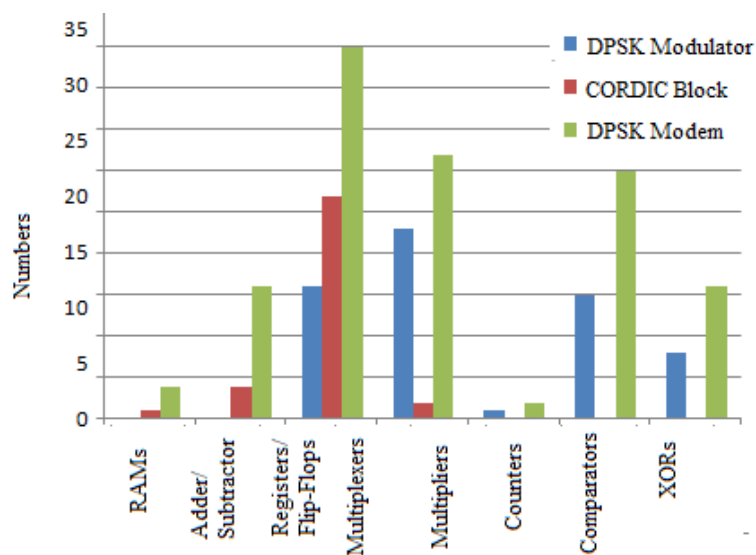


Fig.7.16 Bar-chart showing different parameters of different blocks

Table 7.1 presents the requirements of different block modules and Fig.7.16 represent the bar-charts of the modules which are self explanatory. From table 7.1, we get the HDL synthesis of most important block modules for our design. We have considered the CORDIC module, modulator and modem module only. A comparative study of device utilization

summary for implementing DPSK module in VHDL code (Xilinx14.3) and implemented on FPGA virtex-7 device and Matlab Simulink Xilinx12.1 model and implemented on Spartan 6 device targeting the SDR device is shown in Table 7.2.

From table 7.2, we get the performance comparison of our CORDIC based DPSK modem implemented on Kintex-7 FPGA board with standard SDR based (non-CORDIC) DPSK modem. It reflects its efficiency regarding hardware requirement, power consumption and delay. In this respect our proposed modem is efficient and suitable for low power, low noise, and portable device application. Our DPSK modem requires minimum slices and leaves a large and remarkable space for advancement and other hardware design.

Table 7.2: A comparative study of Device utilization summary of DPSK modem

Sl.no.	Parameters	CORDIC DPSK modem	non-CORDIC (SDR) DPSK modem
1.	Number of Slice Registers:	20	68
2.	Number of Slice LUTs:	62	60
3.	Number of LUT Flip Flop pairs used:	63	82
4.	Number of unique control sets:	4	6
5.	Number of bonded IOBs:	27	25
6.	IOB Flip-Flops/Latches:	24	26
7.	Number of BUFG/BUFGCTRLs:	3	1
8.	Number of DSP48E1	1	0
9.	Max. Freq.: (MHz)	661.638	362.437
10.	Min. period:	1.511 ns	2.759 ns
11.	Max. Output required time after clock:	0.669 ns	5.731 ns
12.	Max. Power dissipation:	0.252 mW	66.72 mW
13.	Dynamic Power dissipation:	0.029 mW	27.79 mW

The dynamic power dissipation is about 0.029mW and maximum processor delay is 0.669ns only. The average static power dissipation is only 0.252mW. The quality of the modem performance is compared with a non-CORDIC modem developed using SDR platform and it is observed that the hardware requirement is minimized up to one third and speed increases by almost nine times with a very low power dissipation rate.

CHAPTER 8

CONCLUDING REMARKS AND FUTURE SCOPE OF THE THESIS

Chapter 8: Concluding Remarks and Future Scope of the Thesis:

8.1 Concluding Remarks:

Adaptive VLSI Design of RFID and WSN technology based wireless communication systems are presented and described in details here, in this thesis. Development of low power adaptive processor for such wireless communication systems incorporating novel algorithms within them is the objective of this thesis work. In Wireless communication systems, FPGA based system realization has attained much popularity because of its easy implementation and adaptive nature to reconfigure or upgrade the system according to requirement without much effort and time. Hardware implementation up to RTL schematic level has been performed. In order to substantiate our design and real time verification, synthesizable modules are successfully downloaded on high performance FPGA kit.

Designs are performed using high syntax VHDL code language and simulation results are obtained with Xilinx ISE 14.3 simulator. Virtex 5, Spartan 6 and Kintex-7 FPGA boards are used as a hardware implementation platform. The comparative studies with related works are made where possible. Performance evaluation and comparative study with related work is performed in order to substantiate proposed design and developed module.

VLSI Implementation of processor suitable for RFID based power efficient Home/Office automation system is performed as a part of this work. The simulated and synthesized design of the processor works with satisfactory result as we observe in the test bench waveforms. The system switch 'on/off' the lights and fans in a room using RFID reader is in accord to the identification of desired tags. The temperature control unit controls the temperature of the room within a specified range, not only that, the 'alarm' generator signal becomes high to 'on' a buzzer for 'fire-alarm' whenever the temperature of the room exceeds a specified high temperature. So, we achieve our desirable power saving model, which works on RFID technology. The design is also implemented on FPGA kit. Virtual platforms are used to verify the working ability of the proposed model.

The superiority of this technology largely depends on suitable anti-collision algorithm. Power efficient anti-collision algorithms with added priority and security feature

have been proposed and implemented in this work. The static power consumption for the simulation is only 30.45 mW, but in case of practical design, designer may choose different suitable low voltages to reduce power consumption. The processor can be modified in accordance with the design constraints and requirements and can be implemented on easily reconfigurable FPGA. Maximum combinational path delay for the reader module is only 5.729ns in this design whereas hardware utilization is optimized to only 22 % of the FPGA. The hardware realization of EPC Gen2 protocol on FPGA board is performed successfully in this work. The developed model has been simulated for different Q values to achieve the maximum success for tag identification using Matlab 6.5. It is observed that to increase the success rate in an increasing tag population environment Q value must be increased and modified before starting an inventory round. But high value of Q decreases the system efficiency, so the Q value should not increase, beyond a value of 7/8; i.e Reader should select a limited portion (2^Q) of tag population at a time for maximum efficiency and throughput of the system. The static power consumption is only 25 mW with a combinational path delay of 7.25 ns.

PCA based scheme for data security and authentication in RFID system is presented in this thesis. Secured data transfer to authenticated Reader and its VLSI implementation is one of the most important achievements of this work. As the key matrix and the cellular automata rules for different bit matrix is different and depends on the designers choice, the security level is high and only the authenticated Reader can be able to decode the tag ID, and thus, read the information stored within it. On chip static power consumption for data processing is 122.13 mW with a quiescent current of 1.27 mA. The processing time after clock is 0.795 ns only. The hardware utilization is only 37% for the reader module and 26% for the tag module. As the PCA based security scheme minimizes the computational overhead unlike other encryption algorithm based security scheme, it is better in respect of circuit complexity, processing speed and power consumption.

The presence of obstacles creates an unwanted detour and/or dead ends, thereby distorting the sensor networks and may lead to deploy complex and costly routing techniques. In the present work a power efficient DOL algorithm based processor for large WSN has been developed. The VLSI implementation of the proposed processor and its hardware realization has been achieved through Xilinx ISE 14.3 simulation tool and synthesized codes are downloaded into the Virtex-V FPGA kit. The same is subsequently verified using

MATLAB environment. In view of VLSI design of the processor and adopted sleep scheduling of beacons made the proposed system *power efficient*. In this model, there is no need to use the beacons full time active, and a huge power is saved. Power consumed by a single processor is 0.012mW in active mode with a dynamic current of 1.27mA according to the experimental result. As per the simulation result, two sets of beacons will be activated for only 680ns. Therefore, power will be saved by almost 66.67%. This algorithm has been simulated and verified for three different figures to evaluate the *obstacle area detection efficiency*. It is observed that when the obstacle is circular the detection error is minimum.

Design and implementation of a power efficient FPGA based adaptive DPSK modem for wireless communication system is performed in this work. CORDIC algorithm has been used in this article to get rid of the costly multipliers which introduce more power consumption, more hardware and noise effects. Generation of carrier on chip also solves the problem related to noise. CORDIC algorithm has been employed because of the simplicity of the operations incorporated in it which makes it well suited for VLSI implementation. Our FPGA based DPSK modem has been implemented using Kintex-7 architecture working at frequency of 661.638MHz which is suitable for data transmission in the mobile communication channel. The dynamic power dissipation is about 0.029mW and maximum processor delay is 0.669ns only. The average static power dissipation is only 0.252mW. The quality of the modem performance is compared with a non-CORDIC modem developed using SDR platform. It is observed that the hardware requirement is minimized up to one third and speed increases by almost nine times. Similarly, in case of static and dynamic power dissipation, it is evident that the CORDIC based modem is much better.

8.2 Future Scope of the Thesis:

With the rapid progress and technological advancement in VLSI design technology, processor implementation with hardware description language code like Verilog and VHDL has a growing demand in the electronics industry. To cope up with this technology up gradation, reconfigurable architecture with the adaptive nature finds its suitable field in many application areas in wireless communication systems. As it is a vast area, the candidate has limited her research work within RFID technology and wireless sensor network only and developed few adaptive processors providing justified solutions to some specific problems

defined in this thesis. Future scope of this research work is the more sophisticated FPGA based model realization for fast growing and ever changing wireless communication systems. It is applicable for every advanced electronic system, not limited to the wireless communication system. In Medical technology, Bio-medical technology where tiny sensors take an important role to play, intensive data processing is major concern; FPGA is suitable due to its ability to do so.

REFERENCES:

- [1] Dr. K.V.K.K.Prasad, Kattula Shyamala, “VLSI Design Black Book”, Wiley & Sons Inc.
- [2] Douglas Perry, “VHDL by Example” (e-version in the library).
- [3] Peter Ashenden, “VHDL cookbook” ,
- [4] M.Smith, “ASIC – The Book”, On-line Version.
- [5] “VHDL and VHDL FAQ”, University of Hamburg:
- [6] Jun Zheng, Abbas Jamalipour, “Wireless Sensor Networks: A Networking Perspective”, Wiley-IEEE Press. 2009,
- [7] Lin Gu and John A.Stankovic, “Radio-Triggered Wake-Up for Wireless Sensor Networks”, Real-Time and Embedded Technology and Applications Symposium, IEEE,Proceedings. RTAS 2004.
- [8] L.L. Liang, L.F. Huang, X.Y.Jiang, V. Yao, “Design and implementation of wireless smart-home sensor network based on ZigBee protocol,” International Conference on Communications, Circuits and Systems, pp. 434-438, 2008,
- [9] Van Der Doom, B. Kavelaars, W and Langendeon. K, “A prototype low cost wake up radio for the 868 MHz band”, Int. Journal of Sensor Networks, Inderscience vol.5,no.1, pp.22-32.2009.
- [10] Renyan Zhou, Leibo Liu, Shouyi Yin, Ao Luo, Xinkai Chen, Shaojun Wei, “A VLSI Design of Sensor Node for Wireless Image”, IEEE, pp.149-152. 2010
- [11] Aki Hopponen, “Low power design for Wireless Sensor Networks”. Springer, 2012
- [12] Byrne, J., Cosgrove, M. and Mehra, R. “Stereo based obstacle detection for an unmanned air vehicle”, Proceedings of IEEE International Conference on Robotics and Automation, pp.2830–2835. 2006
- [13] Li, Q., Rosa, M.D. and Rus, D. “Distributed algorithms for guiding navigation across a sensor network”, Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM), pp.313–325. 2003

- [14] Reichenbach, F., Salomon, R. and Timmermann, D. “Distributed obstacle localization in large wireless sensor networks”, IWCMC ‘06, July, ACM 1-59593-306-9/06/0007, Vancouver, British Columbia, Canada. 2006
- [15] Wong, C.Y. and Qidwai, U, “Intelligent sensor network for obstacle avoidance strategy”, in Published in: Sensors, IEEE conference, DOI: 10.1109/ICSENS.2005.1597721. 2005
- [16] Funke, S. “Topological hole detection in wireless sensor networks and its applications”, Proceedings of Joint Workshop on Foundations of Mobile Computing, pp.44–53. 2005
- [17] Fekete, S.P., Kaufmann, M., Krölller, A. and Lehmann, K. “A new approach for boundary recognition in geometric sensor networks”, in Proceedings of Canadian Conference on Computational Geometry, pp.82–85. 2005
- [18] Fekete, S.P., Krölller, A., Pfisterer, D., Fischer, S. and Buschmann, C. “Neighborhood-based topology recognition in sensor networks”, Proceedings of International Workshop on Algorithms Aspects of Sensor Networks (ALGOSENSORS), pp.123–136. 2004
- [19] Mark Hempstead, Michael J. Lyons, David Brooks, and Gu-Yeon Wei, “Survey of Hardware Systems for Wireless Sensor Networks”, Journal of Low Power Electronics vol.4, pp.1–10, 2008
- [20] Zhou, R., Liu, L., Yin, S., Luo, A., Chen, X. and Wei, S. “A VLSI design of sensor node for wireless image sensor network”, Proc. IEEE International Symposium on Circuits and Systems (ISCAS), pp.149–152. 2010
- [21] I.F. Akyildiz, W. Su, Y. Sankara subramaniam, E. Cayirci, “Wireless sensor networks: a survey” Computer Networks vol.38 no.4, pp.393–422, 2002
- [22] J. M. Rabaey, M. J. Ammer, J. L. da Silva, Jr. D. Patel, S. Roundy, “Pico radio supports ad hoc ultra-low power wireless networking”, IEEE Computer, vol 33 no.7. pp. 42-48, Aug 2000
- [23] Peng Guo, Tao Jiang, Senior Member, IEEE, Qian Zhang, Fellow, IEEE, and Kui Zhang, “Sleep Scheduling for Critical Event Monitoring in Wireless Sensor Networks” IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 2, Feb 2012

- [24] Gang Lu, Narayanan Sadagopant, Bhaskar Krishnamachari, Ashish Goel, “Delay Efficient Sleep Scheduling in Wireless Sensor Networks” INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE pp.2470 - 2481 vol. 4, Mar.2005
- [25] Jeremy Landt “The history of RFID”, IEEE Potentials, October 2005,
- [26] “Data from radio frequency identification – a basic primer”, Association for Automatic Identification and Mobility, Aug.2001, <http://www.aimglobal.org> and from Wikipedia Encyclopaedia, <http://en.wikipedia.org/wiki/RFID>.
- [27] Motorola, “The next-generation warehouse Megatrux improves service and reduces costs with RFID”, RFID world, <http://www.motorola.com>
- [28] Beth Bacheldor, “U.N.’s Universal Postal Union Gears Up for Large RFID Pilot”, RFID Journal, Dec 10, 2008
- [29] Jonathan Collins, “Aussies Track Mail Service via RFID”. RFID Journal, Dec 01, 2005.
- [30] Larry Dignan, “FedEx couples Google Earth with active package tracking”, ZDNet, Feb.2007.
- [31] Pala. Z and Inanc. N, “Smart Parking Applications Using RFID Technology”, RFID Eurasia, pp1-3, Sept.2007.
- [32] Li Guangjin, “RFID Application in 2008 Olympic Beijing”, Presentation Solution, Vol 29, No. 4, 2008.
- [33] Jimson Lee, “First RFID Lap Counters, Now Microchipped Olympic Tickets?” Speed Endurance, May 31, 2008
- [34] Institute of Medicine, “Crossing the Quality Chasm: A New Health System for the 21st Century”, Institute of Medicine publication, 2001.
- [35] Cangialosi A., Monaly J.E. and Yang S.C., “Leveraging RFID in hospitals: Patient life cycle and mobility perspectives”, IEEE Communication Magazine, Vol 45, No. 9, Sept. 2007.
- [36] A. M. Wicks, J. K. Visich and S. Li, “Radio Frequency Identification Applications in Hospital Environment”, held ref publications, Hosp. Top., Vol 84, No. 3, pp. 3–9, 2006.

- [37] Koh R, Schuster E.W., Chackrabarti, I., and Bellman A., "Securing the Pharmaceutical Supply Chain", Auto-ID Center, Mit-AutoID-WH-021, 2003.
- [38] World Health Organization, <http://www.who.int>
- [39] A. Aguilar, W. van der Putten, and F. Kirrane, "Positive patient identification using rfid and wireless networks," in HISI 11th Annual Conference and Scientific Symposium, Nov. 2003.
- [40] J. E. Bardram, "Applications of context-aware computing in hospital work: examples and design principles," in SAC '04: Proceedings of the 2004 ACM symposium on Applied computing. New York, NY, USA, pp. 1574–1579. ACM, 2004
- [41] J. Dalton and S. Rossini, "Using RFID technologies to reduce blood transfusion errors," white Paper by Intel Corporation, Autentica, Cisco Systems and San Raffaele Hospital, 2005.
- [42] W. Yu, P. Ray, and T. Motoc, "A RFID technology based wireless mobile multimedia system in healthcare," e-Health Networking, Applications and Services, 2006. HEALTHCOM 2006. 8th International Conference on, pp. 1–8, Aug. 2006.
- [43] F. Wu, F. Kuo, and L.-W. Liu, "The application of RFID on drug safety of inpatient nursing healthcare," in ICEC '05: Proceedings of the 7th international conference on Electronic commerce. New York, NY, USA: ACM, pp. 85–92. 2005
- [44] J. Halamka, "Early experiences with positive patient identification," Journal of Healthcare Information Management, vol. 20, no.1, pp. 25–27, 2006.
- [45] S.-W. Wang, W.-H. Chen, C.-S. Ong, L. Liu, and Y.-W. Chuang, "RFID application in hospitals: A case study on a demonstration RFID project in a Taiwan hospital," HICSS, System Sciences, HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on, vol. 8, page. 184a, Jan 2006.
- [46] E. J. Jaselskis, M.R. Anderson, C.T. Jahren, Y. Rodrigues, and S. Njos, "Radio-frequency identification applications in construction industry", J. of Constr. Eng. and Man. vol. 121, no. 2, pp. 189-196. 1995,

- [47] S. Chin, S. Yoon, Y. Kim, J. Ryu, C. Choi, and C. Cho, "Realtime 4D CAD - RFID for Project Progress Management," Construction Research Congress 2005: Broadening Perspectives, San Diego, California. 2005,
- [48] Peyret, F. and Tasky, R. "Asphalt quality parameters traceability using electronic tags and GPS," Proc. ISARC '02, IAARC, Washington, DC, pp.155-160. 2002
- [49] Ergen, E., Akinci, B., Sacks, R. "Tracking and Locating Components in a Precast Storage Yard Utilizing Radio Frequency Identification Technology and GPS", Automation in Construction, vol.16, Issue 3, pp. 354-367.2007
- [50] J.Bhasker, "A VHDL synthesis Primer", BS Publication
- [51] Wayne Wolf, "Modern VLSI Design; 4th edition", PHI Learning Private Limited, 2009.
- [52] Stephen Brown and Zvonko Vranesic, "Digital Logic design", Tata McGraw Hill Publication' 2008.
- [53] www.vhdl.org
- [54] www.edaboard.com
- [55] Ahso n, S. and Ilyas, MRFID Handbook: Applications, Technology, Security, and Privacy, CRC Press, Boca Raton.2008
- [56] Miles, S.B., Sharma, S.E. and Williams, J.R. 'RFID Technology & Applications', Cambridge University Press, New York. 2008
- [57] Drew Gislason, "Zig Bee Wireless Networking",Elsevier,2008
- [58] David Egan, "Zig Bee Propagation for Smart Metering Networks", Electric Light & Power, vol.17, Issue 12.Dec 2012.
- [59] "Zig Bee Specification FAQ", Zig Bee Alliance, Retrieved 14th June,2013
- [60] Jinyun Zhang; Orlik, P.V.; Sahinoglu, Z.; Molisch, A.F.; Kinney, P.; "UWB Systems for Wireless Sensor Networks," Proceedings of the IEEE , vol.97, no.2, pp.313-331, Feb. 2009
- [61] Matischek, R.; Herndl, T.; Grimm, C.; Haase, J.; "Real-time wireless communication in automotive applications," Design, Automation & Test in Europe Conference & Exhibition (DATE), pp.1-6, Mar. 2011

- [62] Shaokun Lu; Meiyin Duan; Ping Zhao; Yunwen Lang; Xiaoyin Huang; "GPRS-based environment monitoring system and its application in apple production," Progress in Informatics and Computing (PIC), IEEE International Conference on , pp.486-490, Dec. 2010
- [63] Dar, K.; Bakhouya, M.; Gaber, J.; Wack, M.; Lorenz, P.; "Wireless communication technologies for ITS applications [Topics in Automotive Networking]," Communications Magazine, IEEE , vol.48, no.5, pp.156-162, May 2010
- [64] Bing Shi; Zhenghua Ma; "Application of wireless communication based on GPRS in power plant's CEMS," Computer and Automation Engineering (ICCAE), The 2nd International Conference on , pp. 529-532, Feb. 2010
- [65] Min Chen; Gonzalez, S.; Leung, V.; Qian Zhang; Ming Li; "A 2G-RFID-based e-healthcare system," Wireless Communications, IEEE , vol.17, no.1, pp.37-43, Feb. 2010
- [66] Turcu, C.; Popa, V.; "An RFID-Based System for Emergency Health Care Services," Advanced Information Networking and Applications Workshops, WAINA International Conference on , pp. 624-629, May 2009
- [67] S.-W. Wang, W.-H. Chen, C.-S. Ong, L. Liu, and Y.-W. Chuang, "RFID application in hospitals: A case study on a demonstration RFID project in a Taiwan hospital," HICSS, System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on, vol. 8, page. 184a, Jan 2006.
- [68] Woodward Laboratories, 2004, referred 2.6.2009, available [http://www.woodwardlabs.com/pdfs/iHygiene Press Release.pdf](http://www.woodwardlabs.com/pdfs/iHygiene%20Press%20Release.pdf).
- [69] M. Kodialam and T. Nandagopal, "Fast and reliable estimation schemes in RFID systems," in MobiCom '06: Proceedings of the 12th annual international conference on Mobile computing and networking. New York, NY, USA: ACM, 2006, pp. 322–333
- [70] J. Song, C.T. Haas, and C. H. Caldas, "Tracking the Location of Materials on Construction Job Sites." J. of Construction Eng. and Management, vol. 132,no. 9. 2006

- [71] P. M. Goodrum, M. A. McLaren and A. Durfee, "The application of radio frequency identification technology for tool tracking on construction job sites," *Automation in Construction*, vol. 15, no. 3, pp. 292-302. 2006,
- [72] R. Navon and Eytan Goldschmidt, "Can Labor Inputs be Measured and Controlled Automatically?" *J. of Construction Eng. and Management*, vol. 129, no. 4. 2003,
- [73] Saad, S.S.; Nakad, Z.S;"A Standalone RFID Indoor Positioning System Using Passive Tags," *Industrial Electronics, IEEE Transactions on*, vol.58, no.5, pp.1961-1970, May 2011.
- [74] Syed Ahson & Mohammad Ilyas, "RFID Handbook, Applications, Technology, Security and Privacy" by CRC Press , Boca Raton,2008
- [75] Konstantinos Domdouzis, Bimal Kumar and Chimay Anumba, "Radio-frequency Identification (RFID) applications, A brief introduction", *Advanced Engineering informatics*. ,vol. 21, pp: 350—355. 2007
- [76] K. Finkenzeller, "RFID Hand Book: Fundamentals and Applications in Contactless Smart Card and Identification", Second Edition, John Wiley & Sons Ltd, 2003
- [77] C.M.Roberts, "Radio frequency identification (RFID)", *Computers & Security, Elsevier*,vol.25,issue-1,pp: 18—26, Feb.2006
- [78] D. R. Hush and C. Wood, "Analysis of Tree Algorithms for RFID Arbitration," in *Proceedings of IEEE International Symposium on Information Theory*, pp 107, 1998
- [79] M. Jacomet, A. Ehram and U. Gehrig, "Contactless Identification Device with Anticollision Algorithm," in *Proceedings of IEEE Conference on Circuits, System, Computers and Communications*, pp. 269-273, Athens, Greece, July 1999. .
- [80] Bagnato, Maselli, Petrioli, and Vicari, "Performance Analysis of Anti-Collision Protocols for RFID Systems", *VTC Spring. IEEE 69th conference publication*, pp: 1-5
- [81] Don R. Hush and Cliff Wood, "Analysis of Tree Algorithms for RFID Arbitration," In *IEEE International Symposium on Information Theory*, 1998.

- [82] J.Myung, W.Lee ,and J.Srivastava, "Adaptive Binary Splitting for Efficient RFID Tag Anti-Collision, " IEEE Comm. Letters, vol. 10, no. 3, pp. 144-146, Mar'2006.
- [83] J. Myung, and W. Lee, "Adaptive Binary Splitting: A RFID Tag Collision Arbitration Protocol for Tag Identification," IEEE International Conference on Broadband Networks, vol. 1, pp. 347- 355, Oct 2005.
- [84] Naval Bhandari, Anirudha Sahoo and Sridhar Iyer, "Intelligent query tree protocol to improve RFID tag Read efficiency", ICIT '06. 9th International Conference on Information Technology, 2006.pp.46-51
- [85] C. Law, K. Lee, and K. Y. Siu, "Efficient Memory less protocol for Tag Identification", In Proceedings of the 4th international workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIALM'00), ACM, pp. 75-84, 2000.
- [86] J. Ryu, H. Lee, Y. Seok, and T. Kwon, "A Hybrid Query Tree Protocol for Tag Collision Arbitration in RFID systems", IEEE International Conference on ICC '07, pp. 5981-5986, June 2007.
- [87] L. Liu, Z. Xie, J. Xi, and S. Lai, "An Improved Anti-collision Algorithm in RFID System," Mobile Technology, Applications and Systems, 2nd International Conference, 2005.
- [88] Y. Jiang and R. N. Zhang, "An adaptive combination query tree protocol for tag identification in RFID systems," IEEE Communications Letters, vol. 16, no. 8, pp. 1192–1195, 2012.
- [89] Y.-H. Chen, S.-J. Horng, R.-S. Run et al., "A novel anti-collision algorithm in RFID systems for identifying passive tags," IEEE Transactions on Industrial Informatics, vol. 6, no. 1, pp. 105–121, 2010
- [90] S. M. A. Motakabber, Mohd Alauddin Mohd Ali, Nowshad Amin, "VLSI Design of an Anti-Collision Protocol for RFID Tags", European Journal of Scientific Research ,vol.28 no.4 pp.559-565, 2009
- [91] Yu Song-sen, Zhan Yi-ju, Wang Yong-hua, "RFID Anti-collision algorithm Based on Bi-directional Binary Exponential Index", IEEE International conference on Automation and Logistics, pp: 2917-2921. Aug'2007,

- [92] Yinghua Cui and Yuping Zhao, "A Modified Q-parameter Anti-collision scheme for RFID systems", Proceedings of the IEEE International Conference on Ultra Modern Telecommunications & Workshops October 12-14, Beijing, China,2009,
- [93] J. H. Choi, D.Lee and H. Lee, "Query Tree-based reservation for efficient RFID tag anti-collision", IEEE Communications Letters, vol. 11, pp.85-87, 2007.
- [94] Ching-Nung Yang and Jyun-Yan He, "An Effective 16-bit Random Number Aided Query Tree Algorithm for RFID tag Anti-collision", IEEE Communications Letters, vol.15, No.5 2011.
- [95] E.Y. Choi, D.H. Lee, J.I. Lim, "Anti-cloning protocol suitable to EPC global Class-1 Generation-2 RFID systems", Computer Standards and Interfaces 31,vol.6,pp.1124–1130. 2009
- [96] "EPCTM Radio-Frequency Identification Protocols Class- 1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz Version 1.0.8," EPC global, Dec. 2004.
- [97] "Draft protocol specification for a 900 MHz Class0 Radio Frequency Identification Tag," Auto-ID Center, Feb 2003.
- [98] S. Sarma, D. Brock, and D. Engels, "Radio Frequency Identification and the Electronic Product Code," IEEE Micro, vol. 21, no. 6, pp. 50- 54, Nov.2001.
- [99] Thing Magic, version 1.0, "A user guide EPC Gen-2", www.thingmagic.com, April 2005,
- [100] Wikipedia, "EPCglobal," <http://en.wikipedia.org/wiki/EPCglobal>. 2010
- [101] Wikipedia, "Electronic Product Code," http://en.wikipedia.org/wiki/Electronic_Product_Code, 2011.
- [102] Wikipedia, "EPC global Network," [http:// en.wikipedia.org/ wiki/EPCglobal_Network](http://en.wikipedia.org/wiki/EPCglobal_Network), 2010.
- [103] EPC Global, "The EPC global Architecture Framework," [http:// www.gs1.org/gsm/kc/epcglobal/architecture/architecture_ 1_ 4-framework-20101215.pdf](http://www.gs1.org/gsm/kc/epcglobal/architecture/architecture_1_4-framework-20101215.pdf),2010.
- [104] T. Staake, F. Thiesse, E. Fleisch, "Extending the EPC network—the potential of RFID in anti-counterfeiting", Proceedings of the ACM Symposium on Applied Computing, Santa Fe, New Mexico, 2005.

- [105] ICC Counterfeiting Intelligence Bureau, “Anti-Counterfeiting Technology Guide”, ICC Commercial Crime Services, 2005.
- [106] H. Bhatt, B. Glover, “RFID Essentials”, 1st ed., O’Reilly, Sebastopol, CA, 2006.
- [107] S. Lahiri, “RFID Sourcebook”, Pearson plc, Upper Saddle River, NJ, 2006.
- [108] EPC global, Inc., “RFID Implementation Cookbook”, Available at: <http://www.epcglobalinc.org/what/cookbook>. 2006
- [109] Vogt, H., “Efficient Object Identification with Passive RFID Tags”, Proceedings of the First International Conference on Pervasive Computing, Springer-Verlag London, UK. 2002
- [110] Jae-Ryong Cha and Jae-Hyun Kim, “Novel anti-collision algorithms for fast object identification in RFID system”, Proceedings of the 11th International Conference on Parallel and Distributed Systems, Sch. of Electr. & Comput. Eng., Ajou Univ., Suwon. 2005
- [111] WT Chen and Guan-Hung LIN, “An efficient Anti-Collision Method for Tag Identification in a RFID System”, IEICE Trans. Commun., vol.E89–B, No.12, pp.3386-3392, 2006.
- [112] Bo Li, Yuqing Yang and Junyu Wang, “AUTO ID LABS White paper” WP-Hardware-047, 2009
- [113] E.W.T. Ngai, K.K.L. Moon, F.J. Riggins, C.Y. Yi, “RFID research: an academic literature review (1995–2005) and future research directions”, International Journal of Production Economics. vol 112 no.2, pp. 510–520. 2008
- [114] Mary Catherine O'Connor, “Gen 2 EPC Protocol Approved as ISO 18000-6C”, RFID Journal, Jul 2006
- [115] E.Y. Choi, D.H. Lee, J.I. Lim, “Anti-cloning protocol suitable to EPC global Class-1 Generation-2 RFID systems”, Computer Standards and Interfaces, vol 31, no.6, pp. 1124–1130. Nov’2009
- [116] D.N. Due, J. Park, H. Lee, K. Kim, “Enhancing security of EPC global GEN-2 RFID tag against traceability and cloning”, in: Proceedings of the 2006 Symposium on Cryptography and Information Security, 2006.
- [117] EPC global, Inc., “EPC global Standards Overview”, Available at: <http://www.epcglobalinc.org/standards>. 2009

- [118] R. Weinstein, "RFID: a technical overview and its application to the enterprise", IT Professional, vol.7,no.3, pp. 27–33. 2005
- [119] "EPC Tags Subject to Phone Attacks" RFID journal White paper, 2012.
- [120] "Data Protection Technical Guidance Radio Frequency Identification: Information Commissioner's Office" [ICO] 2013
- [121] "RFID Data Security" RFID journal White paper, 2011
- [122] Debasis Das, Rajib Misra: "Programmable Cellular Automata Based Efficient Parallel AES Encryption Algorithm", Int. Journal of Network Security & its Applications (IJNSA),vol.3,No.6, pp.197-208, Nov. 2011
- [123] S. Wolfram, "Cryptography with cellular automata," in Advances in Cryprology-Crypto '85 (Springer-Verlag Lecture Notes in Computer Science 218), pp. 429-432. 1986
- [124] P. Dasgupta, S. Chottopadhyay and I. Sengupta, "An Asic for cellular automata based message authentication". Conference proceedings of thirteenth IEEE International Conference on VLSI Design,. pp. 538 – 541; 2000
- [125] R.-J. Chen, Y.-T. Lai and J.-L. Lai, "Architecture design and VLSI hardware implementation of image encryption/decryption system using re-configurable 2-D Von Neumann cellular automata," in Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS '06), Island of Kos, Greece,. pp. 153–156, May 2006
- [126] T. K. York, Ph. Tsalides, B. Srisuchinwong, P. J. Hicks, and A.Thanailakis, "Design and VLSI implementation of a mod- 127 multiplier using cellular automaton-based data compression techniques," in IEEE Proc. E. Comput. Digit. Tech., vol. 138, no. 5, pp. 351-356. 1991
- [127] P. D. Hortensius, R. D. Mcleod, W. Pries, D. M. Miller, and H. C.Card, "Cellular automata based pseudorandom number generators for built-in self-test," IEEE Trans. Cornput.-Aided Design, vol. 8, no 8, pp.842-59, Aug. 1989.
- [128] P. Tzionas, Ph. Tsalides, and A. Thanailakis, "Design and VLSI implementation of a pattern classifier using pseudo @D cellular automata," IEEE Proc. G, vol. 139, no. 6, pp. 661-668, Dec. 1992.

- [129] D. Roy Chawdhury, I. Sengupta, S. Basu, and P. Pal Chaudhuri, "Cellular automata based error correcting codes (CAECC)," *IEEE Trans.Comput.*, vol. 43, no. 6, pp. 759-764, June 1994.
- [130] B. Srisuchinwong, Ph. Tsalides, T. A. York, P. J. Hicks, and A.Thanailakis, "VLSI implementation of mod-p multipliers using homomorphisms and hybrid cellular automata," *IEEE Proc.*, vol. 139. No. 6, pp. 486-490, Nov. 1992.
- [131] Ph. Tsalides, T. A. York, and A. Thanailakis, "Pseudorandom number generators for VLSI systems based on linear cellular automata," in *IEEE Proc. E. Comput. Digit. Tech*, vol. 138, no. 4, pp. 241-249. 1991
- [132] Ph. Tsalides, "Cellular automata based built-in self test structures for VLSI systems," *Electron. Lett.* vol. 26, no. 17, pp. 1350-1352. 1990.
- [133] S. Nandi, B. K. Kar, and P. Pal Chaudhuri, "Theory and Applications of Cellular Automata in Cryptography ", *IEEE Trans. on Computers*, vol. 43, no. 12, pp. 1346-1357, Dec 1994
- [134] Petre Anghelescu, "Programmable Cellular Automata Encryption Algorithm Implemented in Reconfigurable Hardware", *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, vol. 2, no. 2, pp.73-78,2013
- [135] R.-J. Chen, "Novel SCAN-CA-based Image security system using SCAN and 2-D Von Neumann cellular automata", *Signal Processing: Image Communication*, Elsevier,vol.25, pp.413-426; 2010
- [136] Jun-Jie Peng, Liang Teng, and Yi Jin, "Realization of a Tri-Valued Programmable Cellular Automata with Ternary Optical Computer", *Int. Journal Of Computing and Information*. vol. 9, no. 2, pp. 304–311; 2012
- [137] Rong-Jian Chen, Jui-Lin Lai, "Image security system using recursive cellular automata substitution", *Pattern Recognition*, Elsevier, vol.40 pp. 1621 – 1631;2007
- [138] Adam S.W. Man, Edward S. Zhang, Vincent K.N. Lau, C.Y. Tsui, and Howard C. Luong, "Low Power VLSI Design for a RFID Passive Tag baseband System Enhanced with an AES Cryptography Engine" Published in: *RFID Eurasia*, 1st Annual Conference, pp.1– 6; Sept. 2007

- [139] Ignacio Algreto-Badillo, Claudia Feregrino-Urbe, René Cumplido, Miguel Morales-Sandoval, "Efficient hardware architecture for the AES-CCM protocol of the IEEE 802.11i standard", Elsevier, Computers and Electrical Engineering, vol.36, pp 565–577; 2010.
- [140] Wayne Wolf, "Modern VLSI Design; 4th edition", PHI Learning Private Limited, 2009.
- [141] Stephen Brown and Zvonko Vranesic, "Digital Logic design", Tata McGraw Hill Publication' 2008.
- [142] Hongyuan Zha, Xiang Ji, "Localization algorithms for wireless sensor network systems" Doctoral Dissertation Pennsylvania State University, University Park, PA, USA, 2004
- [143] L. Lazos and R. Poovendran. HiRLoc, "High-Resolution Robust Localization for Wireless Sensor Networks". IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, Feb.2006
- [144] Loukas Lazos and Radha Poovendran Srdjan Capkun, "ROPE: Robust Position Estimation in Wireless Sensor Networks" IEEE International Symposium on Information Processing in Sensor Networks, IPSN, pp.324-331, April 2005
- [145] Liu, C., Fang, D., Yang, Z., Chen, X., Wang, W., Xing, T., An, N. and Cai, L. "RDL: a novel approach for passive object", Localization in WSN Based on RSSI'IEEE ICC 2012 – Ad-hoc and Sensor Networking Symposium, pp.586–590. 2012
- [146] Farias, M.S., Nedjah, N. and De Macedo Mourelle, L. "A hardware architecture for subtractive clustering", Int. J. of High Performance Systems Architecture, vol. 3, Nos. 2/3, pp.167–173. 2011
- [147] Da Silva, M.V.C., Nedjah, N. and de Macedo Mourelle, L. "Efficient mapping of an image processing application for a network-on-chip based implementation", Int. J. of High Performance Systems Architecture, vol. 2, no. 1, pp.46–57,2009
- [148] Huang, Y. "Obstacle detection in urban traffic using stereovision", Proceedings of International IEEE Conference on Intelligent Transportation Systems, pp.357–362. 2005

- [149] Khan, H.M., Olariu, S. and Eltoweissy, M. "Efficient single-anchor localization in sensor networks", Proceedings of the Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS '06), pp.1–10,2006
- [150] Jiang, B., Han, K., Ravindran, B. and Cho, H. "Energy efficient sleep scheduling based on moving directions in target tracking sensor network", IEEE IPDPS, pp.1–10, April. 2008
- [151] Junaid Ansari, Dmitry Pankin and Petri Mahonen, "Radio-Triggered Wake-ups with Addressing Capabilities for Extremely Low Power Sensor Network Applications". presented in IEEE PIMRC 2008,
- [152] Byrne, J., Cosgrove, M. and Mehra, R. "Stereo based obstacle detection for an unmanned air vehicle", Proceedings of IEEE International Conference on Robotics and Automation, pp.2830–2835. 2006
- [153] Eshan Nagrath, Kumudesh Jain, Ankit Jaiswal, Sanjiv Mishra and Vikas Srivastava, "Performance of DPSK modulation Scheme using AWGN channel for CDMA system", VSDR-IJEECE, vol.1(1) pp.21-29,2011.
- [154] Herbert Taub and Donald L. Schilling, "Principles of Communication Systems" 2nd Edition, pp-249-319, 1998
- [155] J. E. Volder, "The CORDIC trigonometric computing technique," IRE Trans. Electron. Computers, vol. EC-8, , pp. 330–334, Sept. 1959
- [156] J. E. Volder, "The birth of CORDIC," J. VLSI Signal Process., vol. 25. pp. 101–105, 2000
- [157] J. S. Walther, "A unified algorithm for elementary functions," in Proc. 38th Spring Joint Computer Conf., Atlantic City, NJ, pp.379–385. , 1971
- [158] J. S. Walther, "The story of unified CORDIC," J. VLSI Signal Process., vol. 25, no. 2, pp. 107–112, June 2000
- [159] P. K. Meher, J. Valls, T-B. Juang, K. Sridharan and K. Maharatna, " 50 Years of CORDIC: Algorithms, Architectures and Applications", IEEE Transactions on Circuits & Systems-I: Regular Papers. 2009

- [160] W. Han, Z. Youxi, and L. Xiaokang, "A Parallel Double-Step CORDIC Algorithm for Digital Down Converter," in Communication Networks and Services Research Conference, 2009
- [161] E. O. Garcia, R. Cumplido and Miguel Arias, "Pipelined CORDIC Design on FPGA for a Digital Sine and Cosine Waves Generator," 2006.
- [162] Z. Zhao, Y. Shen, and Y. Bai, "Design and implementation of the BPSK modem based on software defined radio," in Proceedings of the 1st International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC'11), pp. 780–784, Los Alamitos, Calif, USA, October 2011.
- [163] Song W , Yao Q (2010). Design and Implement of QPSK Modem Based on FPGA. ICCSIT 2010 pp. 599-601;Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on (Volume:9)
- [164] Wenmiao Song, Jingying Zhang, Qiongqiong Yao, "Design And Implement Of BPSK Modulator And Demodulator Based On Modern DSP Technology," IEEE International Symposium. pp 1135-1137, 2009.
- [165] Hiroshi Harada, Ramjee Prasad, "Simulation and Software Radio for Mobile Communications," Artech House Publishers Bk&CD-Rom edition. pp.90-93,2002.
- [166] Kishore Padmaraju ; Noam Ophir ; Sasikanth Manipatruni ; Carl B. Poitras "DPSK modulation using a microring modulator" CLEO: 2011 - Laser Science to Photonic Applications [IEEE] 2011 ;Page(s):1 - 2
- [167] Lathi B.P. "Communication Systems", John Wiley & Sons pp-598-600,2012.
- [168] R.P.Singh and S.D.Sapre, "Communication Systems-Analog and Digital",pp-482-502,2006
- [169] Ziemer, R.E.; Tranter, W.H. "Principles of Communications Systems, Modulation, and Noise", John Wiley & Sons: New York, NY, USA, 2010.
- [170] Haytham Azmia, Hamed Elsimary, M. Ibrahim Youssef, Ahmad Safwat, "FPGA based multi-standard configurable FSK demodulator" Integration, the VLSI journal, vol.36. pp. 145–154,(2003).

- [171] M.Garrido and J.Grajal, "Memoryless CORDIC for FFT computation" ICASSP 2007.
- [172] Huan Li and Yan Xin, "Modified CORDIC Algorithm and Its Implementation Based on FPGA",IEEE conference proceedings, ICINIS. pp.618-621,2010.
- [173] Uwe Meyer-Baese. "Digital Signal Processing with Field Programmable Gate Arrays". Springer-Verlag, New York, Inc., Secaucus, NJ, USA, pp. 70-75, 2007.
- [174] T.-Y. Sung, "Memory-efficient and high-speed split-radix FFT/IFFT processor based on pipelined CORDIC rotations," Proc. IEEE Vision, Image Signal Process., vol. 153, no. 4, pp. 405–410, Aug. 2006
- [175] Ray Andraka. "A survey of CORDIC algorithms for FPGA based computers". Proceedings of the 1998 ACM/SIGDA sixth international symposium on Field programmable gate arrays , pp 192-200, New York, NY, USA, 1998. ACM Press.
- [176] F. Angarita, A. Perez-Pascual, T. Sansaloni, and J. Vails, "Efficient FPGA Implementation of CORDIC Algorithm for Circular and Linear Coordinates," International Conference on Field Programmable Logic and Applications, pp. 535–538, Aug 2005.
- [177] Ansari, J.Pankin, D.and Mahonen, P. "Radio-triggered wake-ups with addressing capabilities for extremely low power sensor network applications", 19th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2008).