Technical Report, IDE0603, January 2006

Implementation Study of IEEE 802.15.4

Master’s Thesis in

Electrical Engineering\textsuperscript{1}, Computer Systems Engineering\textsuperscript{2}

Assad Hussain\textsuperscript{1}, Muhammad Kazim Hafeez\textsuperscript{2}
Implementation Study of IEEE 802.15.4

Master’s thesis in
Computer Systems Engineering / Electrical Engineering

January 2006

School of Information Science, Computer and Electrical Engineering
Halmstad University
Box 823, S-301 18 Halmstad, Sweden

©2006
Assad Hussain, Muhammad Kazim Hafeez
All Rights Reserved
Description of cover page picture: Active RFID from Free2move
God could not be everywhere and therefore He made parents.

We Miss Them
And
Love Them
Don’t we?

TO OUR PARENTS
Preface

The document in your hand is a Master’s thesis entitled “Implementation Study of IEEE 802.15.4”. This is a project proposal from the Free2move company, which has strong industrial research relations with Halmstad University. This thesis was carried out at the Computing and Communication laboratory at the School of Information Science, Computer and Electrical Engineering in Halmstad University, under the supervision of CEO of Free2move, Per-Arne Wiberg.

We would like to express our gratitude to our supervisor Per-Arne Wiberg for his guidance throughout this thesis, Latef Berzenji for correcting the language of the thesis. We are also very grateful to Urban Bilstrup, Lecturer at Halmstad University for his time to time guidance towards our project.

Assad Hussain, Muhammad Kazim Hafeez
Halmstad University, January 2006
Abstract

This thesis is analysis-based survey in which our task was to find out the suitability of IEEE 802.15.4 for the RFID systems in terms of power. We studied the different RFID systems. We analyzed the IEEE 802.15.4 to see how much this protocol can facilitate the RFID application, but we just considered the 2.4 GHz physical band as Free2move uses this band for its RFID products. Since semi-passive\textsuperscript{1} RFIDs are the closest competitors of the active RFID, so we also compared the IEEE 802.15.4 with ISO 18000-4 (mode2) to find out their pros and cons.

We also tried to evaluate the hardware architecture proposed by Free2move. We compared proposed hardware components with other competitors available in the market. The main point of focus during hardware evaluation remained its power efficiency. As concluding part we have proposed an idea for using the IEEE 802.15.4 standard in semi-passive RFIDs.

\textbf{KEYWORDS:} IEEE 802.15.4, active RFID, passive RFID, semi-passive RFID, battery-assisted RFID

\footnotesize 1 Terms semi-active, semi-passive and battery-assisted passive refer to the same category of RFID systems so they be used interchangeably

---

iii
## Contents

1 INTRODUCTION

1.1 GOAL 1
1.2 COMPANY’S PROFILE 2

2 RELATED WORK 3

2.1 MEDIUM ACCESS MECHANISM 5

3 DESCRIPTION OF DIFFERENT RFID SYSTEMS

3.1 PRIMARY CLASSIFICATION OF RFID 7
   3.1.1 PASSIVE RFID SYSTEMS 7
   3.1.2 ACTIVE RFID SYSTEMS 7
   3.1.3 SEMI-PASSIVE RFID SYSTEMS 7

3.2 COMPONENTS OF RFID SYSTEMS
   3.2.1 COMPONENTS OF PASSIVE RFID SYSTEM 8
      3.2.1.1 FREQUENCY BASED CLASSIFICATION 9
         LOW FREQUENCY PASSIVE RFID 9
         HIGH FREQUENCY PASSIVE RFID 10
         ULTRA HIGH FREQUENCY PASSIVE RFID 10
      3.2.1.2 READ/WRITE RANGE AND SPEED 10
      3.2.1.3 COMMUNICATION MECHANISMS 11
   3.2.2 COMPONENTS OF ACTIVE RFID SYSTEM 12
   3.2.3 COMPONENTS OF SEMI-PASSIVE RFID SYSTEM 13
   3.2.4 TYPES OF TAG MEMORY 14

4 DESCRIPTION OF PROTOCOLS

4.1 SPECIFICATION OF IEEE 802.15.4 15
   4.1.1 OVERVIEW 15
   4.1.2 FRAME STRUCTURE 16
      4.1.2.1 BEACON FRAME 17
      4.1.2.2 DATA FRAME 17
      4.1.2.3 ACKNOWLEDGE FRAME 18
      4.1.2.4 MAC COMMAND FRAME 19
   4.1.3 PHYSICAL SPECIFICATION 19
   4.1.4 MEDIUM ACCESS CONTROL LAYER 20

4.2 SPECIFICATION OF ISO 18000-4 25
   4.2.1 MODE 2: BATTERY ASSISTED PASSIVE TAGS 25
   4.2.2 COMMUNICATION CHANNELS 25
      4.2.2.1 NOTIFICATION CHANNEL 26
      4.2.2.2 COMMUNICATION CHANNEL 26
      4.2.2.3 SPECTRUM CHECK CHANNEL 26

5 CONTRIBUTIONS

5.1 PROTOCOLS’ ANALYSIS 27
   5.1.1 LOW POWER CONSUMPTION 27
   5.1.2 OPERATING FREQUENCY AND RANGE 27
   5.1.3 SPREAD SPECTRUM TECHNIQUES 27
   5.1.4 ADAPTIVE DUTY CYCLE 28
List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Different Parametric Comparison between WLANs and WPANs</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Collision Problem in Pure Aloha</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>Collision Problem in Slotted Aloha</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>Block Diagram of Passive RFID System</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>Functional Components of Passive RFID Tag</td>
<td>9</td>
</tr>
<tr>
<td>6</td>
<td>Inductive coupling (load modulation)</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>Back Scattered Modulation</td>
<td>11</td>
</tr>
<tr>
<td>8</td>
<td>Block Diagram of Active RFID System</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>Block Diagram of Semi Passive RFID System</td>
<td>13</td>
</tr>
<tr>
<td>10</td>
<td>IEEE 802.15.4 Protocol Stack</td>
<td>15</td>
</tr>
<tr>
<td>11</td>
<td>IEEE 802.15.4 star and peer-to-peer topologies</td>
<td>16</td>
</tr>
<tr>
<td>12</td>
<td>Beacon Frame Structure</td>
<td>17</td>
</tr>
<tr>
<td>13</td>
<td>Data Frame Structure</td>
<td>18</td>
</tr>
<tr>
<td>14</td>
<td>Acknowledgement Frame Structure</td>
<td>18</td>
</tr>
<tr>
<td>15</td>
<td>MAC Command Frame Structure</td>
<td>19</td>
</tr>
<tr>
<td>16</td>
<td>Superframe Structure</td>
<td>20</td>
</tr>
<tr>
<td>17</td>
<td>Communication to Coordinator from Device in Beacon Enabled Network</td>
<td>20</td>
</tr>
<tr>
<td>18</td>
<td>Communication to Coordinator from Device in Non-Beacon Network</td>
<td>21</td>
</tr>
<tr>
<td>19</td>
<td>Communication from Coordinator to Device in Beacon Enabled Network</td>
<td>21</td>
</tr>
<tr>
<td>20</td>
<td>Communication to Device from Coordinator in Non-Beacon Network</td>
<td>21</td>
</tr>
<tr>
<td>21</td>
<td>Unslotted CSMA</td>
<td>23</td>
</tr>
<tr>
<td>22</td>
<td>Slotted CSMA</td>
<td>24</td>
</tr>
<tr>
<td>23</td>
<td>Frame Structure ISO 18000-4 mode 2</td>
<td>25</td>
</tr>
<tr>
<td>24</td>
<td>Traditional IEEE 802.15.4, 2.4 GHz Channels 11-26</td>
<td>32</td>
</tr>
<tr>
<td>25</td>
<td>Modified IEEE 802.15.4, 2.4 GHz Channels 11-26</td>
<td>33</td>
</tr>
<tr>
<td>26</td>
<td>Communication to reader in beacon-less Modified IEEE 802.15.4</td>
<td>33</td>
</tr>
<tr>
<td>27</td>
<td>Communication from reader in beacon-less Modified IEEE 802.15.4</td>
<td>34</td>
</tr>
<tr>
<td>28</td>
<td>Communication to reader in beacon-enabled Modified IEEE 802.15.4</td>
<td>34</td>
</tr>
<tr>
<td>29</td>
<td>Communication from reader in beacon-enabled Modified IEEE 802.15.4</td>
<td>35</td>
</tr>
<tr>
<td>30</td>
<td>Semi-Passive RFID with Temperature Sensor powered from reader</td>
<td>36</td>
</tr>
</tbody>
</table>
# List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EPC Tags’ Classification</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>Properties Comparison of Different Frequencies</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>Comparison of Pure Active and Semi Passive RFID</td>
<td>14</td>
</tr>
<tr>
<td>4</td>
<td>Physical Specification of IEEE 802.15.4</td>
<td>19</td>
</tr>
<tr>
<td>5</td>
<td>Characteristics of RF chips</td>
<td>30</td>
</tr>
<tr>
<td>6</td>
<td>MCU Characteristics</td>
<td>31</td>
</tr>
<tr>
<td>7</td>
<td>Comparison of hardware in terms of power efficiency</td>
<td>32</td>
</tr>
</tbody>
</table>
Acronyms and Abbreviations

ACK Acknowledgement
BE Backoff Exponent
BO Beacon Order
BPSK Binary Phase Shift Keying
CAP Contention Access Period
CCA Clear Channel Assessment
CFP Contention Free Period
CSMA/CA Carrier Sense Multiple Access Collision Avoidance
CTS Clear to Send
CW Contention Window
DSSS Direct Sequence Spread Spectrum
EPC Electronic Product Code
FFD Full Functional Device
FHSS Frequency Hopping Spread Spectrum
GMSK Guassian Minimum Shift Keying
GTS Guaranteed Time Slot
HF High Frequency
IEEE Institute of Electrical and Electronics Engineering
ISM Industrial Scientific and Medical
ISO International Organization for Standardization
LAN Local Area Network
LF Low Frequency
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLC</td>
<td>Logical Link Control</td>
</tr>
<tr>
<td>LR</td>
<td>Low Rate</td>
</tr>
<tr>
<td>MAC</td>
<td>Medium Access Control</td>
</tr>
<tr>
<td>MCU</td>
<td>Micro Controller Unit</td>
</tr>
<tr>
<td>MFR</td>
<td>MAC Footer</td>
</tr>
<tr>
<td>MHR</td>
<td>MAC Header</td>
</tr>
<tr>
<td>MPDU</td>
<td>MAC Protocol Data Unit</td>
</tr>
<tr>
<td>MSDU</td>
<td>MAC Service Data Unit</td>
</tr>
<tr>
<td>NB</td>
<td>Number of Backoff</td>
</tr>
<tr>
<td>O-QPSK</td>
<td>Offset Quadrature Phase Shift Keying</td>
</tr>
<tr>
<td>PHR</td>
<td>Physical Header</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical</td>
</tr>
<tr>
<td>POS</td>
<td>Personal Operating Space</td>
</tr>
<tr>
<td>PPDU</td>
<td>Physical Protocol Data Unit</td>
</tr>
<tr>
<td>PSDU</td>
<td>Physical Service Data Unit</td>
</tr>
<tr>
<td>R/O</td>
<td>Read Only</td>
</tr>
<tr>
<td>R/W</td>
<td>Read and Write</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RFD</td>
<td>Reduced Functional Device</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>RTS</td>
<td>Ready To Send</td>
</tr>
<tr>
<td>SHR</td>
<td>Synchronized Header</td>
</tr>
<tr>
<td>SO</td>
<td>Super Frame Order</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>TDMA</td>
<td>Time Division Multiple Access</td>
</tr>
<tr>
<td>UHF</td>
<td>Ultra High Frequency</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WPAN</td>
<td>Wireless Personal Area Network</td>
</tr>
</tbody>
</table>
Introduction

1. Introduction

Radio Frequency Identification (RFID) is a promising technique that provides wireless communication between reader and tag. Allied Forces used RFID for the first time ever in history to distinguish between their own aircraft and those of the Germans. Applications of RFID range from home appliances to manufacturing industry.

Introduction of barcodes helped manufacturers and retailers to keep track of their inventory. They were well informed about the sold items as well as the items available in stock. Barcodes are considered as products’ fingerprints. They are also helpful to enhance the check out process at store outlets. With the passage of time, passing every product with barcode, through the scanner, was becoming a constant nuisance for retailers, so the idea of a new and more easy to use technology called RFID was introduced.

The new research in this field helped to drop the cost to a level that RFID could be introduced to new applications and outclass existing applications [31]. Now, barcodes are replaced with tags where each tag contains a special circuit containing some information. The advantage of RFID is that it does not need line of sight to operate, and can work in harsh environments where most of the tags can be read through a tag-reader called reader at a distance [32]. This saves us a lot of time, since we don’t have to pass each product through a reader. This is not all, RFID also accommodates the situations where the product passes through different stages of manufacturing or supply chain management and the information on the tag need to be amended / appended. This could be accomplished by using a writeable tag.

Nowadays RFIDs are used in domains like interactive toys, toll collecting systems, animal tracking, sensor networks and supply chain management.

1.1 Goals

To date different vendors are using different Medium Access Control (MAC) protocols in their RFID systems; most of them are custom made and are not interoperable. Although there are some available standards like Electronic Product Code (EPC) and International Organization for Standardization (ISO) that focuses on different aspects of RFIDs, efforts to develop a single standard never stepped forward until 2003 when IEEE launched its first standard that focuses on the MAC layer issues of the low data rate, ultra-low power consumption networks. IEEE 802.15.4 addresses the issues regarding MAC and Physical layers for ultra-low power and low data rate Wireless Personal Area Networks. Active RFIDs also belong to this class of networks so this standard can be used to compensate its issues regarding MAC and physical layers.

Free2move AB, a Swedish company and the proposer of this master’s thesis, wants us to investigate an active RFID system using Chipcon 2420 as RF transceiver chip and Atmel 128L as its MCU since the Chipcon 2420 is not available with full implementation of IEEE 802.15.4. This system will be operative on 2.4 GHz industrial, scientific and medical (ISM) band and will be based on the star topology using single-hop, point-to-point link between the tag and the reader. We will consider these parameters in our thesis.
As the goals of our Master’s thesis we will analyze the suitability of IEEE 802.15.4 for RFID applications. For that purpose we will study this protocol and analyze it with another protocol “ISO 18000-4 mode 2”. The main focus of our analysis would be the power efficiency of the protocols.

Second task of our thesis is to evaluate the proposed hardware in terms of power consumption. For that purpose we will take the hardware from other vendors and compare the functional characteristics of those hardware components with the proposed components to get a clear picture of the power efficiency.

1.2 Company’s Profile
Researchers at Halmstad University founded Free2move. The company still has tight connections to academia and is participating in a number of research projects at Halmstad University. This gives Free2move a cutting edge competence in the wireless communication area.

The company is a spin-off company from research activities at Halmstad University. The products provided by Free2move can be customized to fit a variety of applications.

Free2move integrates RFID technology and Bluetooth for logistic applications. This means reader without batteries are placed in transported goods and information can be sent to a network via Bluetooth enabled readers. These technologies are the cornerstone of the competence of Free2move.

Free2move's product portfolio ranges from high performance surface mounted Bluetooth modules to Local Area Network (LAN) access points, active RFID systems and embedded Linux systems with Bluetooth access.
2. Related Work

Perhaps the cables, installation and maintenance costs led to the idea of wireless networks, which resulted in first wireless LAN standard IEEE 802.11[1], with the data rate ranging from 2-54 Mbps in different variants of Wireless LAN [2,3,4]. Later on a new class of network called Wireless Personal Area Networks (WPAN), that was targeted for less data rate of the order of 1Mbps and less, was realized. This carries standard of IEEE 802.15.1, is normally known as Bluetooth [5]. WPANs hold another flavor, targeting at high data rates for image and multimedia applications, known as High Rate Wireless Personal Area Network which carries the standard of IEEE 802.15.3 [6].

The problem with these Wireless Local Area Networks (WLANs) and WPANs are that they are either used to achieve high data rates or carry power hungry protocols that are not suitable for the RFID applications, which require data rates of the order of 0.25 Mbps and less. Therefore a new set of protocol was needed that could work in resource scarce environment like low processing power, low memory and low power consumption. Figure 1 shows the hierarchy of different WLAN and WPAN standards in terms of data rate and power consumption in operation.

![Figure 1: Different Parametric Comparison between WLANs and WPANs](image)

Earlier work on the RFID specification was based on the two standards called ISO and EPC that came from two different organizations. Both of the standards were closed, which means they were developed to meet the needs of a particular application of that organization rather than an open (generic) protocol that could work well with all or most of the applications of RFIDs. Many Organizations developed their own specification calling them as standards. Moreover efforts were never made to merge these standards into a single one, which led to the growth of both the standards in parallel. Therefore the devices using these two different sets of standards were never interoperable. In some cases two protocols from the same organization were not even backward compatible.
These specifications mainly focused on two different aspects of standardization: the format of the code and the operating frequencies to carry these codes. EPC mainly focuses on defining the format and data-structure of the product code while ISO emphases on air interface.

EPC standards started with EPC class 0, which was a Ultra High Frequency (UHF) based and supported back-scattered modulation and read only tag with 64 bit EPC code and 81 bit of total length, that can be programmed by the manufacturer. It was operated on 860-930 MHz with reading range of 3 meters. In EPC class 0, an 80 bit address was used as tag identification which resulted in a waste of power and higher cost as the reader was able to identify only a couple of thousand tags at a time which could be achieved with a 12 bit code easily [7].

The class 0 was later improved to class 1 with 2 subclasses in it. In generation 1 of class 1 most of the features remained the same but with additional security features in terms of password and increased reading range to 10 m. The memory can now be programmed by the tag users once, but it can be read as many times as desired [8]. This provides additional security features to the tag users who don’t want to reveal the product code to tag manufacturers. For generation 2 which is 8 times faster than generation 1, which means the increase number of tags can be read per unit time, tags are identified by 16-bit random numbers and not with tag-id as was the case in Class 0. A password is required for read and write functionality. Both generations operate on the same frequency as that of class 0 but provide 96 bits of data capacity.

<table>
<thead>
<tr>
<th>EPC Class</th>
<th>Definition</th>
<th>Programming</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 0</td>
<td>Read Only Passive Tags</td>
<td>Programmed once during manufacturing</td>
</tr>
<tr>
<td>Class 1</td>
<td>Write Once Read Many Passive Tags</td>
<td>Programmed once by customer sometime after manufacturing</td>
</tr>
<tr>
<td>Class 1-Gen 2</td>
<td>Write Once Read Many Passive Tags</td>
<td>Programmed once by customer sometime after manufacturing</td>
</tr>
<tr>
<td>Class 2</td>
<td>Rewriteable Passive Tags</td>
<td>Can be programmed many times</td>
</tr>
<tr>
<td>Class 3</td>
<td>Semi Passive Tags</td>
<td></td>
</tr>
<tr>
<td>Class 4</td>
<td>Active Tags</td>
<td></td>
</tr>
</tbody>
</table>

*Table 1: EPC Tags' Classification [9]*

Class 2 operates on the same frequencies as before but Read / Write feature is provided which is different from what we had in class 1 tags. In class 1 Write Once Read Many facility was available but in class 2 we can write as many times as desired. Additional security features are also provided in terms of encryption. These features increased the cost of system. Class 3 introduced an entirely new class of RFIDs called semi-passive or “battery assisted passive tags” with Read/Write facility. The semi-passive tag is described in the introductory section. Semi-passive tags offer an additional functionality to be used
with sensors to measure some physical phenomena from the surrounding area like temperature, motion, humidity etc.

Class 4 symbolizes the active RFID communication which means tags do not rely on the reader for power, since both the tag and reader have onboard battery. The tags can talk to each other, so they can develop a very dynamic and self organized network of thousands of nodes. Wireless Sensor Networks fall under this category. EPC classes are summarized in Table 1.

ISO 18000 series covers air interface of radio frequency identification for item management and provides specification for all the popular frequencies from 135KHz to 2.45 GHz. There are 7 parts of 18000 series that specify standard of different frequencies. Most of the 18000 series parameterize different globally accepted frequencies. ISO 18000 focuses on the physical communication between the reader and the tag, which covers protocols, commands and anti-collision schemes involved in item management domain. In ISO 18000-6 [10] two types of anti-collision methods, are used for the available two types; type A employs aloha-based mechanism, which has the deficiency that will be described later in this section, and type B uses adaptive binary tree mechanism. Part 4 of 18000 [11] provides two modes that focuses on two different classes of RFIDs, mode 1 describes about 2.4 GHz back-scattered passive tags, while mode 2 specifies about the battery-assisted passive tags. Anti-collision is achieved by randomizing the repetition time in mode 2.

2.1 Medium Access Mechanisms
Collision and retransmission are two of the major contributors to power waste in wireless networks. When power shortage is inherited in low data rate networks, it demands acute attention. MAC protocols are responsible to address these kinds of issues with the help of some anti-collision algorithm, which can either be deterministic or probabilistic. Aloha comes under the probabilistic category, while binary-tree-walking is a simple example of deterministic algorithm. The previous anti-collision algorithms had deficiencies, so a great deal of power could be lost. In Aloha, Figure 2, where data is sent over single channel, the protocol efficiency is reduced when multiple sources attempt to send data simultaneously over a single channel. If the acknowledgement is not received within period, it will transmit again; the retransmission results in wastage of power and increase the packet delay and reduce throughput.

![Figure 2: Collision Problem in Pure Aloha](image)
This problem is solved by using slotted Aloha, in which the channel is divided into slots, but the slots are not assigned to devices. Each device is free to send data at the beginning of each slot. In case of retransmission it waits for random time and then retransmit the data. To perform these mechanisms devices should be clock synchronized. Collision Problem still persists in this protocol but channel wastage time is reduced to almost 50% as shown in Figure 3. The probability of node being awake at the same slot at which the base station sends data becomes better than pure Aloha.

Another approach to avoid the collision problem is Time Division Multiple Access (TDMA), in which time is divided into slots where one device correspond to one slot. Thus probability of collision is decreased and the node activate only for the duration of 1/N, Where N is number of devices. Power can be wasted if the allocated slot is not utilized [12]
3. Description of Different RFID Systems

3.1 Primary Classification of RFID

The significance of RFID technology is that it leaves us to store and read the information even without the direct contact or line of sight between reader and tag. Since power is an important point of consideration in RFIDs so this is the basis for the primary classification of RFIDs. RFID systems are classified into three categories based on how would they power up the tags. These classes are passive RFID system, active RFID system and semi-passive RFID system.

3.1.1 Passive RFID System

In passive RFID system, the tag which does not have a battery onboard, uses the power of incoming signal from the reader to read out the desired data from the memory and send it back to the reader after processing it. Battery is a scarce resource, which requires a careful trade-off between power and other functional capacities like the distance between tag and reader, communication speed, amount of data to send. Due to the scarcity of the power, the data transmitted are not much more than a Product ID [13]. The same issue persists for the distance between reader and tag. We cannot afford to have a distance of more than three meters between them otherwise the communication will become impossible [31]. Since in passive RFID systems, tags are powered from the signals of reader, the transmitting power in passive RFID systems are 1000 times of active RFID [31]. Passive RFID has potential use in such applications, where either its impossible to replace batteries like skin implantation, or the cost of batteries is too high for the products that are use it.

3.1.2 Active RFID System

In Active RFID system, the tags are self-powered by onboard battery, which is used to process and transmit data. Active RFID tag transmits the data periodically when requested by the reader or sometimes at its own. Passive RFID tags send the data only upon the request of the reader therefore it uses the power from the incoming signal of the reader. Because of the onboard battery the amount of transmitted data and the transmitting range improves, but limited life of battery is the still the major problem faced in the active RFIDs. Unlike passive tags, where the flow of information is from tag to reader, most of the active tags can store the incoming information from the reader.

3.1.3 Semi-Passive RFID System

The third type of system is of hybrid nature with combined attributes from active and passive RFID systems. It has quite unique architecture available, which uses power from incoming signals for radiating them back to reader and battery as source of internal processing. During our discussion we will focus only about active RFID but take into account the semi-passive RFID where needed.
3.2 Components of RFID Systems

3.2.1 Components of Passive RFID Systems

The passive RFID system consists of a tag with no battery on-board and reader that in turn is connected with a server either through RS 232 or some wireless interface as shown in Figure 4. However, the reader has the abundant power supply, which is supplied externally.

Since the reader has to send very strong signals to communicate with multiple tags, so it needs external power supply in abundance. The power of the transmitted signal from the reader is not sufficient to retrieve the data, so a special circuitry called power generating circuit is placed at the tag. The primary component of this circuit is a charge pump that enhances the power of the incoming signal as well as outgoing transmission as shown in Figure 5.
3.2.1.1 Frequency Based Classification

Passive RFID systems are classified into three categories based on the frequency bands in use. These are called Low Frequency Passive RFID (LF Passive RFID), High Frequency Passive RFID (HF Passive RFID) and Ultra High Frequency Passive RFID (UHF Passive RFID). This is due to the fact that different frequencies have distinct properties that makes them suitable for one application and ineligible for others. For example passive RFIDs with low frequency are more suitable for applications with metal surroundings but they cant be used in environment that generates interference. For such environment high frequency and ultra high frequency RFIDs are better to use that withstand the interference. The comparison table is shown in Table 2.

**Low Frequency Passive RFIDs**

The operating frequencies 125 and 134.2 kHz which can penetrate through almost all kinds of materials, remain unaffected by metal surroundings are ideal for animal identification, metal container and vehicular identification. Automotive industry is the largest user of Low Frequency-RFIDs (LF-RFIDs). The reading range encompasses less than one meter [33].

Since the low frequencies are prone to electrical interference, they cannot be used in industrial applications. Since we need a large antenna for low frequencies, the cost as
Implementation Study of IEEE 802.15.4

compared to High Frequency-RFIDs (HF-RFIDs) will increase [28]. Because of low
frequency, they suffer relatively low data rate. Reader can support only one tag at a time.

High Frequency Passive RFIDs
They use 13.56 MHz frequency band. Penetration properties are almost the same as those
of LF-RFIDs but they are not as effective in metal surroundings compared to LF-RFIDs
because of the relative high frequency in use. In contrast to this, higher frequencies can
sustain the electrical interference, thus they can be easily implemented in industrial
applications. It supports reading multiple tags simultaneously. Reading range is increased
to couple of meters [33].

Ultra-High Frequency Passive RFIDs
The frequency in operation for Ultra High Frequency-RFID (UHF-RFIDs) is between
300 MHz and 5.8 GHz. Because of the high frequency, the size of antenna is reduced
while the reading range falls between 3-6 meters, but the performance degrades in
liquids. Supply Chain industry is the biggest vendor which uses these tags [33].

<table>
<thead>
<tr>
<th>Frequency Range</th>
<th>LF 125KHz</th>
<th>HF 13.56MHz</th>
<th>UHF 300-2500MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Range</td>
<td>&lt; 0.5meter</td>
<td>1 meter</td>
<td>3-6 meter</td>
</tr>
<tr>
<td>Typical Current Application</td>
<td>Animal Tracking, vehicular identification</td>
<td>Smart cards, item level tracking</td>
<td>Toll collection</td>
</tr>
<tr>
<td>Performance Degradation</td>
<td>In Electrical Interference</td>
<td>In Metal surrounding</td>
<td>In Liquid</td>
</tr>
<tr>
<td>Data Transfer</td>
<td>Slower</td>
<td>Higher</td>
<td></td>
</tr>
</tbody>
</table>

*Table 2: Properties Comparison of Different Frequencies*

3.2.1.2 Reading/Writing Range and Speed
Read/write range depends on many factors like size and design of transmitting and
receiving antenna and the frequency in use. Application environment also plays an
important role in defining the reading and writing range. Humidity, rain and density of
product and buildings in the area affect the range. The higher the frequency the more it
will be prone to atmospheric absorption.
Tags contain different designs of antenna depending on different types of the products
using them. Circular antennas are omni-directional, so they are preferable where the tags
are not uniformly positioned. These antennas work uniformly independent of the position
of the Reader antenna. In contrast to this the linear antennas are directional thus they are
used in products whose position is aligned with the reader’s antenna.
3.2.1.3 Communication Mechanism
Since passive RFID systems lie in three different frequency domains, their communication mechanism also varies. Broadly speaking, there are two communication mechanisms based on their frequency domains and their communication fields. There are two types of communication fields: far field and near field. The near field extends to the $1/2f\pi$ meter from the signal source and beyond this point lies the far field. [14]

When communication is to occur within a near field, the inductive coupling method is used in which power is transferred from reader to the tag by electromagnetic inductance. Inductive coupling works the same way as the transformer. The reader and tag antennas are made like coils in transformer. The current in the reader’s coil induces a current in tag antenna. The amount of power transferred is proportional to the size of transmitting and receiving antennas. Normally, low and high frequency RFID systems use inductive principle. The data is transmitted by using load modulation. [14] which is shown in Figure 6.

![Inductive coupling (load modulation)](image)

Figure 6: Inductive coupling (load modulation)

When we intend to communicate farther than the near field, capacitive coupling is the option. Capacitive coupled RFID tag uses electric field for obtaining power.

![Back Scattered Modulation](image)

Figure 7: Back Scattered Modulation
UHF-RFIDs use backscatter modulation principle to transmit data between reader and tag as displayed in Figure 7. [14]

3.2.2 Components of Active RFID Systems
Since we have different method of powering the tag in active RFID system so we have a somewhat different set of components in active RFID systems. Figure 8 shows the block diagram of a typical active RFID System. The major difference lies at the tag. Since the tags at active RFID are supported with the battery and they don’t require the incoming signal to activate its communication, so some components that were needed to boost-up the incoming signals like charge pump has been removed. Tags of the active RFID System can transmit the data periodically even when it is not requested by the reader always.

![Figure 8: Block Diagram of Active RFID System](image)

This characteristic makes them ideal for applications like Wireless Sensor Networks, where all nodes are self-organizing and combine to make ad hoc networks. Hundreds,
sometimes thousands of tags can be read in a second even when in motion. Factors that effect the communication range are [15]:

- Available power at the reader to communicate with tags.
- Available power at tags to respond back.
- Atmospheric conditions like fog and rain, which effect the higher frequencies with ease.
- Buildings’ structure in the area.

Active RFID tags work under highly resource scarce environment. To sustain the market of low valued goods, the cost of an active tag should be under 1 dollar [33]. Almost inaccessible operating environment keeps the battery replacement cost very high. Because of this it is impossible to replace the batteries and the life of active tag ends as soon as the battery is exhausted. [16]

3.2.3 Components of Semi-Passive RFID Systems

As described earlier in this section those semi-passive devices are of hybrid nature. Figure 9 shows system diagram of a typical semi-passive RFID system. In certain applications, semi-passive could be a real competitor for active RFID in terms of battery life, which is a major point to be taken into the consideration for battery operated RFID systems.

Communication is a major source of battery consumption in battery assisted RFID which is replaced by back-scattered modulation in semi-passive Systems enhancing the battery life. But all of this is possible for a certain range which is obviously less than the range of an active RFID tag. Battery is consumed only for internal processing which does not utilize much power, but still waking up the tag is a major source of power consumption in semi-passive tags. If the tag does not receive any incoming signals from the reader during the wakeup time, the power is wasted which is the same way as in active RFID systems. Semi-passive RFID can be installed with sensor node(s), which

![Figure 9: Block Diagram of Semi-Passive RFID System](image-url)
could sense the atmospheric activities and store it on the memory of the tag. As semi-passive tags cannot send this information periodically, so it can only be retrieved at some later time when the reader requests this. The different parameters of active and semi-passive RFID systems are given in Table 3.

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Active RFID</th>
<th>Semi-Passive RFID[17]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>868/915MHz and 2.4 GHz</td>
<td>868/915MHz and 2.4 GHz</td>
</tr>
<tr>
<td>Internal Power</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Communication Range</td>
<td>Up to 100 m</td>
<td>Up to 30 m</td>
</tr>
<tr>
<td>Bit Rate</td>
<td>20, 40, 250 Kbps</td>
<td>16 Kbps</td>
</tr>
<tr>
<td>Memory</td>
<td>128 K bytes</td>
<td>4 K bytes</td>
</tr>
<tr>
<td>Typical Current Applications</td>
<td>Asset Tracking, Security Access Control</td>
<td>Asset Tracking, Long Range Identification, Supply Chain automation</td>
</tr>
<tr>
<td>Multi–Tag Collection</td>
<td>1000 tag / sec at 100 mph</td>
<td>7 tags / sec at 3 mph</td>
</tr>
<tr>
<td>Sensor Capability</td>
<td>Continuous monitor and record sensor input, communicate at any time</td>
<td>Continuous monitor and record sensor input, communicate only when tag gets power from Reader</td>
</tr>
</tbody>
</table>

Table 3: Comparison of Pure Active and Semi-Passive RFID

3.2.4 Types of Tag Memory
RFIDs are either used as identification system or supported with sensors to measure some surrounding observations/surveillance. In either case, we need memory to store the data on the tag, which can later be retrieved by the reader, or sometimes the tag itself transmits that information periodically. These memory chips are different in nature. Some of them are read only while others can be read and written multiple times. They can be categorized into three classes; read-only (R/O), read-write (R/W) and write-once-read-many (WORM).

Information in read only chips is programmed at the time of production. They are cheap, and information on them can be read but not altered later on. The read-write chips are costly because we can amend/append information multiple times even after the production. These kinds of chips are useful in such application in which the status of goods changes as they pass through the supply chain management. WORM chips are different in nature from the chips we described earlier. WORM is written once but not at time of production, and it can only be read once it is written. It is best for security applications.
4. Description of Protocols

4.1. Specification of IEEE 802.15.4

4.1.1 Overview
IEEE 802.15.4 is an appearing standard specially used for Low Rate Wireless Personal Area Networks (LR-WPAN). The main purpose of this standard is to provide ultra low complexity, ultra low power consumption and low cost wireless networking solution in low data rate networks within the Personal Operating Space (POS) 10 m offering data rate of 250 Kbps but longer range can be achieved at lower data. The Physical layer (PHY) and MAC sub layer specifications are defined by IEEE 802.15.4, shown in Figure 10. LR-WPAN network can support two types of devices, a Full-Function Device (FFD) and a Reduced–Functional Device (RFD). FFD is capable of being a network coordinator and complete protocol stack is implemented in it, while in the RFD the reduce protocol stack is used [19].

IEEE 802.15.4 provides a reliable communication mechanism; Carrier Sense Multiple Access (CSMA/CA) to avoid collision and supports both star and peer to peer topology as shown in Figure 11.

In star topology, communication is carried out through the Personal Area Network (PAN) coordinator, it has application in home automation and interactive toys. In peer to peer
topology, any device can communicate with the other device as long as they remain in the range of each other. Asset tracking, industrial control is to use this type of topology.

**Star Topology**

**Peer-to-Peer Topology**

```
  PAN Coordinator
```

- Full function device
- Reduce Function device
- Communication Flow

*Figure 11: IEEE 802.15.4 star and peer-to-peer topologies [19]*

### 4.1.2 Frame Structure

IEEE 802.15.4 provides support for following four types of frames

1. Beacon frame
2. Data frame
3. Acknowledgment frame
4. MAC command frame
4.1.2.1 Beacon Frame
A beacon frame originates from MAC sublayer. A coordinator is responsible for the transmission of a beacon frame in beacon-enabled network; the structure of beacon frame is shown in Figure 12. The beacon is used to synchronize the attached devices, identify the PAN and describe the structure of superframe.

<table>
<thead>
<tr>
<th>Octets</th>
<th>2</th>
<th>1</th>
<th>4 to 10</th>
<th>2</th>
<th>k</th>
<th>m</th>
<th>n</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Sublayer</td>
<td></td>
<td>Frame Control</td>
<td>Sequence Number</td>
<td>Addressing Field</td>
<td>Superframe Specification</td>
<td>GTS Field</td>
<td>Pending Address Field</td>
<td>Beacon Payload</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MHR</td>
<td>MSDU</td>
<td>MFR</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Octets</th>
<th>4</th>
<th>1</th>
<th>1</th>
<th>7 + (4 to 10) + k + m + n</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHY Layer</td>
<td>Preamble Sequence</td>
<td>Start of Frame Delimiter</td>
<td>Frame Length</td>
<td>PSDU</td>
</tr>
<tr>
<td></td>
<td>SHR</td>
<td>PHR</td>
<td>MPDU</td>
<td>13 + (4 to 10) + k + m + n</td>
</tr>
</tbody>
</table>

Figure 12: Beacon Frame Structure [19]

4.1.2.2 Data Frame
Data frame originates from the upper layers and passes to the MAC sublayer. Data payload in the MAC sublayer is known as MAC service data unit (MSDU). The MSDU is prefixed with MAC Header (MHR) and appended with MAC Footer (MFR). The MHR, MSDU and MFR together form the MAC data frame. The MAC protocol data unit MPDU, which is passed to PHY layer, prefixed an Synchronized Header (SHR) and PHY Header (PHR). The SHR, PHR and PSDU form the PHY data packet. The structure of data frame is shown in Figure 13.
4.1.2.3 Acknowledgment Frame

The acknowledgement frame originates from the MAC sublayer. The organization of the acknowledgement frame is stated in Figure 14. Acknowledgement frame, which is optional, is sent after the successful reception of the frame.

![Figure 13: Data Frame Structure [19]](image1)

![Figure 14: Acknowledgement Frame Structure [19]](image2)
4.1.2.4 MAC Command Frame

MAC command frame, which is used for requesting the data from the device emanates from the MAC Sublayer. The MSDU contains the command type field and command payload. The construction of MAC command frame is shown in Figure 15.

Octets 2 1 4 to 20 1 n 2

MAC Sublayer

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Sequence Number</th>
<th>Addressing Field</th>
<th>Command Type</th>
<th>Command Payload</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MHR</td>
<td>MSDU</td>
<td>MFR</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Octets 4 1 1 6 + (4 to 20) + n

PHY Layer

<table>
<thead>
<tr>
<th>Preamble Sequence</th>
<th>Start of Frame Delimiter</th>
<th>Frame Length</th>
<th>MPDU</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHR</td>
<td>PHR</td>
<td>PSDU</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>12 + (4 to 20) + n</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PPDU</td>
<td></td>
</tr>
</tbody>
</table>

Figure 15: MAC Command Frame Structure [19]

4.1.3 PHY Specification

The physical layer controls the radio of the device, to perform the energy detection (ED) within the channel, and implement the Clear Channel Assessment (CCA) for CSMA/CA before sending the packet and collection or transmission of the data over the correct channel. The major source of power consumption is idle listening, this problem can be solved by entering the Radio Frequency (RF) transceiver into sleeping mode and activate RF transceiver after some specific time.

The IEEE 802.15.4 defines three frequency bands, with a total number of 27 channels. Sixteen channels are there in 2.4GH, 10 in the 915 MHz, and 1 in the 868 MHz. The structure of 2.4 GHZ is shown below. The device on which IEEE 802.15.4 protocol stack is implemented uses the Direct Sequence Spread Spectrum (DSSS) to increase the bandwidth of the transmitted signal for a reliable communication. Physical specifications are given in details in Table 4.

<table>
<thead>
<tr>
<th>PHY(MHz)</th>
<th>Frequency Band MHz</th>
<th>Spreading Parameters</th>
<th>Data Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Chip Rate K chips/s</td>
<td>Symbol Rate K symbol/s</td>
</tr>
<tr>
<td>868</td>
<td>868-868.6</td>
<td>300</td>
<td>20</td>
</tr>
<tr>
<td>915</td>
<td>902-928</td>
<td>600</td>
<td>40</td>
</tr>
<tr>
<td>2450</td>
<td>2400-2483.5</td>
<td>2000</td>
<td>250</td>
</tr>
</tbody>
</table>

Table 4: Physical Specification of IEEE 802.15.4 [19]
4.1.4 Medium Access Control Layer

The 802 group divides the data link into a sublayer MAC and a Logical Link Control (LLC). The LLC layer, which is standardized in 802.2, is common in the rest of IEEE 802 standard. The MAC sublayer is responsible for the PAN association and disassociation. It also provides optional superframe structure, as given in Figure 16, which has active and inactive portion and is bounded by a beacon for synchronization. The coordinator will interact with PAN during active portion and the device enters into low power mode during inactive portion, following figure showing the structure of superframe. MAC sublayer provides two mechanisms for channel access, which are contention based and contention free. In the contention-based period, devices use a CSMA/CA backoff algorithm, while Guaranteed Time Slots (GTS) are used for access in contention free period. Communication throughput decreased below a threshold detected by the upper layer and MAC sublayer is instructed to perform energy detection. Upper layer is switched to channel who has lower power based on Energy Detection (ED). CCA is performed based according to the energy scan.

![Figure 16: Superframe Structure [19]](image)

In beacon-enabled network, communication is controlled by coordinator, which communicates at will with the nodes. In beaconless network, a node can send data to the coordinator at will however it cannot communicate at will with the nodes, but must be invited by a node to communicate. The communication patterns are displayed in Figure 17-20.

![Figure 17: Communication to Coordinator from Device in Beacon Enabled Network [19]](image)
Figure 18: Communication to Coordinator from Device in Non-Beacon Network [19]

Figure 19: Communication from Coordinator to Device in Beacon Enabled Network [19]

Figure 20: Communication to Device from Coordinator in Non-Beacon Network [19]
LR-WPAN MAC sublayer employs two types of channel access mechanisms that depend on network configuration. Before the transmission of data or MAC command frames, it shall wait random period. Non-beacon-enabled network uses unslotted CSMA/CA (Figure 21), for channel access. If the channel is found busy following backoff period, the device will wait for another random backoff, before trying to access the channel again. In the beacon-enabled if the channel is found idle following backoff period, the device will transmit it data. In beacon-enabled network, slotted CSMA/CA is used (Figure 22), where backoff are aligned when beacon transmission starts. Each device that wishes to transmit data, starts at the beginning of the slot boundary. Acknowledgement and beacon frames are transmitted without CSMA/CA mechanism. Number of Backoff (NB) is the number of backoff required for CSMA/CA algorithm and the maximum value is 4 before declaring access failure. Contention window (CW) defines how many times CCA is to be performed. Backoff Exponent (BE), which is related to the backoff delay, describes how many backoff periods wait before accessing the channel whose value in the range of \([0, 2^{BE} -1]\).

This standard also supports Direct Sequence Spread Spectrum for data transmission. In the standard one bit is mapped against 32 bit spreading code.
Unslotted

NB=0, BE=macMinBE

Delay forrandom(2BE-1) unit backoff period

Perform CCA

Channel idle?

NB=NB+1, BE=min(BE+1, amaxBE)

NB > maxMaccsma

Backoff

Failure

Success

Figure 21: Unslotted CSMA [19]
Figure 22: Slotted CSMA [19]
4.2 Specification of ISO 18000-4

ISO 18000-4 is the common achievement of the International Organization for standardization (ISO) and the International Electrotechnical Commission (IEC). This standard states that the air interface of RFID operates in 2.4 GHz. It provides two modes; first is for a passive tag and the other is for battery assisted tag. The minimum features supported by devices that are defined according to ISO/IEC 18000 identify multiple tags, read / write, select subgroup of tags and error detection in the rage of the reader.

4.2.1 Mode 2: Battery Assisted Passive Tags

This mode supports battery assisted passive tags for long range RFID applications. Reader broadcasts two carriers at the same time; one is modulated by Gaussian Minimum Shift Keying (GMSK) and other is a CW carrier. One carrier is used for transferring data from reader to tag and communication carrier is used for backscatter modulation. In case of R/O, only one carrier is required. All information is read out in R/O tag during notification process. Time division multiplexing is used for communication between reader and tag. Time slots are being used for transmitting the data. Each subframe is divided into 14 time slots, where maximum subframes can be up to 64 bits. In each slot, 200 bits or 40 bits are transmitted at the data rate of 384, 66.8 Kbps respectively as shown in Figure 23. Randomizing the repetition reduces the collision. ISO 18000-4 (mode 2)

![Frame Structure ISO 18000-4 mode 2](image)

ISO 18000-4 (mode 2) also support spread spectrum for transmitting data. It provides support for Frequency Hopping Spread Spectrum (FHSS). Frequency hopping sequence and frequency hopping rate is adaptive as specified by the local regulatory authorities.

4.2.2 Communication Channels

This mode supports the following three logical channels that perform different tasks:

- **Notification Channel**
- **Communication Channel**
- **Spectrum Check Channel**
4.2.2.1 Notification Channel
New tag uses the notification channel to send synchronization information to the reader so that the reader can extract the tag-id correctly. In R/W tag, notification channel carries out bi-directional communication. The notification channel would be ended when the tag read the first command in the R/W tag. Complete information transmission from tag to reader occurs in the notification channel.

4.2.2.2 Communication Channel
Between reader and tag, the communication channel is used to perform the read and write operation. The channel will begin on the completion of first command at the tag and end by reader when it sends the end of communication signal.

4.2.2.3 Spectrum Check Channel
Searching for a free frequency channel is done by using of spectrum check channel, which channel will be active in the absence of communication channel or notification channel.
5. Contributions

5.1 Protocols’ Analysis

5.1.1 Low Power Consumption
Limited available power was the leading driving force for the whole new design of protocol stack. This is the single factor that has the utmost importance in designing the protocols of these networks. Most of the power is consumed during the receiving of the packets. There are different trade-offs between power and other parameters like frame length, duty cycle, operational range, medium access mechanism and sleep mode support etc.

5.1.2 Operating Frequency and Range
Although 802.15.4 supports three ISM bands 868MHz, 915MHz and 2.4 GHz, but 2.4 GHz will remain the center of our attention because its the band that is being used both in IEEE 802.15.4 and ISO 18000-4.

2.4 GHZ is an unlicensed band ISM, which gives an edge over other ISM bands because of its unrestricted worldwide availability, while other ISM bands have some restrictions in Europe and USA. But worldwide availability of this band attracted vendors of other wireless solutions too. This creates the problem of interference of 2.4GHz RFID systems with other systems operating in the same frequency range. Interference can result in retransmission of data and reduced power efficiency of the system. By controlling the transmission power of the transmitter, this situation can be reduced. Most of the time the local regulatory authority gives you an upper bound limit for the transmission power.

5.1.3 Spread Spectrum Techniques
Spread spectrum technique is used to overcome the interference noise. IEEE 802.15.4 standard uses DSSS while FHSS is used by ISO 18000-4. In 802.15.4 DSSS provides a static approach by spreading the 1 bit with 32 bit spread code, while the FHSS in ISO18000-4 provides an adaptive approach for the frequency hop rate and frequency hop sequence. Due to this adaptive approach user can set the hop rate and hoping sequence to keep the energy consumption to the minimum level.

Although the DSSS systems require large and power hungry components compared to FHSS, but DSSS provides a better error recovery than FHSS. Main advantages of DSSS is that it provides a high data rate and the main drawback is that it has a threshold for interference (noise), if the noise under the threshold system works appropriately but if the noise is above the threshold, the system will stop working completely. FHSS offers more resistance against interference and its data rate decreases slowly comparing to the sudden drop to zero in DSSS [28]. Data rate in FHSS is less than the DSSS. IEEE supports 250 Kbps as compared with ISO 18000-4, which offers 384 Kbps that looks contradictory of what we have described earlier. Infect IEEE operates on DSSS which maps 1 bit to 32 bits spreading code, that makes it actually offering 250000 x 32 = 8 Mchips/sec, which is quite higher than ISO 18000-4.
Considering these pros and cons, both technologies can be used alternatively depending on the application. DSSS is used in networks where heavy traffic with large data packets in contrast to the FHSS.

5.1.4 Adaptive Duty Cycles
Ratio of being active and sleep is called duty cycle, which plays an important role in power consumption. Since RFID applications are power critical, so duty cycles should be adjusted accordingly to meet the deadline of data as well as the power constraints of the device. High duty cycle will consume more power but we will receive more frequent data, while the reduced duty cycle will be hazardous in time critical applications. IEEE standard supports adaptive duty cycle while this is not the case with ISO standard.

Duty cycle should be under 1% for LR-WPANs to meet the power constraints in low power WPANs [19]. It can be adjusted with the help of Superframe Order (SO) and Beacon Order (BO) parameters depending on the nature of the application. BO and SO help decide the time period of beacon’s period and active period simultaneously.

\[
\text{Beacon time period} = (2^{BO} \times \text{aBaseSuperFrameDuration})
\]

\[
\text{Active period} = (2^{SO} \times \text{aBaseSuperFrameDuration})
\]

\[
\text{Duty Cycle} = \frac{2^{SO}}{2^{BO}}
\]

5.1.5 Variable Frame Length and Types
In power deficient networks it is always better to have adaptive frames as per requirement. It is not prudent to send a relative small control information using the standard and large set of frame.

IEEE standard supports flexible frame length by providing different frame types for diverse nature of traffic. IEEE 802.15.4 standard introduces four types of frames; data, beacon, acknowledgement and MAC command frames. Transmission power can be inflected according to the frame length. The frame with more data requires more power to transmit compared to low data frame for the same destination. The maximum packet length that is transmitted to channel is 133 bytes to minimum 11 bytes. Use of the beacon frame in IEEE 802.15.4 abates the power consumption as the devices can synchronize easily in beacon-enable mode. The beacon conveys a message to the devices telling about next time the coordinator is going to up, so the device can become alive just before the beacon frame arrives and goes back to the sleep mode if the coordinator has not pending message for it. Acknowledgement frame is optional, so it can be avoided in such applications where the amount of traffic is too low in the network because low date means less possibility of collision. But in certain domains, which involve water substances and humid environments, despite the low traffic parameter we have to have

* Taken from [19]
acknowledgment frames enabled; because the 2.4 GHz is prone to such environments and we can observe data loss.

5.1.6 Channel Access Mechanism
In wireless medium, we cannot send data and detect collisions later on, but we can avoid it before sending the data. Collision means low throughput and more power wastage. IEEE 802.15.4 uses the CSMA/CA method as described in section 4.1.4. This method makes a double check to ensure that the physical channel is available before sending the data. This double check is waste of power, as the probability to access the channel remains same. Channel selection procedure is performed every time a transmission is likely to occur. This procedure is distributed in nature e.g. procedure will occur at reader if transmission is started by the reader or at tag’s end if traffic is to be initiated at tag. The distributed nature of this protocol consumes more power. Unlike 802.11, Ready To Send/Clear To Send (RTS/CTS) is not used here, since RTS/CTS shows excellent data reliability in heavy traffic situations. In 802.15.4, the volume of data is not too high, so RTS/CTS will only increase the data overhead and degrade the network throughput in RFID application.

In contrast to this, ISO 18000-4 (mode 2) uses TDMA approach to access different tags. Therefore each frame is divided into different subframes, and designated as different time slots. Each subframe is allocated to a device. The reader allocates this subframe to each tag permanently during communication and bi-directional transmission between reader and tag is done using this subframe. The tag doesn’t have to make a selection again for backward link. This way no energy is consumed for subframe selection on backward link, but TDMA has some inherited drawbacks. Since TDMA is decided at reader for whole network, so the probability of single point of failure increases. In case of variable delay time of the tags, time synchronization can be a problem in TDMA supported systems. TDMA faces another problem that we don’t experience in CSMA; in ISO 18000-4, tag uses the same channel as specified by the reader so it will have to use it for backward link even if the channel experiences noise. But in case of CSMA, the tag can scan the availability of noise free channel before it sends data at backward link.

5.2 Hardware Suitability in Terms of Power Efficiency
If we do care about optimal power consumption in power scarce networks, we must take into consideration the design parameters at two different levels; one is the protocol level, and the other is at hardware level, where the protocol is actually been implemented.

The different aspects of power saving at the protocol level have already been discussed in previous sections. In this section we would like to focus on how the choice of hardware affects battery consumption which in turn influences the life of the system. Free2move has proposed (transceiver chip Chipcon 2420 and micro-controller ATmega128L) for its upcoming Active RFID product. We would see if the offered hardware platform (transceiver chip Chipcon 2420 and micro-controller ATmega128L) is optimal for the power deficient environment, or we can use some other alternatives available in the market without violating the IEEE 802.15.4 standards. Another design constraint is the
cut-off voltage of a battery, which can be described as the least voltage at which the battery is considered completely discharged. A battery with high cut-off voltage means the battery will stop operating although it has good percentage of leftover quantity. This factor will not only increase the cost of the device but will also decrease the operating life of the device.

Selecting a radio transceiver chip that complies with the standard and offers the most efficiency in terms of operating power consumption in different modes is a tedious job. We have considered here some of the available RF chips supporting IEEE 802.15.4 standard. For now we have a couple of transceivers that offer IEEE 802.15.4 solution on a single chip including Chipcon 2420, Ember 2420, and Motorola MC13191/92/93. The specifications of these chips are given in Table 5.

<table>
<thead>
<tr>
<th>RF Transceiver Model</th>
<th>Operating Voltage (Volts)</th>
<th>Receive Current (mA)</th>
<th>Transmit Current (mA)</th>
<th>Sleep Current (µA)</th>
<th>Encryption</th>
<th>Buffering (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chipcon 2420[20]</td>
<td>2.1 – 3.6</td>
<td>19.7</td>
<td>17.7</td>
<td>1</td>
<td>Available</td>
<td>128</td>
</tr>
<tr>
<td>Motorola MC13191/2[21]</td>
<td>2.0 – 3.4</td>
<td>37</td>
<td>30</td>
<td>1</td>
<td>Not-Available</td>
<td>133</td>
</tr>
<tr>
<td>Ember 2420[22]</td>
<td>2.1 – 3.6</td>
<td>19.7</td>
<td>17.4</td>
<td>0.5</td>
<td>Available</td>
<td>128</td>
</tr>
</tbody>
</table>

Table 5: Characteristics of RF chips

Micro-Controller is the second most important component in our active RFID architecture, so care must be taken to choose a micro-controller which takes less wakeup time as well as maintain less power in the sleep mode since the devices in low power personal area networks are sleeping most of the time. Here we are going to compare the Atmel Mega 128L with some other lower power consumption MCUs like Texas Instruments’ MSP430F169 and MSP430F2013.

<table>
<thead>
<tr>
<th>MCU</th>
<th>Operating Voltage (Volts)</th>
<th>Active Current (mA)</th>
<th>Sleep Current (µA)</th>
<th>Wakeup Time (µs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atmel 128L 8 bit[23]</td>
<td>2.7 – 5.5</td>
<td>8</td>
<td>15</td>
<td>180</td>
</tr>
<tr>
<td>MSP430F169 16 bit[24]</td>
<td>1.8 – 3.6</td>
<td>330 µA</td>
<td>0.2</td>
<td>6</td>
</tr>
<tr>
<td>MSP430F2013 16 bit[25]</td>
<td>1.8 – 3.6</td>
<td>220 µA</td>
<td>0.1</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 6: MCU Characteristics
Table 5 shows that operating voltage of all the chips is the almost same but the cut-off voltage for Motorola MC13191/2 is slightly better (2.0 volts) than the rest. Which means if the system is running at batteries connected serially, with combined cut-off voltage less than or equal to 2.0 volts, then Motorola RF transceiver will remain operative for a longer time (assuming that other characteristics remain same for both MCUs). On the other hand, the Motorola transceiver chip consumes almost double the current in receiving and transmission mode than others. Since the devices in low power networks like RFID’s sleep most of the time, so we must take into account the current consumed by transceivers during the sleep mode, in which case Ember 2420 shows 50% reduced current consumption than Chipcon and Motorola.

Now considering the micro-controllers; in Atmel 128L the consumption of current in active as well sleep modes is much higher than the MSP family of micro-controllers. This is also true for the wakeup time, which is 30 times, and in some cases 180 times higher than MSP family.

Let us take a situation in which architecture is supported by two coin cells connected serially, with 3 volts each, having combined cut-off voltage equals to 4 volts. Each battery has 2400mAh. Assume that we want to achieve duty cycle of 1%. Further we take an upper bound of the current consumption, by assuming that the device is in receive mode during its active period.

If we apply the above situation to a combination of Chipcon 2420 and Atmel 128L controller then with the help of the following formulae, we find that the system will run up to 355 days. But if we combine the Motorola transceiver chip with Atmel 128L, then the system will run its life of 250 days which shows that it has 30% less life than (Chipcon + Atmel).

*Calculate the Duty Cycle:

\[ T_{on} = \frac{I_{avg}}{I_{on} - I_{slp}} \]

\[ T_{on} = \text{Duty Cycle}, I_{avg} = \text{Average Current consumption}, I_{slp} = \text{Current consumption in sleep mode}, I_{on} = \text{Current consumption in active mode} \]

*Calculate Average Current:

\[ I_{avg} = T_{on}(I_{on} - I_{slp}) + I_{slp} \]

*Calculate life of the Battery:

\[ \text{Time (in hours)} = \frac{\text{Battery}}{I_{avg}} \]

* Formulae taken from [26]
It looks obvious from Table 6, that Atmel 128L is consuming much more power and is lagging behind in almost all aspects from the other two competitors. So we calculate new values for a system with Chipcon 2420 and MSP430F169. The values we obtain after calculation shows a tremendous increase in the life span of the system reaching 497 days, which is almost 29% more than the (Chipcon + Atmel)

The above analysis shows that only the design consideration at the protocol level is not sufficient but the right hardware is deeply needed to realize the true results of the design requirements (Table 7). We would need to select the optimal combination of RF chip transceiver with appropriate controller and then try to use the batteries with the cut-off limit that can work as far as possible with the lower voltage limits of the transceiver chip and controller.

<table>
<thead>
<tr>
<th>Combination</th>
<th>Life Time Span (days)</th>
<th>Efficiency with respect to (CC2420 + Atmel 128L)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC 2420 + Atmel 128L</td>
<td>355</td>
<td>Standard</td>
</tr>
<tr>
<td>MC13191/2 + Atmel 128L</td>
<td>250</td>
<td>30% Decrease</td>
</tr>
<tr>
<td>CC 2420 + MSP430F169</td>
<td>497</td>
<td>29% Increase</td>
</tr>
</tbody>
</table>

*Table 7: Comparison of hardware in terms of power efficiency*

### 5.3 Proposal

**5.3.1 Modified IEEE 802.15.4**

Motivation behind this proposal is the fact that the reader in most of the RFID systems have external source of power, so we feel that this unlimited source of power should be used as a contributory factor to enhance the life of the tags.

We are going to propose some amendments in IEEE 802.15.4, so it can be used as semi-passive RFID, which means the tags will now experience a longer life with the same batteries because they will not use the batteries anymore to send the data. Batteries will now be used only for wake up and receiving. Although transmitting state consumes somewhat less power than receiving, but in either case, we will be saving power, and in turn enhance the life of the tag and the system.

In a traditional IEEE 802.15.4, we have 16 channels at 2.4 GHz, each with 3 MHz bandwidth and guard band of 2 MHz as shown in figure 24. To use 802.15.4 as a semi-passive RFID system, we need to generate a reference carrier all the time which can be used as a back-scattered medium in 802.15.4.

![Figure 24: Traditional IEEE 802.15.4, 2.4 GHz Channels 11-26](image-url)
We have a spacing of 2 MHz between each subsequent channel, either of which can be used to generate the reference carrier. Because of the narrow guard band, we assume that we are occupying the first spacing for reference carrier to minimize the interference effect of the data carrier as shown in Figure 25. We are proposing here that the bandwidth of the reference carrier will be 1 MHz, and there will be a guard band of 0.5 MHz between the reference carrier and the first data carrier channel. To avoid the adjacent channel interference, we can skip the allocation of the first data carrier channel with center frequency 2405 MHz, and can start with frequency of 2410 MHz.

5.3.1.1 Working of Modified IEEE 802.15.4

In beacon-less mode the reader has two carriers; the first is reference carrier, which is sent out continuously on air medium and is responsible to fetch on reverse link (from tag to reader). The second is the data carrier, which awakes only at the time of sending data at forward link (from reader to tag). The working of the data carrier and most of the functionalities of the standard will remain the same as it was in defined in IEEE 802.15.4. When tag comes within the range of the reader, it will be associated with the reader by backscattering its ID in data frame to the reader using the reference carrier. All the remaining processes of acknowledgment and retransmission of data, in case of acknowledgement failure, will be based on the 802.15.4 standard.
The same process will be followed, if the tag is equipped with some sensor node. On achieving a threshold value, the tag will wake up and send the data frame on reference carrier.

Since this is a beaconless mode in which tag always talks first so, in situations where the reader wants to write data to the tag, it has to wait for a request from the tag which asks for any data that the reader wants to write to the tag. Data request will be sent on reference carrier, while the acknowledgement of the request and data from the reader will be sent by using data carrier. Later on, the acknowledgement from the tag will be sent to the reader using reference carrier. This process is shown in Figure 27.

![Figure 27: Communication from reader in beacon-less Modified IEEE 802.15.4](image)

In beacon-enabled mode, where the reader talks first, the beacons are generated periodically by the reader. The beacons will be carried to tags on data carrier. The data from the tag will be transmitted back to reader at reference carrier, which in turn sends the acknowledgement on data carrier as shown in Figure 28.

![Figure 28: Communication to reader in beacon-enabled Modified IEEE 802.15.4](image)

In beacon-enabled network, when the reader wants to send data to the tag, it sends out the pending data message in the beacon to the tag using data carrier and the tag generates a data request for the reader using reference carrier. The reader sends back the
acknowledgment as well as data on data carrier. Upon receiving the data, the tag sends the acknowledgment using reference carrier. This process is shown in Figure 29.

This suggested modification best suits most of the RFID environment, where the reader is provided with external power supply. The modified standard will not only help to improve the lifetime of the system but it will also provide the interoperability between different vendors whose products will be based on the modified standard. Since the reader will have abundant power supply, so the power restriction lies at the tag side only. With the modified standard, we will be saving the power that was earlier being used in the transmitting phase. The down side is a shorter range than the original standard, because of the backscatter modulation. If we want to keep the range to conform with the original standard i.e 10 meters, then we may have to increase the power of the reference carrier. Since the increased power of the reference carrier may increase interference with other wireless systems operating at 2.4GHz in the same premises, so this increase in power is subject to the local regulatory authority.

The modulation techniques in the modified system can be addressed in the following way. For forward link, the data carrier is modulated on Orthogonal Quadrature Phase Shift Keying (O-QPSK), which is the same as per the original standard, while the tag will have demodulator of the O-QPSK. For reverse link, the same modulation can be used at the tag for reference carrier, and a demodulator for O-QPSK is needed at the reader. Although O-QPSK is more tolerant to interference than other modulation techniques like Binary Phase Shift Keying (BPSK), but the O-QPSK consumes more power than BPSK, which can be a good choice for reference carrier since the data rate is not so high in RFID systems. In BPSK we do not achieve a complete phase shift of 180, which cause a higher bit error rate. So BPSK and O-QPSK can be used alternatively considering their tradeoffs.

The complexity of the system will increase, since this will be a hybrid system in nature, because there will be two different antennas, one for the reference carrier and the other for the data carrier at the reader’s end, and also if we are using two different modulation techniques (O-QPSK for data carrier and BPSK for reference carrier). Since the reference carrier is quite close to the data carrier, so we also need to use filters with much improved...
sensitivity level, which may increase the cost of the system. Most of all we also need to tightly synchronize the data carrier and reference carrier together when we will be using superframe structure.

5.3.2 Powering the Sensor with Reference Carrier

In the previous section we had the situation in which RFID is used purely as the identification system and our modified standard was able to meet the goals with somewhat more complexity than original standard. But RFIDs are not used always only as identification systems but sometimes they are supported with sensors to measure different physical conditions of the products like temperature, humidity etc. Since in sensor-supported semi-passive RFID systems the tags are supposed to wake up for multiple purposes, like receiving beacon or sensing the atmosphere, which makes the life of the battery shorter. In this section we will use the reference carrier to power the sensor circuitry which will extend the battery life of the tag. The specification of the reader is the same as we have assumed in the previous section. The changes will be at the tag end.

Figure 30: Semi-Passive RFID with temperature sensor powered from reader

Figure 30 shows a tag with sensor installed on it. This semi-passive RFID architecture is somewhat different than a normal semi-passive RFID architecture. In normal semi-
passive architecture the battery on board powers the sensor and RF chip both, while the
transmission is performed by reflecting the incoming signal from the reader. In this
architecture we have two antennas reference-carrier antenna and data-carrier antenna. RF
circuit is clocked by its personal oscillator and is powered by the on-board battery. RF
circuit is responsible to receive data on data-carrier antenna. Since we are assuming that
reader is on and radiating signals (reference carrier) all the time, so energy from reference
carrier can be used to operate the sensor and perform operations associated with its
circuitry.

The incoming signals are converted into DC volts using the RF-DC rectifier, the output of
the rectifier is then stored in capacitor. The capacitor will store the power in it up to a
certain level, after which it will start providing power to the sensor circuit. This will
happen only when the reference-carrier antenna is in receiving mode. During the
transmitting mode of antenna, the capacitor will provide the stored power to sensor
circuit. Due to the fact that sensor has a built-in oscillator, it will consume less power
than an external clock. This oscillator will wake the sensor circuit after some interval to
take the atmospheric reading. This reading will be stored in memory. Sensor circuit is
capable of writing the data in this memory while RF circuit can only access this memory
for reading purpose. When sensor circuit achieves a threshold limit it will call an interrupt
to wake the RF circuit. This interrupt will also switch the state of reference-carrier
antenna to transmitting mode. Interrupt generated by sensor circuit would be able to wake
the RF circuit only when it is operated in beaconless mode. In beacon-enabled mode, the
local oscillator of the RF circuit will woke it up based on the incoming beacons of the
reader.

There are certain factors that need to be considered to get the most of the incoming power
to activate the sensor circuitry. The most important thing is the impedance matching
between the reference-carrier antenna and sensor circuit. The relation between power
received at antenna and the power transferred to circuit is given as,

\[*\]

\[ V_{in} = 2 \sqrt{2 P_{ant} R_{in} \left( R_{in} / (R_{in} + R_{ant}) \right)} \]

Where \( V_{in} \) = Input voltage for rectifier
\( R_{ant} \) = Real part of the antenna’s impedance
\( R_{in} \) = Real part of circuit impedance

With the increase of \( R_{ant} \) the \( V_{in} \) will also increase. If we want to transfer the maximum
power from antenna to the sensor circuit then, \( R_{in} \) should be equal to \( R_{ant} \)

\[*\] Taken from [27]
Power received by tag antenna in free space can be calculated as,

\[ P_a = P_r G_r G_t \left( \frac{\lambda}{4\pi d} \right)^2 \]

\( P_a \) is Receive power at tag antenna, \( P_r \) power at reader antenna, \( G_t \) is gain at reader antenna, \( G_r \) is gain at tag antenna, \( d \) is distance between tag and antenna.

Sensor circuit needs a certain minimum power \( P_{th} \) to operate. This power can be received only if the tag lies at a certain distance from the reader. This reading range can be calculated by using the formula,

\[ \text{Read Range} = \frac{\lambda}{4\pi} \sqrt{\frac{P_t G_t G_r \tau}{P_{th}}} \]

\( \tau \) is the reflection coefficient

We assume that both the reader and the reference-carrier antenna at the tag are isotropic, so the gain of antenna can be calculated as,

\[ G = \frac{4\pi A_e}{\lambda^2} \]

\( A_e \) is the effective area of antenna, for Isotropic antenna \( A_e = \frac{\lambda^2}{4\pi} \)

If we assume a reader with transmitting power 4 W, and minimum threshold needed for sensor circuit is 70uW [30] (for oscillator and sensor with digital output) and suppose that antenna are perfectly match for maximum power transfer, i.e. \( \tau \) is 1, so read range would be approximately 2 meters.

This would be possible with isotropic antenna with transmitting frequency 2.4 GHz, (wavelength is 0.125 m). If we use same power for the passive tag without temperature sensor, then circuit will have minimum threshold power 2.7 uW and the range will be 12 meters.

* Taken from [28]
** Taken from [29]
6. Conclusion

Our main problem was to analyze the different RFID systems based on the power efficiency and investigate how much IEEE 802.15.4 can be a feasible candidate for RFID system. During our investigation, we observed that despite some anomalies like double check of communication medium IEEE 802.15.4 standard, will prove a good seeker for active-RFID systems. As all the previous standards of IEEE 802 group addressed the MAC and physical layer problems and gained world wide acceptability and adaptability, we are sure that this standard will receive the same response.

Low power consumption does not lie only at efficiently designed MAC protocol, but it depends on many other factors like, upper layer protocols (specially network layer protocol in case of multi-hoping routing), cutoff voltage of battery, and power efficient hardware design. This is due to the fact that different hardware components can be designed in many ways to achieve the same goal, with different power consumption. So focusing only at designing a power efficient protocol will not solve this power management issue. We found that choosing the right hardware architecture and proper supported batteries would help to extend the life of the RFID systems.

The use of IEEE 802.15.4 standard in semi passive-RFID systems is possibility as specified in our proposal. This will help to stay close to the standard, but the complexity of the system will increase. So there will be trade-off between power consumption and cost /complexity of the system. The revisions in the standard would be a possibility by the time but that will bring some good to this standard’s performance.
7. Future Work

During our investigation we found that there is no supportability for the multicasting and broadcasting at the MAC layer in RFID systems. So efforts need to be done to explore this horizon.

We proposed a modification in IEEE 802.15.4 to have efficient use of available power, but still tried to keep it close with the original 802.15.4 standard as much as possible. Although we proposed an idea, which looks very feasible for RFID systems but different issues need to be resolved like placement of reference carrier at 2.4 GHz band, its power, adjacent channel interference and suitable modulation schemes before the deployment of the modified IEEE 802.15.4. Further we foresee that our proposal should be implemented to see the real results of the proposed system.
8. References


