

**YAŞAR UNIVERSITY  
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES**

**MASTER THESIS**

**CONSTRUCTION OF SELF ORGANIZING AND  
UPDATING WIRELESS SENSOR NETWORKS USING  
ENERGY EFFICIENT MICROPROCESSORS**



**Atilla Osman Mert GEMALMAZ**

**Thesis Advisor: Prof. Dr. Mustafa GÜNDÜZALP**

**Department of Electric and Electronic Engineering**

**Presentation Date: 07.08.2017**

**Bornova-İZMİR  
2017**

We certify that we have read this thesis and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science / the Doctor of Philosophy.

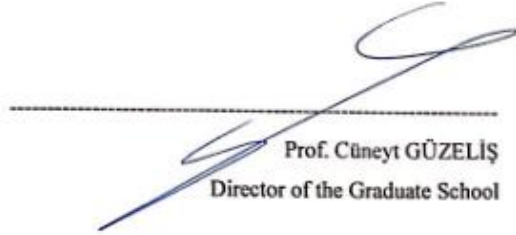
**Jury Members:**

Prof. Mustafa GÜNDÜZALP  
Yaşar University

Asst.Prof. Tuncay ERCAN  
Yaşar University

Asst.Prof. Özgür TAMER  
Dokuz Eylül University

Signature:  
  
  


  
Prof. Cüneyt GÜZELİŞ  
Director of the Graduate School

## ABSTRACT

### CONSTRUCTION OF SELF ORGANIZING AND UPDATING WIRELESS SENSOR NETWORKS USING ENERGY EFFICIENT MICROPROCESSORS

Gemalmaz, Atilla Osman Mert

Msc. Electric & Electronics Engineering

Advisor: Prof. Mustafa GÜNDÜZALP

September 2017

In the study of wireless sensor network, which will be one of the key technology that simplifies our life in near future, necessary algorithms are validated by field studies. Instead of simulations, algorithms are tested on systems which consist of specially designed circuits. The investigation of this thesis is about increase the range of the system with self-discovery and configuration algorithms. In addition, the other motivation of this study is to consider energy efficiency while increasing the range.

Improvements on the processors and sensor technologies performance and price, wireless sensor networks are becoming widened. As a result, there is variety of different protocols and applications on the field. Therefore, there should be protocol converters or connectors. In case of custom sensor network which is not dependent on common protocols like ZigBee and Bluetooth, a gateway design should be implemented in order to connect this custom protocol to a known one. In this thesis it is aimed how the range of the gateway node is increased in order to gather data from custom designed sensor network while keeping energy consumption low.

After implementation, test, and validation phase, it is observed that the designed algorithm successfully increases the coverage of the gateway node.

**Key Words:** wireless sensor networks, coverage, self-discovery, WSN gateway.

## ÖZET

# ENERJİ VERİMLİ MİKROİŞLEMCİLER VE ALGORİTMALAR KULLANARAK KENDİNİ YAPILANDIRABİLEN VE GÜNCELLEYEBİLEN KABLOSUZ SENSOR AĞLARI OLUŞTURULMASI

Gemalmaz, Atilla Osman Mert

Yüksek Lisans Elektrik-Elektronik Mühendisliği Bölümü

Tez Danışmanı: Prof. Mustafa GÜNDÜZALP

Eylül, 2017

Günümüzün gelişen teknolojisi ile kablosuz sensör ağları uygulamaları sayesinde hayatımızın kolaylaştırılabilmesi için, gerekli algoritmalar oluşturulmuş olup; bu algoritmalar saha çalışmaları ile test edilerek doğrulanmıştır. Bu çalışmanın amacı kendini yapılandırabilen algoritmalar kullanarak, sensör ağının kapsama alanını arttırmak ve bunu yaparken de enerji verimli sistemi oluşturmaya çalışmaktır.

İşlemci ve sensör teknolojilerindeki fiyat ve performans iyileştirmeleri, sensör ağları uygulama ve araştırmalarını arttırmıştır. Buna bağlı olarak farklı protokoller ve uygulamalar ihtiyaca göre artış göstermiştir. Artık farklı protokolleri birbirine çeviren cihazlara da ihtiyaç artmaya başlamıştır. Bilinen ZigBee ve Bluetooth gibi protokollerin dışında, özel isteğe göre uyarlanmış sensör ağlarında bir protokoller arası iletişimi sağlayan bir yapıya ihtiyaç bulunmaktadır. Bu tezde protokoller arası iletişimi sağlayan yapının sensör ağının yardımı ile kapsama alanının arttırılması ve bunu mümkün olduğunca az enerji tüketerek yapması planlanmıştır.

Yapılan çalışma sonunda, tasarlanan protokolün, protokol dönüştürücünün sensör ağını kullanarak kapsama alanının arttırılmış olduğu gözlenmiştir.

**Anahtar sözcükler:** Kablosuz sensör ağları, sensör ağlarında kapsama alanı, kendini yapılandırabilen sensör ağları.

## ACKNOWLEDGEMENTS

At the beginning, I would like to express my sincere gratitude to my supervisor Professor Mustafa GUNDUZALP for his guidance, support and patience during this study. I have learned so much from him in the process of preparing this thesis and algorithms.

I also would like to express my love to my parents, who are always willing to courage me in every possible way in my life.

Furthermore, I also thank my beloved friends Sermet and Güneş for sharing their precious time.

Finally, I would like to thank my dear girlfriend for her patience and support.

Atilla Osman Mert GEMALMAZ

İzmir, 2017

## **TEXT OF OATH**

I declare and honestly confirm that my study, titled “Construction of Self Organizing and Updating Wireless Sensor Networks Using Energy Efficient Microprocessors” and presented as a Master’s Thesis, has been written without applying to any assistance inconsistent with scientific ethics and traditions. I declare, to the best of my knowledge and belief, that all content and ideas drawn directly or indirectly from external sources are indicated in the text and listed in the list of references.



Atilla Osman Mert Gemalmaz

.....  
September 26, 2017

# TABLE OF CONTENTS

	<b>Page</b>
<b>ABSTRACT</b>	ii
<b>ÖZET</b>	iv
<b>ACKNOWLEDGEMENTS</b>	v
<b>TEXT OF OATH</b>	vi
<b>TABLE OF CONTENTS</b>	vii
<b>INDEX OF FIGURES</b>	xi
<b>INDEX OF TABLES</b>	xiv
<b>INDEX OF SYMBOLS AND ABBREVIATIONS</b>	xv
<b>1 INTRODUCTION</b>	<b>1</b>
<b>2 FUNDAMENTALS OF WSN DESIGN</b>	<b>3</b>
2.1 Definition of a sensor node:	3
2.2 Hardware Components of a WSN	3
2.3 Fundamentals of RF Communication	6
2.3.1 Electro Magnetic Spectrum and Radio Spectrum:	6
2.3.2 RF Communication Systems:	6
2.3.3 Wireless Communication Systems	8

•	Modulation	10
•	Wireless Channel Effects:	15
2.4	Network Topologies	17
2.4.1	Point to Point Network Topology	18
2.4.2	Bus Network Topology	19
2.4.3	Ring Network Topology	20
2.4.4	Star Network Topology	21
2.4.5	Mesh Network Topology	22
2.5	Routing Protocols in Mesh Networks	23
2.5.1	Problems of Routing	24
•	Energy Consumption:	24
•	Scalability	24
•	Addressing	25
•	Robustness	25
•	Topology	25
•	Application	25
2.5.2	Network Routing Protocols	26
•	Data-Centric and Flat Routing Protocols	27



○	Flooding:	27
○	Gossiping:	28
○	Sensor Protocols for Information via Negotiation (SPIN)	29
○	Directed Diffusion:	30
3	METHODOLOGY	33
3.1	Problem Statement	33
3.2	Methodology	34
3.2.1	Discovery & Configure Procedure (DCP)	37
•	Detailed Operation of DCP	39
3.2.2	System Architecture	45
•	Software Layers	45
•	Radio Message Frame Structure	48
3.3	Protocol Message Sequences	53
3.4	Special Cases	57
3.4.1	Special Case 1: Battery about to die	57
3.4.2	Special Case 2: Unreachable Node	57
3.4.3	Special Case 3: Changing place of the node	58
3.5	Implementation of Protocol	58

3.5.1	Hardware Studies	59
3.5.1.1	Test Node Structure	59
3.5.1.2	MCU Kit	60
3.5.1.3	RF Development Kit	62
3.5.2	Software Studies	64
3.6	Test and Validation	66
4	CONCLUSION AND FUTURE WORK	71
	REFERENCES	72

## INDEX OF FIGURES

Figure 1 Generic WSN architecture .....	4
Figure 2- EM Spectrum .....	6
Figure 3-Simplex Mode Communication .....	7
Figure 4- Half Duplex Communication .....	7
Figure 5-Full Duplex Communication .....	8
Figure 6-Generic Analog RF system: (a) transmitter architecture, (b) receiver architecture .....	9
Figure 7-Generic Digital RF system: (a) transmitter architecture, (b) receiver architecture .....	10
Figure 8-(a) baseband signal, (b) passband signal.....	11
Figure 9-RF microelectronics, Simple communication system.....	12
Figure 10-Amplitude Modulation.....	12
Figure 11- Phase and Frequency Modulation.....	13
Figure 12-Digital Modulation Schemes.....	14
Figure 13- Reflection.....	16
Figure 14- Refraction.....	16
Figure 15- Diffraction.....	17
Figure 16- EM wave scattering.....	17

Figure 17-Physical and Logical Topology .....	18
Figure 18-Point-to-Point Topology .....	19
Figure 19-Bus Network Model .....	20
Figure 20-Ring Network Model.....	21
Figure 21- Star Network Topology .....	21
Figure 22-Mesh Network Topology .....	23
Figure 23-Flooding Scheme.....	27
Figure 24-Gossiping.....	29
Figure 25-Process of SPIN Routing Protocol .....	30
Figure 26-Process of Directed Diffusion .....	32
Figure 27-Problem Statement .....	34
Figure 28- State Machine of DCP and Operation .....	37
Figure 29-Coverage of Master Node .....	38
Figure 30- Separation of different Networks .....	39
Figure 31-DCP- Step1: Broadcasting .....	40
Figure 32- DCP Step 2 .....	41
Figure 33- Node-2 sends DCP table .....	43
Figure 34- Node-1 starts DCP sequence .....	44

Figure 35-Node-3 DCP Operation.....	45
Figure 36-Layered Architecture of Our WSN System .....	47
Figure 37-Layered Architecture of Messages between two nodes .....	48
Figure 38- DCP Protocol Message Sequences .....	55
Figure 39- DCP Normal Operation Message Sequences.....	56
Figure 40- WSN Test Node .....	60
Figure 41- FRDM-KL25Z Kit.....	61
Figure 42- TI CC1120 RF Kit .....	62
Figure 43- Ordinary RX Mode .....	63
Figure 44- RX Sniff Mode.....	63
Figure 45- Radio Message Structure Definition.....	65
Figure 46- Protocol Message Frame Structure .....	66
Figure 47- Test and Validation Setup.....	67
Figure 48-Communication Log Between Master and PC.....	68

## INDEX OF TABLES

Table 1- Routing Protocols	26
Table 2-DCP Table status	40
Table 3-DCP Status Tables	43
Table 4-Transport Layer Frame	50
Table 5- Protocol Layer Frame	51
Table 6- ARM Cortex-M Architectures	61
Table 7- CC1120 RX Modes	63
Table 8- Measured Current Consumptions	69
Table 9- Power Consumptions of 4 Scenarios	69

## INDEX OF SYMBOLS AND ABBREVIATIONS

### Symbols

### Explanations

$w(t)$

Central Frequency



## Abbreviations

SOC	System on Chip
MCU	Micro Controller Unit
RCU	RF Control unit
WSN	Wireless Sensor Networks
RF	Radio Frequency
RCU	RF Control Unit
DCP	Discovery and Configuration Procedure
AM	Amplitude Modulation
FM	Frequency Modulation
ASK	Amplitude Shift Keying
FSK	Frequency Shift Keying
PSK	Phase Shift Keying



# 1 INTRODUCTION

A Wireless Sensor Network (WSN) is a cluster of sensor nodes organized into a network for sensing and controlling the physical events in the coverage area. Each node is distributed over an area for monitoring conditions of a physical field and send the relevant data to each other. Moreover, most of these nodes can consist of MCUs, SOCs, memories, RF transceivers, power source and sensors. Some WSNs are powered with a limited battery source while others use AC grid.

Considering price is the most important aspect in the market, most of the WSNs have limited performance of MCUs and limited battery power. Therefore, these systems should be cost and energy effective. In order to achieve this goal, these nodes should be designed with highly effective algorithms in order to increase the lifespan of the battery.

The algorithm developed for this thesis is applied on home applications. In home applications, it is unwise to use these sensor nodes with cables or AC power supplies, because installation becomes harder and architectural issues can be raised. However, battery life should be as much as increased with a good engineering design for these nodes so that batteries do not have to be changed frequently.

In most of the “Internet of Things” applications, field results, in our case home data, should be sent to the cloud servers. For example, after temperature of the rooms is monitored, the results are transmitted through the internet servers to be processed. In other words, first local sensor network collects data from home and then this data is sent via internet. Most of the home applications depend on a modem or a mobile phone with an internet access to be used as a gateway through the internet. As a result, there should be a master node which can communicate with all the sensors and the modem. Since there are many different protocols for monitoring and controlling of the field sensors, there should be a master node which is a bridge between internet and the local protocol.

Although battery life is an important aspect for WSNs, energy effective coverage area phenomenon is another issue. Generally, antenna spends the most of the power in WSN nodes, thus increasing the antenna power for more coverage is resulted by a low battery life. In this point of view, radio should be used as less as possible.

My goal in this thesis is to increase the range of the master node of the sensor network by using less energy. In other words, it is planned to increase the range of the WSN with the same antenna power. In order to solve this phenomenon an algorithm called Discovery and Configuration Protocol is built. For testing and validation, a system which implements Discovery and Configuration Procedure (DCP) algorithms is constructed. Special circuit is built and used for validation of this algorithm in the field.

In discovery and configuration protocol, range increase is provided by using nodes as routers instead of using them just for monitoring and controlling points. This protocol decides when a node should be acted as a router. Using this approach, gateway range performance is tried to be increased so that control over the sensors increases.

The aim of this thesis is to determine the behavior of the gateway included self-configurable systems. The main contribution of this thesis is to increase coverage area of the gateway between sensor network and the real world while trying to minimize the energy consumption.

This thesis is divided into 4 chapters. Fundamentals of WSN design, including wireless communication basics and routing protocols, is represented in Chapter 2. In Chapter 3, methodology of the thesis is explained which consists of Discovery and Configuration Procedure algorithm and its frame structure with the test and validation steps are explained. The chapter 4, is related with conclusion and recommendation of author. Finally, references and appendix are included.

## **2 FUNDAMENTALS OF WSN DESIGN**

Designing a wireless sensor network requires deeper knowledge including wireless technologies, networking, embedded system design, digital signal processing and engineering. [Akyıldız et al., 2010] In this part it will be examined the hardware considerations influencing the wireless sensor network design.

### **2.1 Definition of a sensor node:**

A wireless sensor network consists of units of sensor nodes. Apart from sensing physical conditions on the application field, each sensor node also responsible for communicating with other nodes. The following operations are handled by a sensor node:

- Gathering the sensor data from its sensing unit.
- Sending this sensor data to related node,
- Routing or repeating the signal of other sensor nodes to destination node

For instance, a temperature sensor node meters the temperature value and after processing this data, it sends the related node.

### **2.2 Hardware Components of a WSN**

Hardware selection is one of the most important parts in wireless sensor networks. Although different applications need different configurations, system designer should always consider the network size, cost and energy consumption [Karl et al., 2005]. In some cases, power consumption has high importance to the designer whereas in other cases the cost is the most important asset.

Briefly, there is a system architecture for supporting most of the WSN solutions which consists of micro controller unit, Sensor Unit, Communication Unit, power unit. Hardware structure is explained in the Figure-1 below.

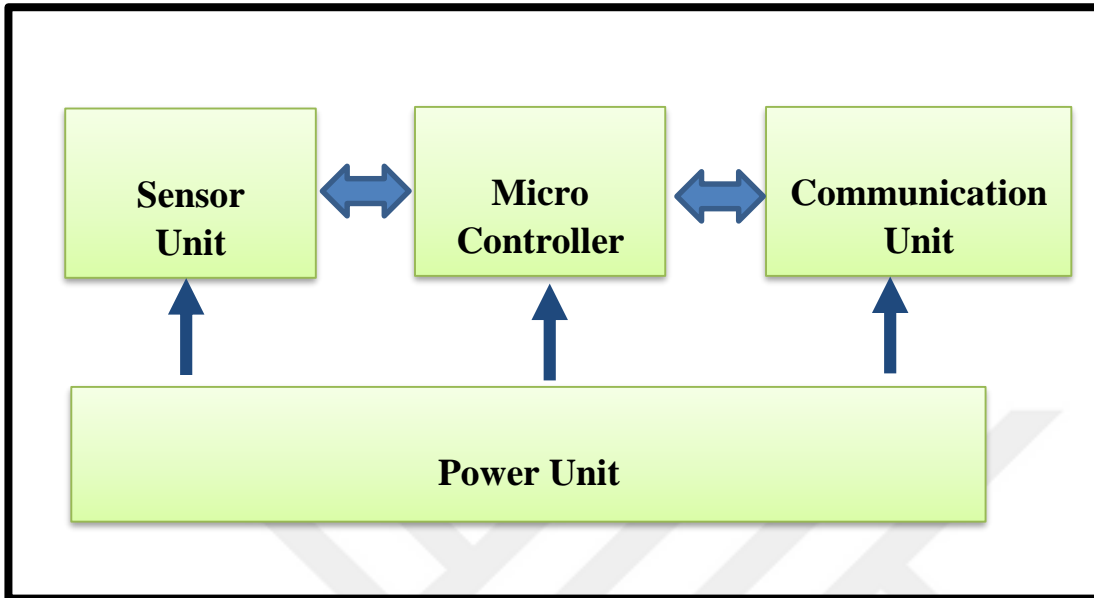


Figure 1 Generic WSN architecture

According to Figure 1, all the blocks are explained below:

- **Microcontroller Unit:**

This part can be considered the brain of the sensor node, since The fact that micro controller unit process and manage all data traffic. One of the main responsibility of micro controller unit is to gather data coming from sensor unit and process it. In addition to sensor activity, MCU is also responsible for managing the communication with other sensor nodes by sending and delivering messages to radio control unit. Furthermore, MCU is also responsible for sleep management of the system in order to decrease power consumption. In some applications integrated circuits can be used for sensing and communicating unit. In this case microcontroller use serial communication technologies to communicate integrated circuits such as SPI, I2C, UART etc. Moreover, improvements of silicon technology results in System-On-Chip (SOC) solutions. In some SOC solutions communication unit and MCU is implemented in same chip.

- **Power Unit:**

As the name suggests power unit is the power source of the system. This unit feeds MCU, communication device and sensor unit so that they can work properly. Some systems use AC mains while other use battery power. However, most of the WSN application uses battery power. Considering the battery power is a limited source, system should save as much energy as possible.

- **Sensor Unit:**

Sensor unit is the interface between sensor node and physical world. Main role of this unit is to collect data on field and send it to MCU. Sensors convert physical signals into electrical signals so that MCU can understand. (Wang, 2010). Take into consideration that different applications need different kind of sensors.

- **Communication Unit:**

Communication unit is the interface between other nodes and the micro controller unit. In view of the fact that our topic is wireless sensor networks, the communication unit is wireless capable communication unit. Owing to the fact that wireless systems do not use cables, it is easy to implement and easy to place. Most communication units have an antenna, antenna match circuit and RF integrated circuit. Moreover, in some designs, instead of RF-IC, microcontroller itself is used as an interface with antenna. However, this results in more complex programming. RF-IC turns the signal coming from antenna into related RF protocol in necessary frequency. RF-IC is, on the other hand, communicates with microcontroller so that microcontroller just processes its data not also the RF protocol implementation. In addition, Using RF-IC also saves memory and process power of microcontroller unit. The goal of antenna is to send and deliver the RF signals. The efficiency of the antenna is very important since communication module uses most of the energy of a sensor node.

## 2.3 Fundamentals of RF Communication

### 2.3.1 Electro Magnetic Spectrum and Radio Spectrum:

Electromagnetic spectrum defines the range and scope of all kinds of electromagnetic radiations. This spectrum starts with sound which has low frequency and goes to high frequencies which are harmful radiations like gamma-ray. Figure 2 indicates how electromagnetic spectrum is divided and also it shows the radio spectrum.

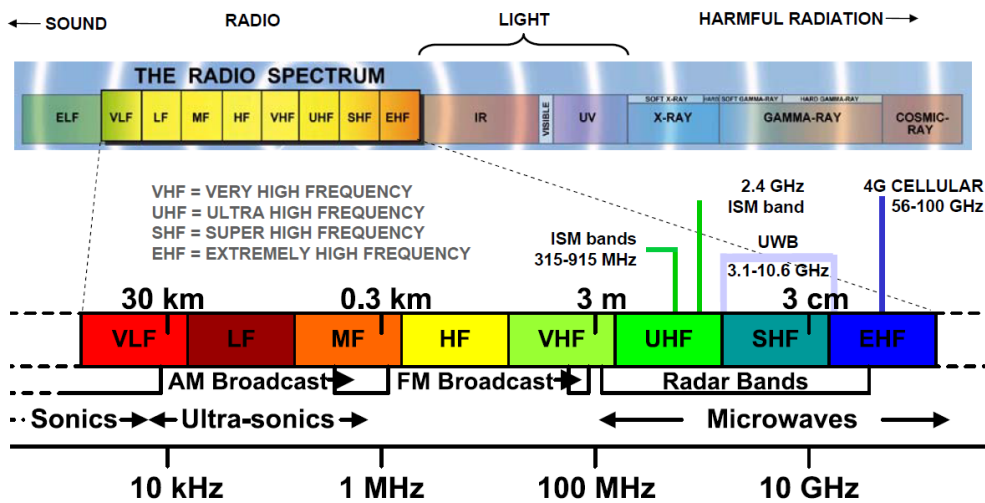
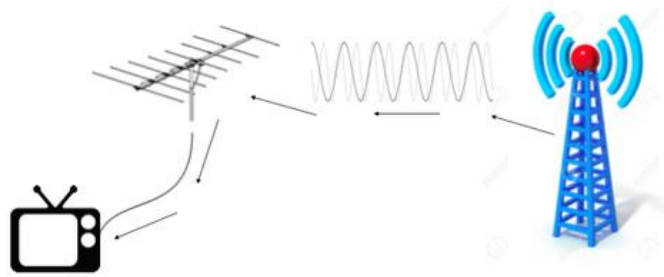


Figure 2- EM Spectrum

### 2.3.2 RF Communication Systems:

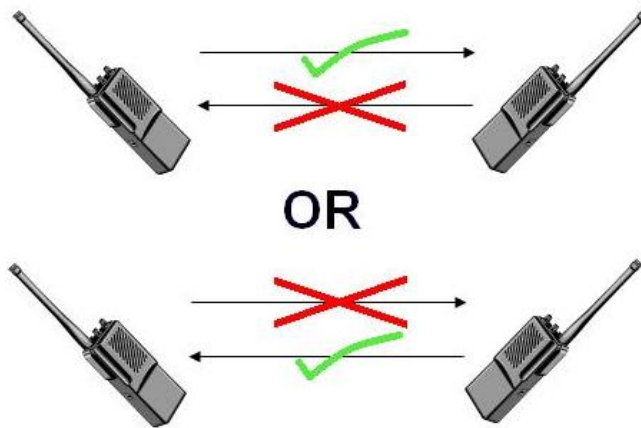
According to RF data flow of data, communication is divided into three parts called simplex, half duplex and full duplex.

In simplex mode, one-way communication between transmitter and receiver is occurs. For instance, FM radio and TV uses simplex transmission since they broadcast data to our devices.



**Figure 3-Simplex Mode Communication**

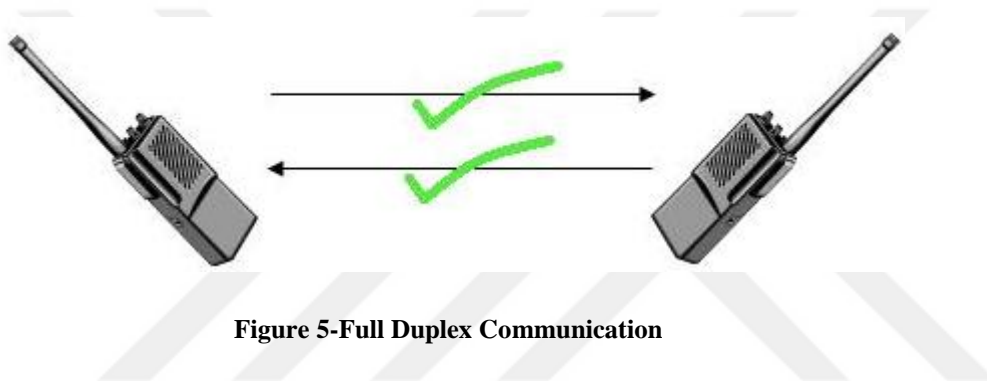
Half duplex systems are bi-directional so that they can transmit and receive data. However, simultaneous communication is not allowed. While one device transmitting the other device cannot transmit data. Although communication is bi-directional over the same frequency, duration of the message is unidirectional As figure 4 demonstrates walkie-talkie systems and wireless mouses are very well known examples for half duplex communication.



**Figure 4- Half Duplex Communication**

In full duplex communication is similar to half duplex communication in terms of bi-directional connection. Full duplex communication can be considered as a simultaneous half duplex communication.

Two communication frequencies are used to establish communication channel. Using each of the frequencies data is transmitted and received solely. As figure 5 states cellular phones are the best known full duplex communication since both of the devices can transmit and receive data at the same time.



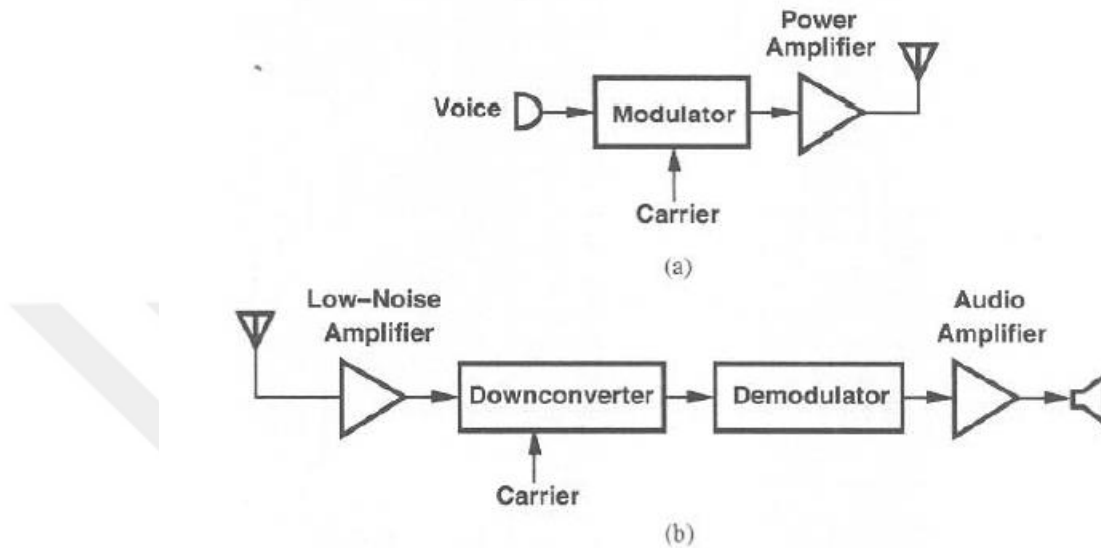
**Figure 5-Full Duplex Communication**

In the light of the information above, our protocol is planned to use half-duplex communication. Because our RF IC module has got only receive, transmit and idle modes in one instance. Moreover, our protocol does not need full-duplex communication feature since we do not need to communicate with the nodes during communication instance in order to spend less energy.

### **2.3.3 Wireless Communication Systems**

In wireless communication systems, data sent from transmitter to receiver over the communication channel. There are two types of generic RF systems which are described as analog and digital systems [Razavi et al.,1998]. Basic structure of an analog RF system is shown in Figure 6.





**Figure 6-Generic Analog RF system: (a) transmitter architecture, (b) receiver architecture**

In the path of transmission(Figure-6-a), first input signal comes to modulator with high frequency carrier. Then, power amplifier amplifies the signal and drives the antenna. On the other hand, considering receive path(Figure-6-b), the input signal comes from transmitter comes to a low-noise amplifier (LNA), then by using downconverter to convert high frequency in put signal into lower frequencies. After converting the signal to a low frequency, demodulation operation is processed and then demodulated output is amplified. After last amplification, the message coming from the transceiver is processed and received.

The digital RF transceiver operation is indicated in the Figure 7 in terms of architecture of transceiver and receiver.

Considering transceiver architecture Figure 7(a), first, the input signal shown as voice, is converted from analog signal into a digital signal by the help of an analog to digital converter (ADC). In addition, digitalized signal is compressed to decrease the bit rate so that the bandwidth. After this, coding and interleaving operation formats the

data for receiver to minimize the transmission errors when RX reverse operations are made. In the next operation, pulse shaping, signal is shaped before modulation and power amplifier due to the fact that rectangular pulses are not optimum for modulating the data.

After transmission, the signal carries through the air to the receiver which is indicated in Figure 7(b). Receiving data process is started with amplification with LNA and it is followed by down-conversion and digitalization in order. These operations are followed by demodulation, equalization, decoding and de-interleaving and decompression in the digital domain. As can be seen these operations are reverse of the digital transceiver operation. Finally, the digital signal is converted to analog signal via DAC and after amplification the final signal is received.

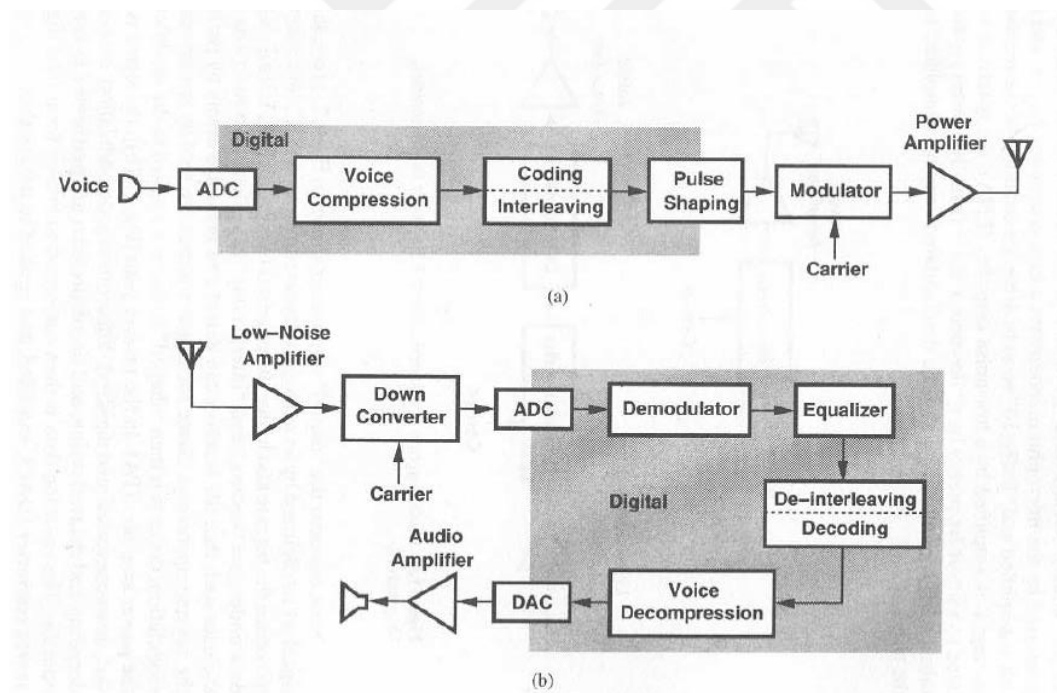


Figure 7-Generic Digital RF system: (a) transmitter architecture, (b) receiver architecture

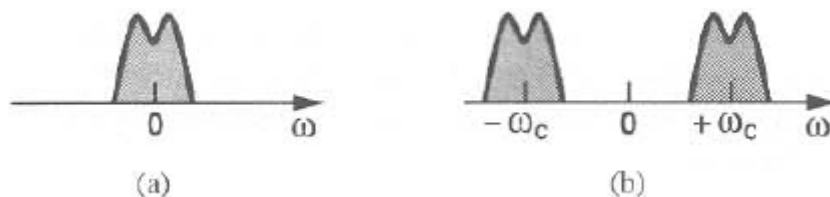
- **Modulation**

The waveform of the transmission signal is generally carried by a high frequency carrier which is modulated by original signal. [Razavi, B. et al 1998] In other words,

modulation is the process of imposing a low frequency signal onto a high frequency signal in order to prepare a transmit packet. On the contrary, demodulation is the reverse operation of the modulation. The aim of performing demodulation process is to extract the original baseband signal with minimum noise and distortion. Usually, data signal is modulated in the transmitter side while signal is demodulated in receiver side. Figure 10 indicates the modulation and demodulation process. The reasons why modulation is needed in modern RF systems are:

- Electromagnetic waves which are ranged between 20 Hz and 20 kHz cannot be radiated efficiently in the space. That's why low frequency signals should be converted into a high frequency signal by modulation process.
- In wireless systems, antenna size is very important and it is dependent to wavelength to reach necessary gain.
- RF communication should be done in certain spectrum due to regulations.

In modulation concept, there are two types of signals defined which are baseband and pass-band. Baseband signal is the signal whose spectrum is different from zero in the vicinity of " $\omega = 0$ ". On the other hand, passband signal is a signal whose spectrum is different from zero around carrier frequency ( $\omega_c$ ) and outside of this band is negligible.

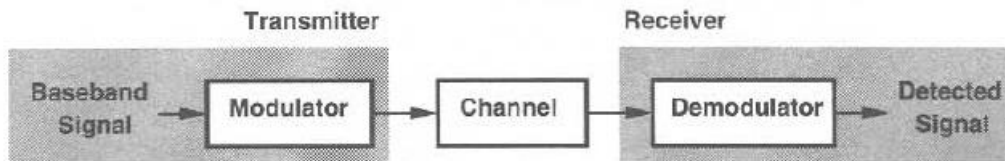


**Figure 8-(a) baseband signal, (b) passband signal**

Modulation is a conversion of a baseband signal to a pass-band instance. Pass-band signal can be shown as:

$$x(t) = \alpha(t) \cos[(\omega_c t + \vartheta(t))]$$

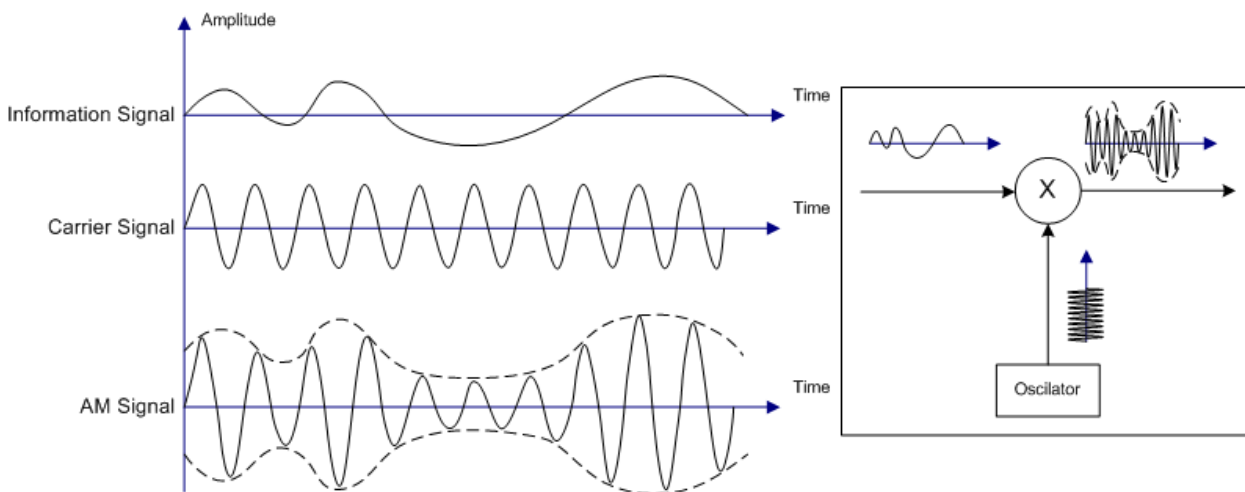
Where “ $\alpha(t)$ ” and “ $\vartheta(t)$ ” are time functions. “A  $\cos(\omega_c t + \vartheta)$ ” is the periodic carrier signal and by altering its phase or amplitude we can do modulation.”  $\omega_c t + \vartheta(t)$ ” is called the total phase where “ $\vartheta(t)$ ” is the excess phase. Instantaneous frequency is “ $\omega_c + \frac{d\vartheta}{dt}$ ”



**Figure 9-RF microelectronics, Simple communication system**

Modulation types are divided into two parts which are called digital modulation and analog modulation. Analog modulation is separated into Amplitude Modulation (AM), Frequency Modulation (FM) and Phase Modulation (PM).

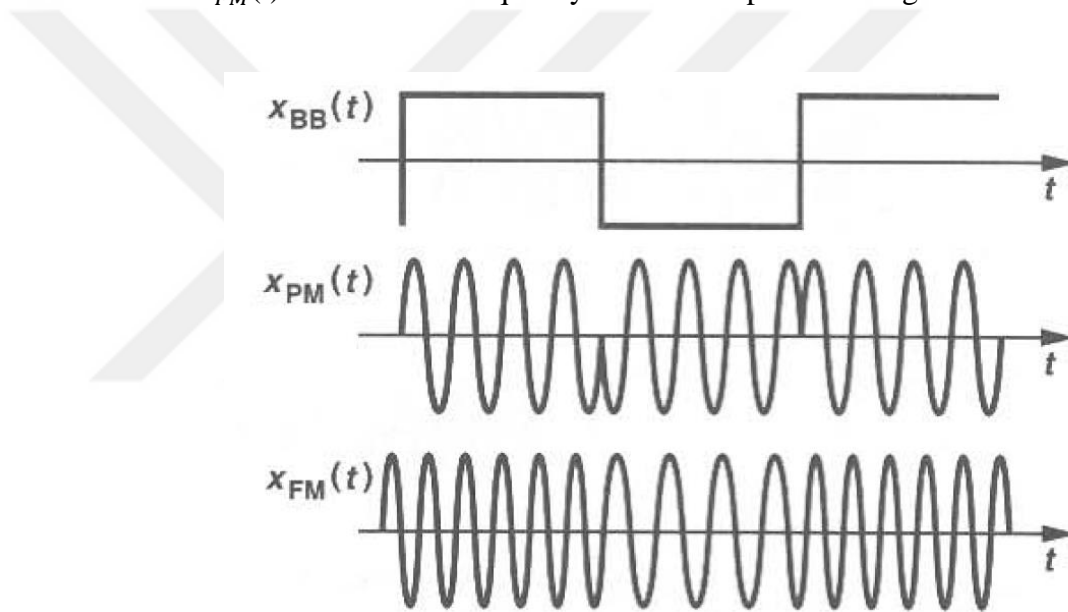
The amplitude of the carrier signal is increased or decreased in compliance with the input signal.



**Figure 10-Amplitude Modulation**

As can be seen the Figure 10, the information signal or input signal, are mixed so that input signal is carried by the carrier signal in order to transmit. The final signal, AM signal, is created by varying carrier signal according to the information signal [Razavi, B.et al 1998]. The advantage of using amplitude modulation is reaching to the long distances. On the other hand, eliminating high noise on the receiver side.

The following figure explains the operation of frequency and phase modulation operation.  $X_{BB}(t)$  is the baseband signal.  $X_{PM}(t)$  shows the phase modulated signal while  $X_{FM}(t)$  indicates the frequency modulation processed signals.



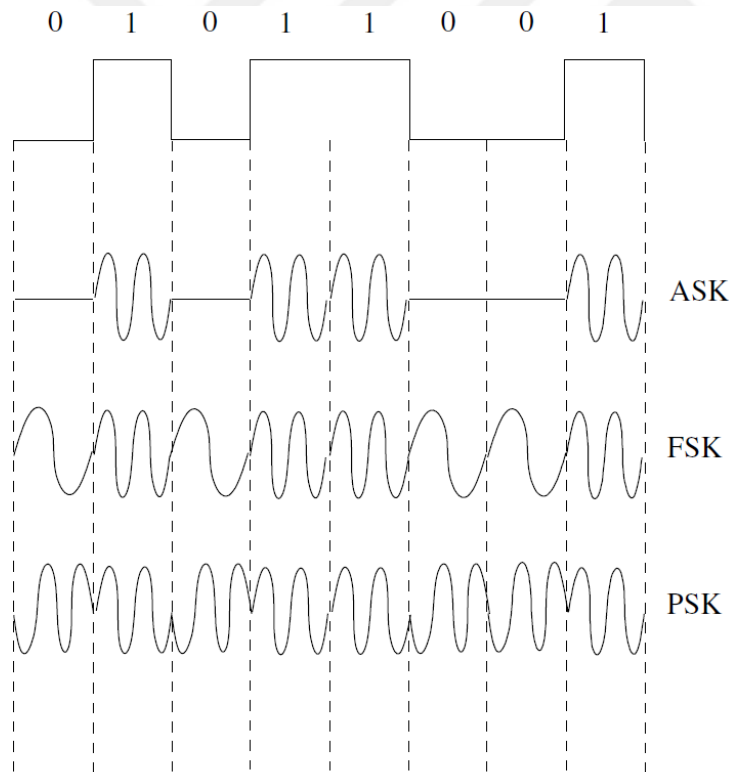
**Figure 11- Phase and Frequency Modulation**

The frequency of the carrier changes with respect to baseband signal in the definition of Frequency Modulation whereas in the phase modulation technique, phase of the carrier varies according to baseband signal.

Analog FM uses more than analog PM since it is easier to modulate and demodulate the waveforms [Razavi, B.et al 1998]. The benefits behind using FM are minimized noise effects compared to AM since amplitude does not change. However, compared to AM, FM has a less coverage.

Considering source and channel coding are done in digital domain which the data is processed in bits while wireless communication occurs in analog domain which RF waveforms transmits over an antenna. There should be a conversion between digital domain and analog domain by using modulation techniques which is digital modulation [Akyildiz, I. F. et al,2010]

Digital modulation usually known as “Shift Keying”. The bits of digital signal, like analog modulation, is modified with respect amplitude, frequency and phase before transmitted. Digital modulation is divided into three parts which are called Amplitude Shift Keying (ASK), Frequency Shift Keying(FSK) and Phase Shift Keying(PSK). The following figure shows shift keying operations:



**Figure 12-Digital Modulation Schemes**

As it can be seen from the Figure 12, ASK modulation is modulating the amplitude of the waveform according to information bit which consists of ones and zeros. On-Off Keying (OOK), which is very simple form of ASK, transmits a signal

when information signal bit is 1 whereas it transmits nothing when digital bit is 0. Although ASK is easy to implement which is an advantage, during amplification process, the waveforms are susceptible to noise.

FSK is one of the mostly used digital modulation techniques. In this process, the frequency of modulated signal varies according to digital bit of ones and zeros. The operation is explained in the Figure 12. Compared to ASK, FSK is less susceptible to noise. However, in theory, transmitting FSK modulated signal requires more bandwidth. Very known usage of frequency shift keying on popular protocols is Bluetooth.

PSK is established upon altering phase of the waveform with respect to bits trying to transmit. According to figure 12, varying input bits results in modification of the phase on the output signal.

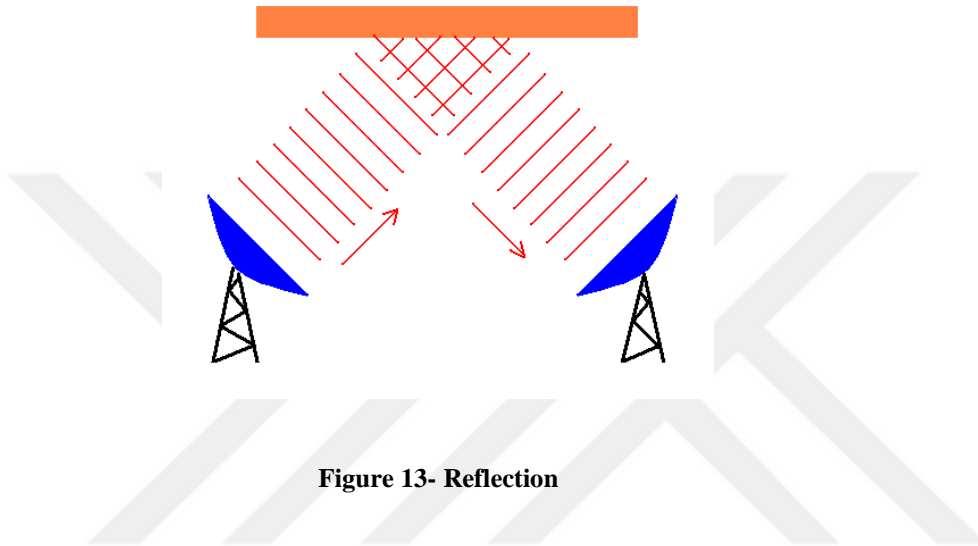
PSK modulated systems, less susceptible to noise and they are bandwidth efficient. The main disadvantage of having a PSK modulated system is that PSK needs synchronization in phase and frequency which complicates the receiver and transmitter design. ZigBee is a very popular PSK modulated protocol.

- **Wireless Channel Effects:**

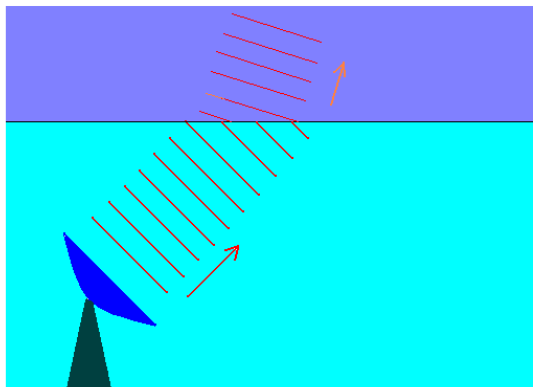
In the previous chapter, we have talked about the modulation and kinds of modulation. Modulated waveforms is transmitted from the transmitter as electromagnetic signals through the air till its destination which is the antenna of the receiver side. During the propagation of these EM signals are distorted via external factors which results in failure in the data or loss of data at the receiver.

The sources of the distortions on the transmitted EM waveforms are described as attenuation, diffraction, scattering and reflection/refraction [Akyildiz, I. F. et al,2010]. EM wave propagates through the air; attenuation occurs on the signal strength so that path loss occurs for radiated waves on the air. The definition of reflection occurs when EM wave is encounter with a boundary which consist of two different kinds of material,

a certain amount of the wave is hopped from the surface. As the result of reflection multiple waves can reach the receiver and transmitter side. On the hand, in the refraction case, a certain amount of the EM wave can propagate through the boundary which results in fading on the signal. See Figure-13 and Figure-14.



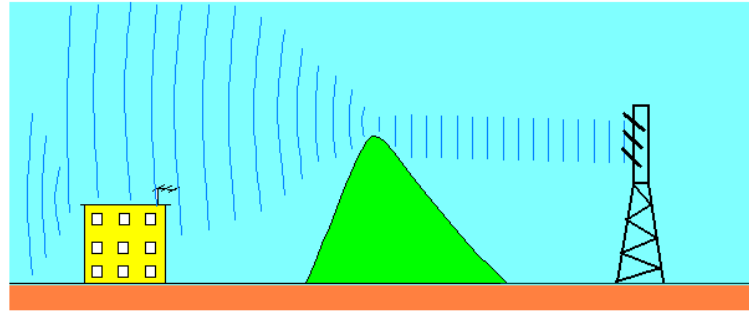
**Figure 13- Reflection**



**Figure 14- Refraction**

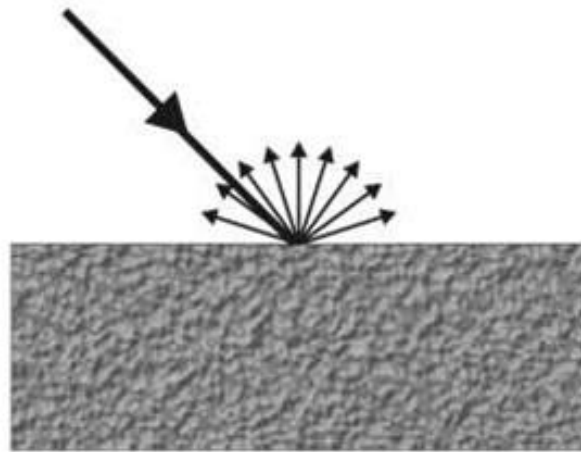
Diffraction occurs when a EM wave is penetrated through a sharp obstacle or it is propagating into a hole with dimensions close to its wavelength, the phenomenon of diffraction occurs.





**Figure 15- Diffraction**

**Scattering** occurs when EM waves strike on surfaces, they scatter along the different directions.

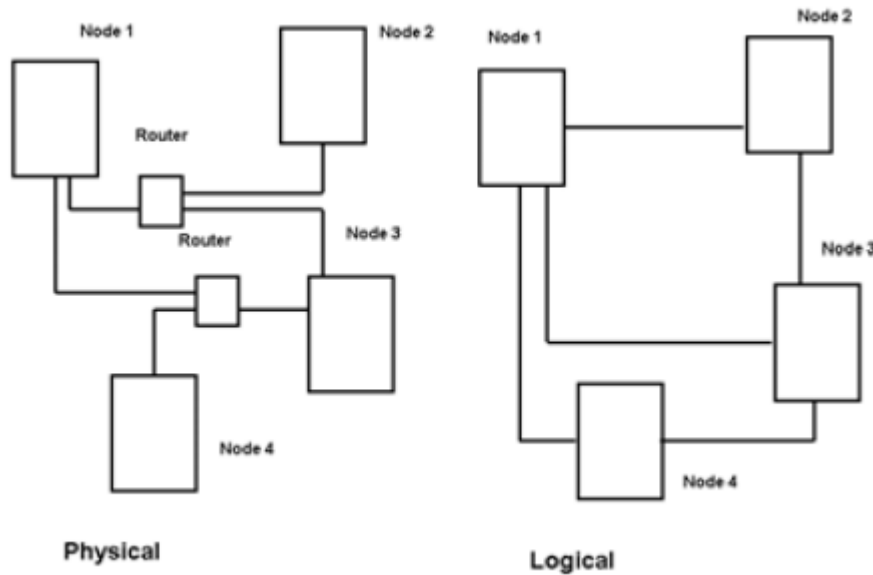


**Figure 16- EM wave scattering**

## **2.4 Network Topologies**

In terms of mathematics, the topic of topology examines the objects which have constant characteristics under distortion. Furthermore, computer network topology concept investigates the configuration of system elements and the interconnection of these elements [Santra, S. et al,2013]. Network topologies can be investigated into 2 parts which are known as physical and logical. Physical network topology term is

related to the hardware connections between nodes. The logical network topology, also known as signal topology, is associated with the flow of the data on the network. Signal topology can be configured via routers so that while physical connections remains same, logical connection can be altered. Figure 17 explains this phenomenon:

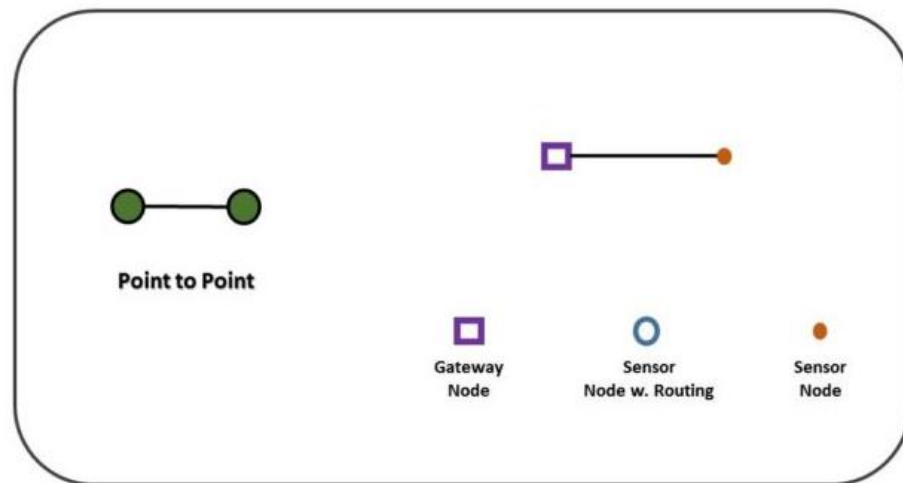


**Figure 17-Physical and Logical Topology**

Eight different physical topology is defined which are “Point to Point”, “Bus”, “Star”, “Ring”, “Mesh”, “Tree”, “Hybrid” and “Daisy Chain”. In this section, network topologies will be investigated in terms of their nature, advantages and disadvantages.

### 2.4.1 Point to Point Network Topology

In this concept, two endpoints are linked directly. This is the simplest network in terms of topology. Bluetooth is a well-known technology that uses point to point topology. Bluetooth is the link between the mobile phone and the device.



**Figure 18-Point-to-Point Topology**

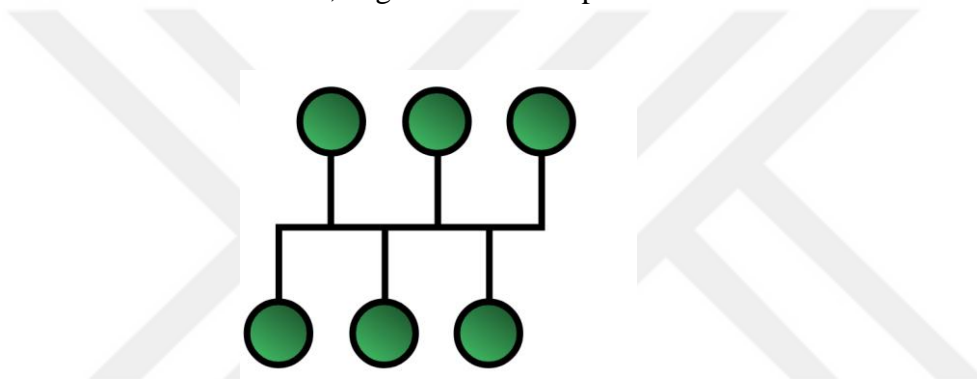
The advantages of using this kind of technologies are low system cost and easy installation. However, this kind of usage limits range of the system by depending on the 2 node's antenna structure and power. That's why usually one device has to gateway capabilities to reach the internet. Considering Bluetooth example, a field sensor can connect to mobile phone and sends its data, then mobile device sends this data to the internet. The following figure demonstrates how point to point networks can be adopted to IOT.

#### **2.4.2 Bus Network Topology**

In this topology, each node is connected to each other via a single line. When a node transmits data, it broadcasts this message to all devices connected to this line. Each node controls destination address message whether it matches its own source address or not. If the destination and its own source address is same, target node takes this message and processes it. Else if the addresses do not match, target skips this message.

Easy to implement nature and cheap cost of this topology is best for small networks. Local Area Networks (LAN) and Wireless-LAN (W-LAN) uses this topology.

The disadvantage of this topology is that every node on the bus sees the message transmitted from the source which is resulted in security issues. Moreover, every message should be checked by all target devices which causes a traffic on the network. In addition, if any fault occurs on the main line, whole network will be crashed. In case of fault detection and maintenance, engineers should spend more time for solution.



**Figure 19-Bus Network Model**

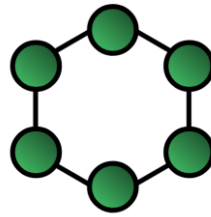
### **2.4.3 Ring Network Topology**

This topology is like a closed loop version of bus topology. In ring topology, all nodes are connected to next node in a circular manner. The data passes from one device to other until it reaches its destination in the ring. While the data is travelling from source node to destination node, repeaters are the middle players for carrying the messages. Data can be moved to clockwise and counter clockwise direction or both.

This kind of topology better than bus network topology in case of load handling. Moreover, it is easy to locate where the fault occurs on the network.

The biggest disadvantage of having ring network topology is that one of the failed nodes causes the failure of the entire network. In addition, adding or removing an

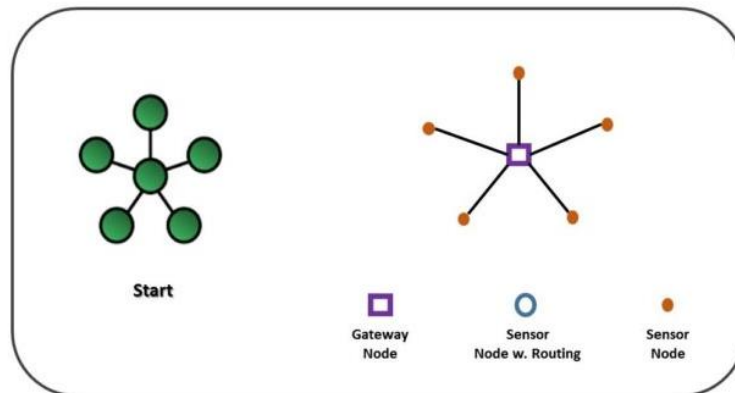
element of the network affects whole network. System has a security drawback which is caused by the movement of data one node to another through intermediate nodes.



**Figure 20-Ring Network Model**

#### 2.4.4 Star Network Topology

In star networks, each network device connects to a central device with a point to point connection. Central device manages the network operations and traffic. All devices are indirectly connected to each other via central device.



**Figure 21- Star Network Topology**

In star networks, it is easy to add a new node to the system. The fact that all devices are connected to the central device, this operation minimize the security risks. Moreover, centralized nature of these networks, creates an isolation for each of the network components. Furthermore, detecting the failures are easy since every device should talk to central node. Apart from all advantages, the biggest risk in this kind of

network is that the failure on the central device. If any failure occurs on the central device, network operations would be failed. In addition, network size depends on the performance of the central device because its resources are the limits for this network. Finally, although it is easy to implement a star network, it also has a high setup cost.

Wi-Fi network hub is one the best famous examples of star networks. The following figure illustrates a field application of star network topology for controlling field sensor nodes.

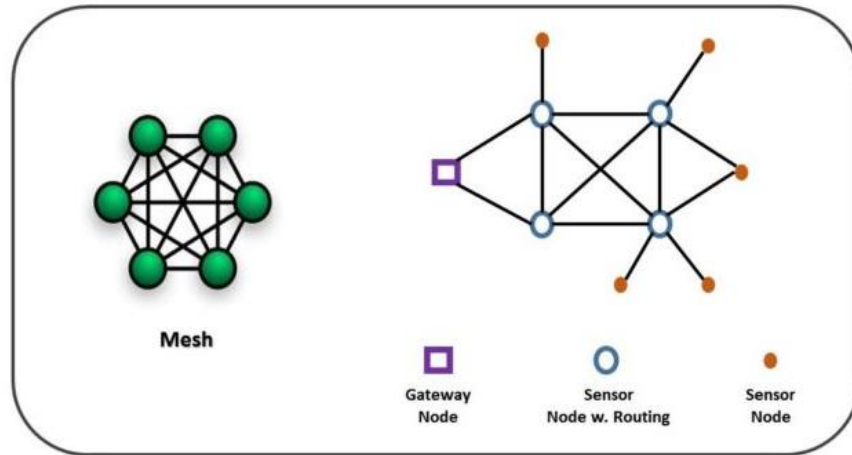
#### **2.4.5 Mesh Network Topology**

In this type of network topology, all nodes are interconnected to each other. Mesh networks are designed to transmit data to specific node not from a one node but more [Berker,B.,2010]. By using this topology, if a device fails network, usually covers this fault and sends the relevant messages to other nodes. Generally, there are two types of nodes which are simple sensor nodes and router/repeater capable sensor nodes. Simple nodes only answer the messages coming from other nodes. The other type of nodes in the mesh network is responsible for routing or repeating the messages to other nodes. In addition, due to improvements in IOT technology, mesh networks need one more node type which is responsible for connecting internal mesh network to the outside world. This gateway type node act as a bridge between mesh network and internet by collecting data from field nodes as in the star network topology. In this kind of networks, mesh nodes are placed such that every node has to be in the coverage are of at least one node.

Mesh networks have a variety of usage areas including building automation, long range coverage, data mining etc.

One of the best advantages of mesh networks is that redundancy of connections so that data can go to its target from different paths. In other words, in terms of covering failures, mesh network structure is the better compared to the other network topologies.

Furthermore, coverage can be increased in this kind of topology. For example, the gateway node can connect to the nodes which are beyond its coverage.



**Figure 22-Mesh Network Topology**

On the other side, main disadvantages of using mesh networks are the high cost and high complexity. Having included repeater and router nodes and node hops increase the latency of the network.

## **2.5 Routing Protocols in Mesh Networks**

Routing is one of the most important factors in design of wireless sensor networks. Furthermore, the data is more important than who sent the data in WSN systems. This structure of WSN challenges to use traditional routing techniques. Moreover, node resources such that energy, memory and processing power should be managed carefully. In addition, the routing and system design is shaped from application to application. For instance, in some application quality of service is the most important design decision than the other design decisions such as health monitoring applications.

In this part, challenges for routing and routing approaches will be taken into account in detail.

### 2.5.1 Problems of Routing

In design of routing on the WSN energy consumption, scalability, addressing, robustness, topology and application is described as the main challenges [Akyıldız et al.,2010].

- **Energy Consumption:**

In the former chapters, it is mentioned that most of the modern wireless sensor network systems uses battery not mains. Due to limited battery which is a limited energy source, the data delivery between nodes should be as much efficient as it could be in order to build a better WSN design. Energy consumption can be classified into two major part which are neighborhood discovery and communication vs. computation.

- **Neighborhood Discovery:** Most of the routing protocols uses the information exchange with the neighbors. In order to keep energy consumption low, the local data exchange between neighbors should be minimized without negatively affected the routing system of the network.
- **Communication vs. Computation:** In the case of energy consumption, communicating with other nodes need more energy consumption than the computational work such as MCU processes. That's why, mostly energy consumes by the communicating unit. For instance, decreasing the system traffic, as a result system demands less power which is directly related to the routing.

- **Scalability**

High density of the nodes should support scalability where most of the time data gathering is happens more than the information of the node itself in order to decrease the load so energy consumption.



- **Addressing**

The huge amount of the sensor nodes on the field prevents unique address assignment to all nodes. Although local addressing mechanism can be used to communicate between neighbors, address-based routing protocols are not efficient due to the fact that it is hard to address all large amount of the sensor nodes. In conclusion, there should be routing technique that does not use unique ID for each node.

- **Robustness**

WSNs uses multi-hop mechanism to deliver data to other nodes. So, these nodes at the same time gather physical data from the field, at the same time they do routing jobs which are not similar to the dedicated routers we use for internet. Due to low cost components are used as nodes there is a possibility that sensor nodes can experience unexpected failures. As a result, the routing protocols for WSN should be robust against these kind of failures. Moreover, nodes should not relay on just a single packet which can be gone if anything happens to related sensor node.

- **Topology**

Predetermined and random strategy can be used as the deployment of WSN. Although predetermined topology can have more efficient routing protocols, this not always true for WSNs since individual nodes do not aware of the initial topology of the whole system. Therefore, routing protocols must adapt to dynamic changes of the topology.

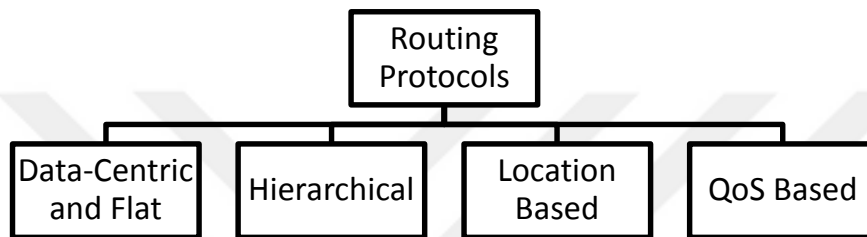
- **Application**

Routing protocols varies from application to application. While monitoring applications use static routes periodically, in the case of event-based applications route generation is made whenever event occurs.

## 2.5.2 Network Routing Protocols

According to Akyildiz et al. routing protocols are divided into four groups such that data-centric and flat architecture, hierarchical, quality of service (QoS) based and location-based routing. See Table-1.

**Table 1- Routing Protocols**



- In data-centric and flat routing protocol applications, users use instead of querying a specific node, querying the attribute to all nodes. Flooding, gossiping, SPIN and directed diffusion are the well-known routing protocol examples for this group.
- Hierarchical routing protocols divide the system into clusters. LEACH, PEGASIS, TEEN, APTEEN and EECR are the mostly used hierarchical routing techniques.
- In the location based routing protocols, neighborhood information is provided by geographically placement of the nodes. MECN, SMECN and PRADA are common examples for location based routing protocols.
- QoS based routing adds extra metrics to energy metric so that the cost and network life time are affected negatively. SAR and Min-Cost-Path algorithms are best examples for QoS based routing protocols.

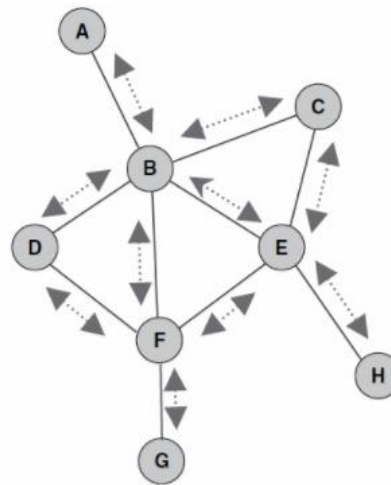
- **Data-Centric and Flat Routing Protocols**

Large number of sensor nodes on the system makes harder to assign specific IDs or addresses to all nodes. Therefore, address based approaches are not preferred in WSNs; instead data-centric approach should be taken into account. Data-centric routing intends to use attribute-based naming instead of node IDs.

Flooding, gossiping, SPIN, directed diffusion uses data centric protocols. For a deeper understanding let's examine some of the examples of data-centric routing.

- **Flooding:**

Flooding is the simplest technique uses data-centric routing approach for multi-hop networks. When a node receives a data packet, it broadcasts this message to its neighbors. This phenomenon continues until all the nodes receives this messages. Flooding can be limited by number of hops or flooding can be finished whenever data arrives the destination node.



**Figure 23-Flooding Scheme**

The main advantage of flooding is its simplicity since no neighborhood knowledge is needed so that no complex routing schemes are required. Although it is a simple approach, flooding has some disadvantages:

- **Implosion:** Considering the architecture of flooding does not prevent multiple broadcast messages receives at the same time from same node, message duplication occurs so that same messages come from neighbors.
- **Overlap:** Closely related sensors can sense same thing at the same time. In other words, duplicated messages can be flooded to neighbors.
- **Resource blindness:** Although, a WSN system should spend its energy carefully, flooding is not a mechanism that care about energy consumption.

- **Gossiping:**

Implosion problem procedure which is the message duplication caused by transmission of multiple broadcast messages, is one of the main disadvantage of flooding. Gossiping, a derivation from flooding, solves this problem by avoiding implosion by selecting a single node instead of all neighbor nodes for relaying the message. In other words, when a packet is received by a node it selects a random node from its neighbor nodes and send the message to that node. After, neighbor node receives the packet it forwards this data to the randomly selected from its neighbors. Although, duplicated message problem is solved by gossiping, latency of delivering message to all nodes increases due to information distribution speed decreases. In addition, preventing multiple copies of messages energy consumption is improved compared to flooding. In the Figure 24 below which explains the gossiping process, node 2 randomly selects node 1 which is the neighbor node of node 2. Then node 1 selects node 4 randomly and packet reaches to the node 3.

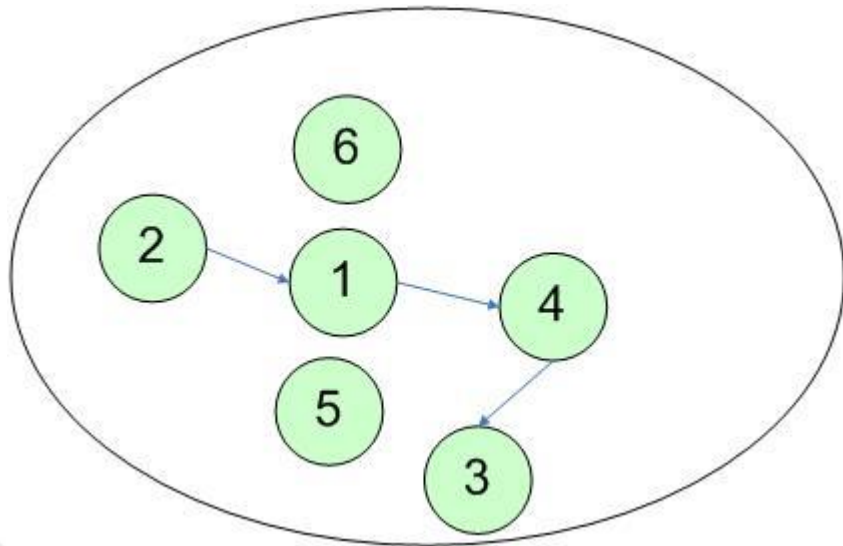
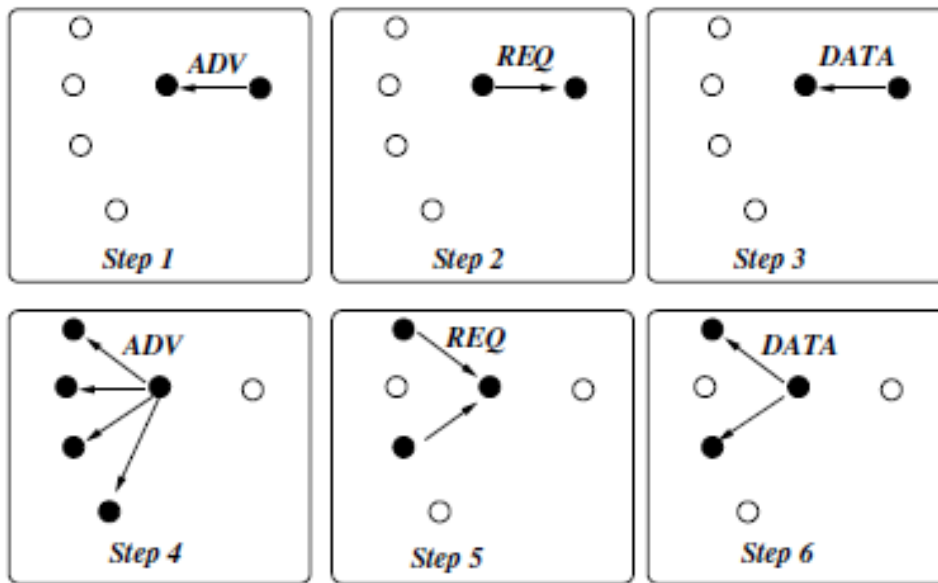


Figure 24-Gossiping

- **Sensor Protocols for Information via Negotiation (SPIN)**

SPIN is created in order to increase the efficiency of flooding by using three types of messages which are described as advertisement (ADV), request (REQ) and data. Following Figure-X explains the operation of SPIN:

- **Step 1:** Before sending the actual data packet, sensor node broadcasts ADV message which contains information of the data packet where the size of ADV packet is smaller than the actual DATA packet.
- **Step 2:** Then, if any node is interested in this ADV message, it sends back to REQ message.
- **Step 3:** Finally, the actual DATA sends to the node which previously sent REQ packet.



**Figure 25-Process of SPIN Routing Protocol**

One of the main disadvantages of using SPIN can be explained in steps 4, 5, 6 of Figure-25 above. In the case of more than one node is interested in broadcasted ADV packet and replies back with REQ messages, DATA packet is sent to these nodes as shown in Step 5 and Step 6. Whenever more than node is requested data packet results in a waste of resources. Moreover, SPIN does not prevent REQ packet collusion if multiple REQ messages are received at the same time.

Using ADV, REQ and DATA packet architecture, SPIN is decreases energy consumption by %70 compared to flooding technique. However, latency is higher than the flooding due to distribution of data consists of three different packets [Akyıldız et al.,2010].

- **Directed Diffusion:**

Although SPIN supports an efficient approach where only interested nodes are requested the data in order to initiate traffic flow from sensors to sink, this type of traffic flow is not always preferred from the users which need specific data from sensor nodes. Directed diffusion is created for this problem to be solved. Four phases, which

are named as interest propagation, gradient setup, reinforcement and data, delivery are created in order to create routes between sensors and sink. [Intanagonwiwat, C. et al,2003]

➤ Interest propagation:

As figure 26(a) demonstrate the process starts with when the sink sends interest packet to all nodes by flooding through the all nodes in the network. Interest messages explores the indication of matching data for a specific task. While task continues, sink node continues to periodic interest messages.

➤ Gradient Setup:

After receiving interest message coming from sink, each node saves this interest cache which can consists of timestamp, interval, duration and gradient. Timestamp indicates the time when interest message is received. Gradient shows the node which sends the interest packet. Moreover, the aim of using the field of gradient is to form reverse path through the sink. In figure 26(b) the node floods back through the sink which in first place sends the interest message. See Reinforcement:

In Figure 26(c) due to unlimited number of gradients, there can be multiple paths from source to sink. This is where reinforcement process deals with which path should be use. The selection of the path can be done in terms of best link quality, latency etc.

➤ Data Delivery:

In figure 26(d) the final phase after selecting source node path between sink and source is defined.

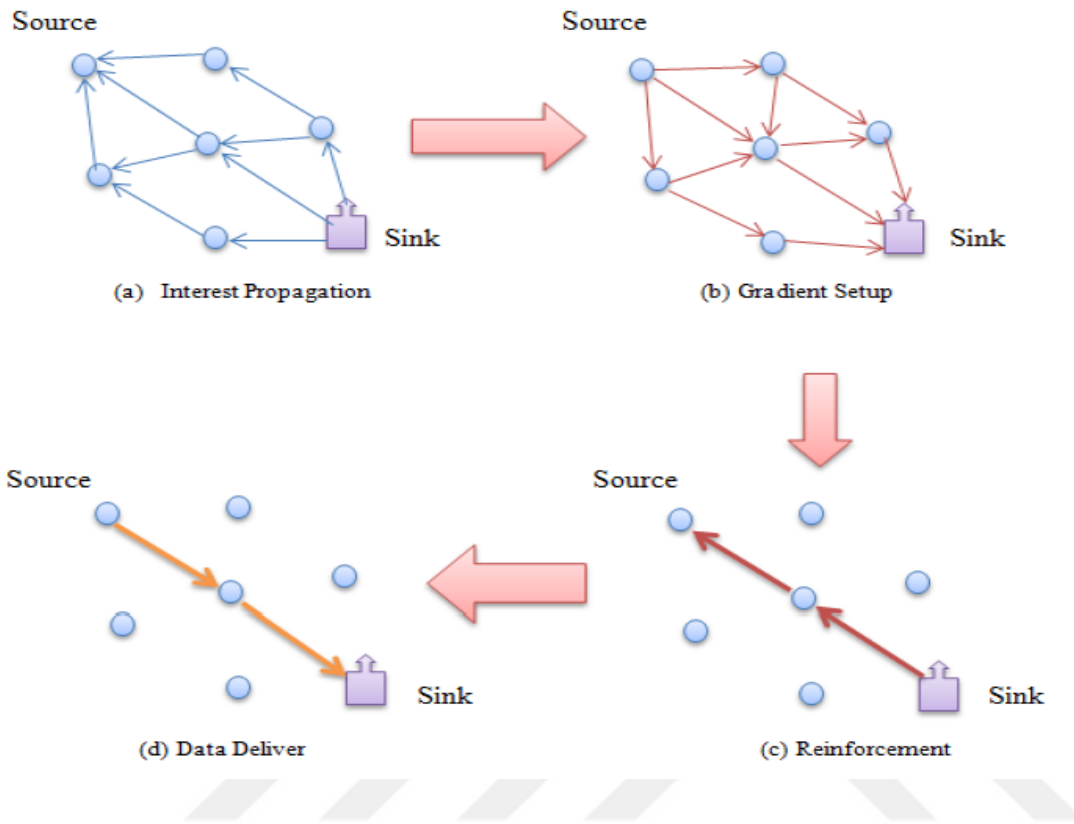


Figure 26-Process of Directed Diffusion



### 3 METHODOLOGY

#### 3.1 Problem Statement

Take into consideration that there are different protocols are created in modern wireless sensor network systems, a mechanism which connects local WSNs to other networks is also needed. Therefore, a gateway mechanism between protocols should be designed.

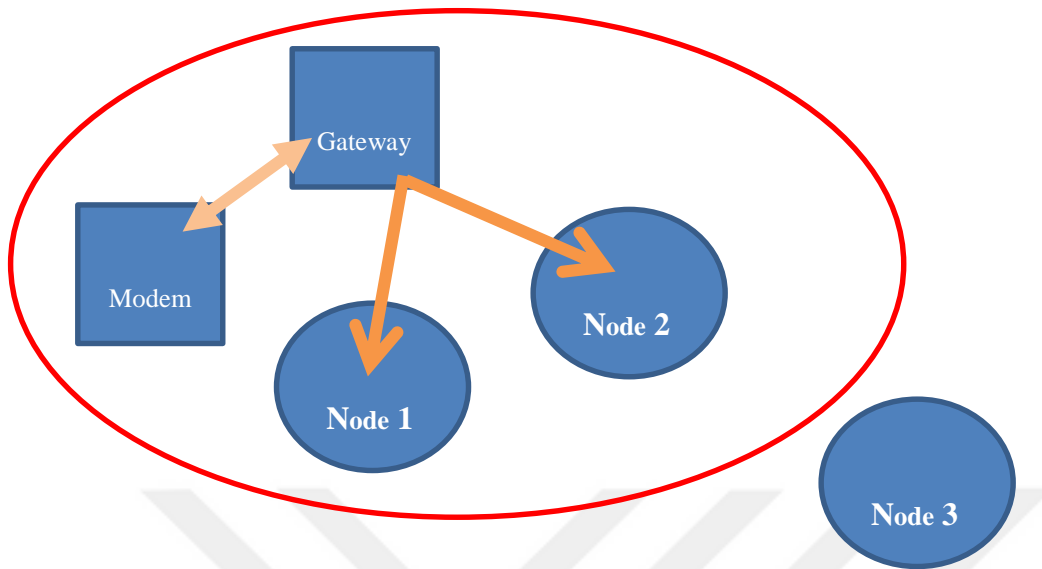
For instance, imagine a WSN system uses Bluetooth protocol in the home environment and there is data gathering PC which do not possesses Bluetooth protocol. In order to read data gathered from sensor network a gateway between Bluetooth and PC should be designed. However, the range of this gateway is limited since it has limited antenna coverage. If a sensor is beyond the range of gateway, gateway cannot convert the data coming from that sensor which results in data loss on the PC side.

To solve this problem gateway should be communicated all sensors by using sensor nodes as router or repeaters if necessary to increase its coverage. In our thesis we focus on the solution of this problem.

Hardware architecture of wireless sensor networks consist of power, sensing, processing and communication units as previously mentioned in Chapter-2.

While sensor node has a local protocol to communicate each other on the field like Node-1, Node2 and Node-3, a gateway node is needed to connect this sensor network through the world. This gateway node is responsible for gathering data from sensor network and convert it the protocol that modem uses. For example, after local sensor network reads temperature data, gateway node collects the data and then send it to the modem so that we can reach these data from our computers, laptops, mobile phones and tablets etc. However, as described in Figure-27 below, gateway node cannot reach Node-3 since it is out of coverage of gateway.

This thesis studies, how to extend the range of gateway node using local sensor network thus, field sensor data is gathered and send it to the outer networks via modem. Gateway node uses local sensor nodes as routers so that make hops until reach destination node.



**Figure 27-Problem Statement**

### 3.2 Methodology

In order to reach nodes that are out of Master's range, following algorithm was developed. In the algorithm, all nodes use same equipment.

Master Node's responsibilities:

- Manage communication between all slaves
- Discovery Table operations
- Take field data from slaves
- Send sensor data to the station
- Configuration via Terminal

Slave Nodes' responsibilities

- Read field data
- Obey master's instructions
- If necessary, run routing operations

The algorithm is made of two important parts called “Discovery” and “Operation”. It is best to understand when these 2 modes use. In Discovery mode, Master node searches for available nodes. After available nodes are found and they are written to Discovery Table, Operation mode which is main mode of the system starts. Following figure shows the state machine of this operation.

In the beginning, Master checks whether its Discovery Table is empty or not. Empty Discovery table means that there are no slaves added to master. If there is no slave node attached, master initiate discovery protocol in order to find nearby nodes. After, discovery process completes, previously found slave nodes are added to discovery table of master node. From now on, master uses this table to reach slaves. In other words, Master tries to communicate with these nodes on the discovery table.

End of Discovery process is followed by starting of Operation mode. In this mode, cyclic operations such as reading sensors, collecting and analysing data are handled. Apart from Communication errors or addition of a new node; Operation mode is the main mode of the system. For example, when master cannot reach a node on the table for several times, it tries to reach it by updating discovery table via discovery protocol.

In order to reach nodes that out of Master’s range, following algorithm was developed. In the algorithm, all nodes use same equipment.

Master Node’s responsibilities:

- Manage communication between all slaves
- Discovery Table operations
- Take field data from slaves
- Send sensor data to the station
- Configuration via Terminal

Slave Nodes’ responsibilities

- Read field data
- Obey master's instructions
- If necessary, run routing operations

The algorithm is made of two important parts called “Discovery” and “Operation”. It is best to understand when these 2 modes use. In Discovery mode, Master node searches for available nodes. After available nodes are found and they are written to Discovery Table, Operation mode which is main mode of the system starts. Following figure shows the state machine of this operation.

In the beginning, Master checks whether its Discovery Table is empty or not. Empty Discovery table means that there are no slaves added to master. If there is no slave node attached, master initiate discovery protocol in order to find nearby nodes. After, discovery process completes, previously found slave nodes are added to discovery table of master node. From now on, master uses this table to reach slaves. In other words, Master tries to communicate with these nodes on the discovery table.

End of Discovery process is followed by starting of Operation mode. In this mode, cyclic operations such as reading sensors, collecting and analysing data are handled. Apart from Communication errors or addition of a new node; Operation mode is the main mode of the system. For example, when master cannot reach a node on the table for several times, it tries to reach it by updating discovery table via discovery protocol.

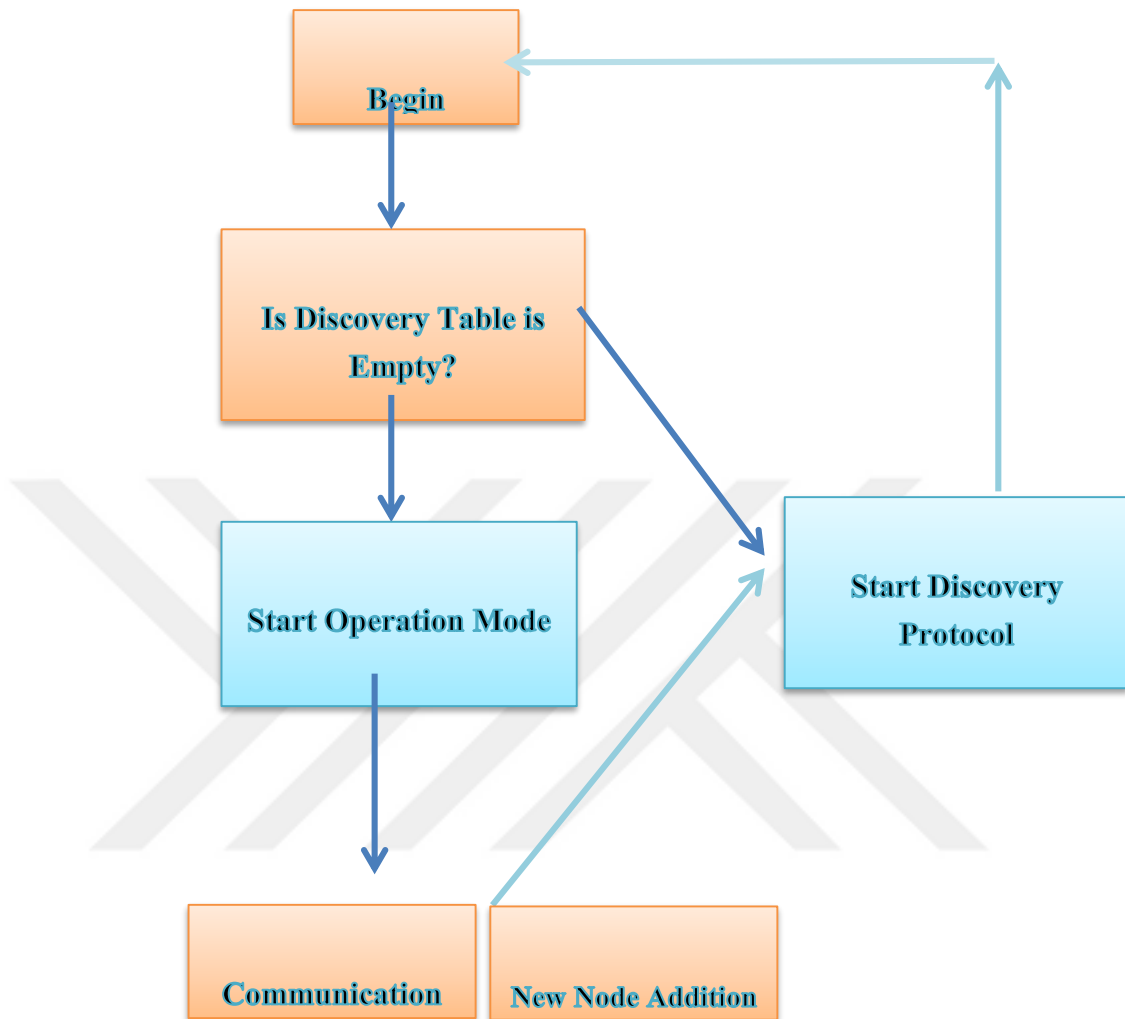
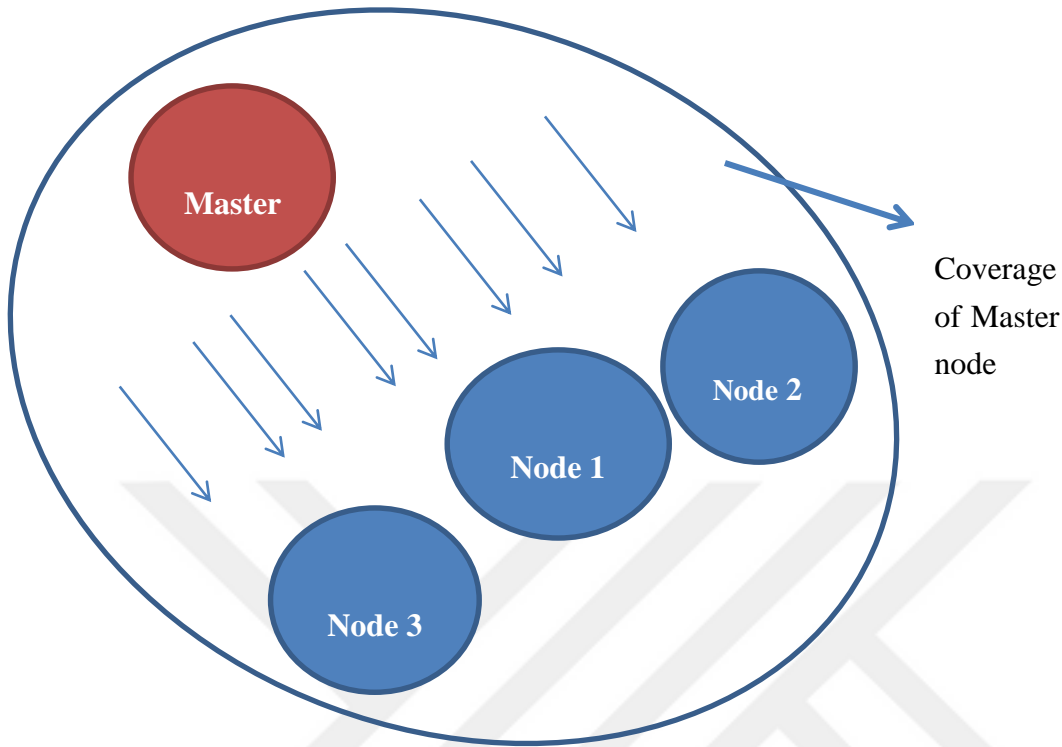


Figure 28- State Machine of DCP and Operation

### 3.2.1 Discovery & Configure Procedure (DCP)

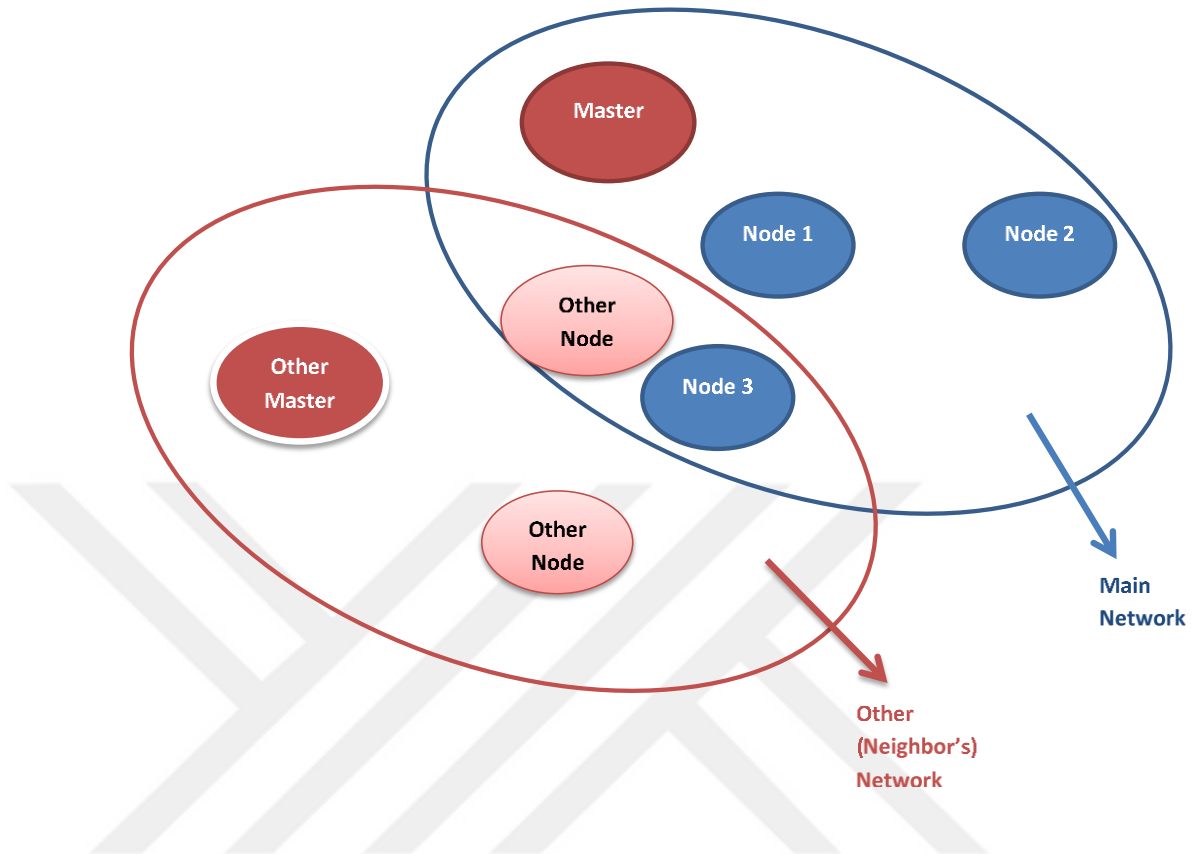
In our methodology, WSN system uses DCP in order to find nearby and available nodes. As mentioned before, if there is no data on Discovery Table of Master Node, Master starts DCP protocol to fill this table.



**Figure 29-Coverage of Master Node**

At the beginning Master sends a broadcast signal to its coverage area. If there are nearby and available nodes in the Master's coverage area, these nodes are answer that they can attach to network of Master. Moreover, while these nodes are answering they also say that they are using routing capabilities or not. This routing topic will be covered later

Moreover, considering one of the most important challenges is the security issues, in order to eliminate this complication, every node uses a unique address and password. Address info is used as the name of the nodes whereas password info is used to distinguish which nodes are attached to which master's network. For example, considering these systems are applied to home environment, the neighbour's network and main network can be crossed. In other words, main network can read neighbour's temperature sensor mistakenly. Due to the fact that networks can be intersected, to prevent this situation every node has a password which shows them to their master node. As a result, close networks are separated and risk of interference is minimized.



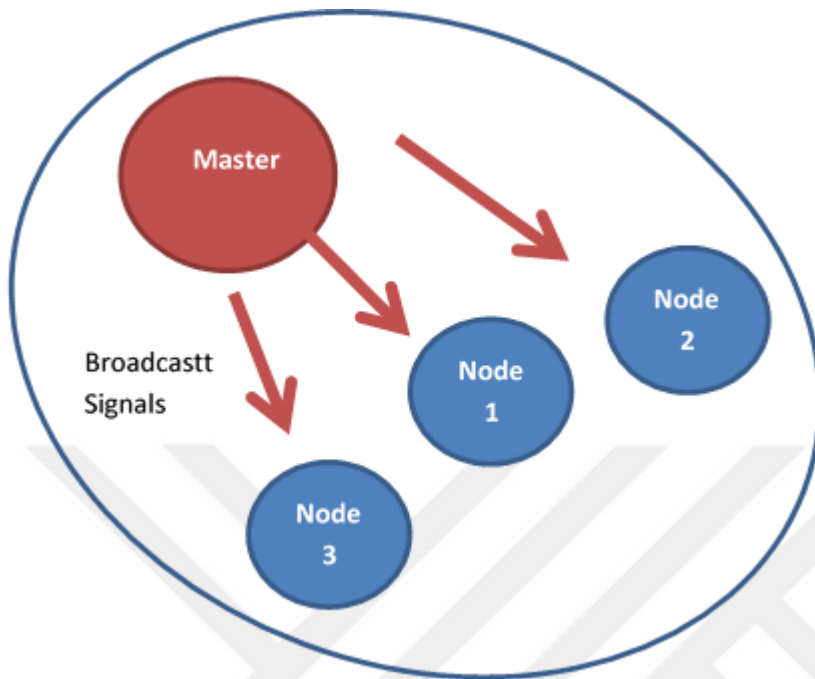
**Figure 30- Separation of different Networks**

So far it is mentioned that Master sends a broadcast signal and as answers comes from available nodes, Master fills its Discovery Table. Now, it is time to go to details of this operation.

- **Detailed Operation of DCP**

Like the test setup, 3 nodes are used. Moreover, the information can be found about filling the Discovery Table is shown below

1. Master Node sends a broadcast signal called DCP to its coverage area and waits for answers from the other nodes.



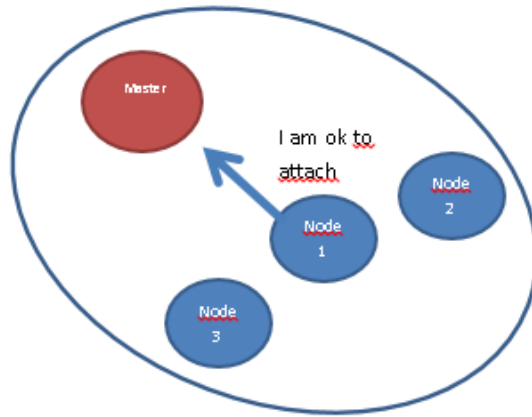
**Figure 31-DCP- Step1: Broadcasting**

**Table 2-DCP Table status**

Discovery Table
NULL
NULL
NULL
NULL

2. Master waits for answers from other nodes. When an answer comes from slaves it writes this data to Discovery Table which shows the attached nodes. Master node has a hardware solution for the messages that comes at the same time. Moreover, after sending broadcast message Master waits for other devices to respond its DCP call. As soon as answer comes, Master writes info to Discovery table with its interrupt driven RX message parser algorithm.

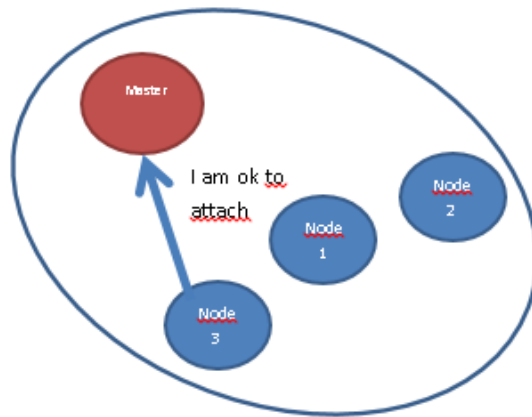




Discovery Table
<b>Node 1</b>



Discovery Table
Node 1
<b>Node 2</b>



Discovery Table
Node 1
Node 2
<b>Node 3</b>

Figure 32- DCP Step 2

3. Now Master is gathered info of nearby nodes. However, what if there is a node which is placed apart from Master's range? In order to range extension this system can use its slaves as a router if necessary. In this step, Master checks its Discovery Table that which addresses of slaves are recorded. Now, Master orders from its slaves, that addresses are found in DCP Table, to run DCP algorithm one by one. In addition, Master wants their slaves to create their own DCP Tables. What is more, slaves send back to their DCP Tables to the Master one by one. Master compares its DCP table and tables coming from slaves. If there is a different address that cannot be found on DCP Table of Master node, Master adds this address to its DCP table. In other words, if there is an extra address that found by slave, it means that there is a node that master cannot reach while a slave can reach. From now on Master try to reach this node that is out of its range by using this slave node. In this case the slave which finds an extra node that is out of Master's reach will be used as a router to connect this extra node to Master. Therefore, Master can cover more slaves even the slave is out of its coverage area. In this case, because of the fact that to cover the same area Master should use more antenna power, energy consumption due to antenna power of master would be decreased while Master's range is extended. The following sections show that how this range extension mechanism works.

- i. Master orders the nodes on its DCP table to initiate DCP and send the results to the master. In this case, Master sends "Start\_DCP" messages to "Node-1", "Node-2" and "Node-3". If one of these nodes sends a different node address, Master adds this node to its DCP table. The node that sends the different address one of the addresses not found on Master's DCP table will be defined a router node.
- ii. First, Node-2 sends DCP message to nearby units and send its DCP table results to Master.

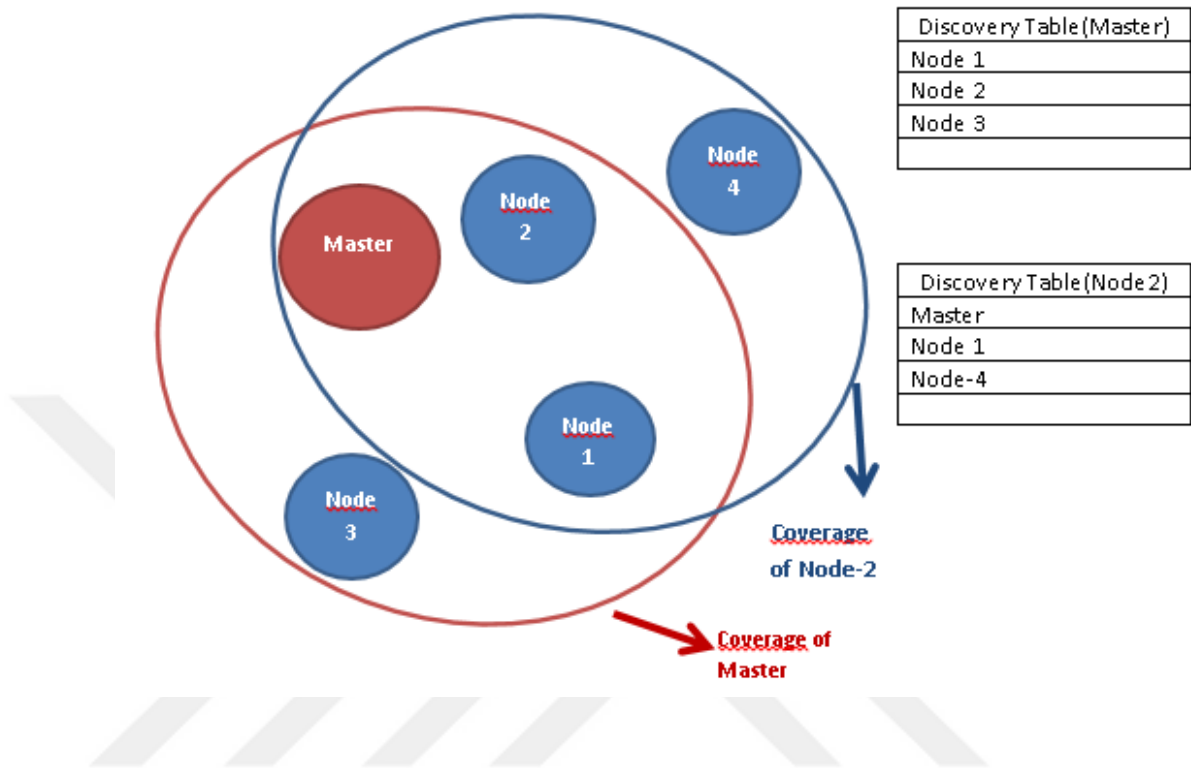


Figure 33- Node-2 sends DCP table

- iii. Master compares its DCP table and Node-2's table. In this case "Node-4" is the extra one.

Table 3-DCP Status Tables

Discovery Table(Master)
Node 1
Node 2
Node 3

Discovery Table(Node2)
Master
Node 1
<b>Node-4</b>

- iv. Master should add "Node-4" into its DCP table.

- v. Master add a node that beyond its range. From now on, Master will reach this node via Node-2 and vice versa. In radio message frame master, change Node-4's "Directory Address" as same as Node-2's.
- vi. Secondly, Node-1 starts DCP operations

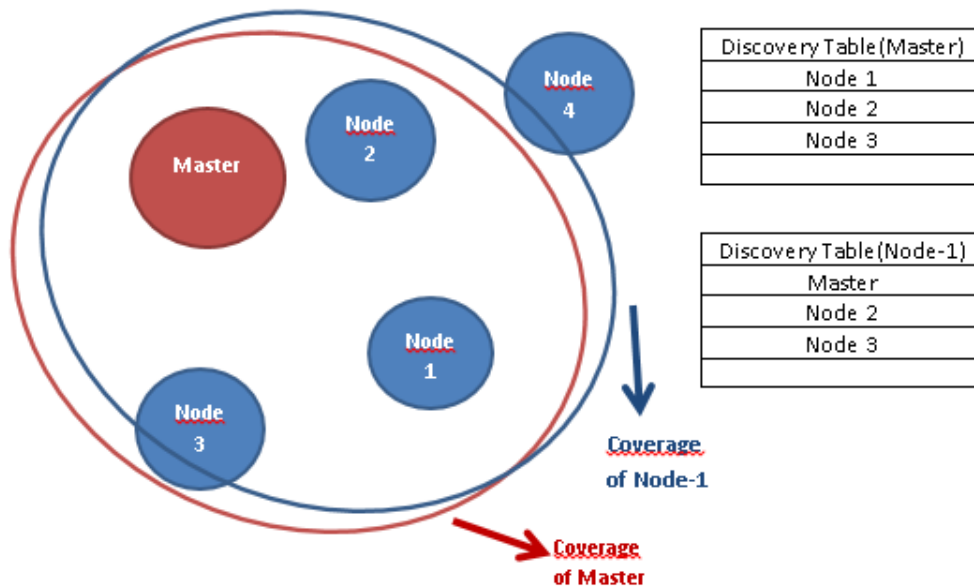


Figure 34- Node-1 starts DCP sequence

- vii. Master compares the DCP table coming from Node-1 and its own. As a result, there is no difference. It means there is no extra node which is beyond Master's reach.
- viii. Finally, Node-3 starts its DCP operations.
- ix. Finally, Master compares the DCP table results coming from Node-3 and its own. As it can be seen, there is no difference

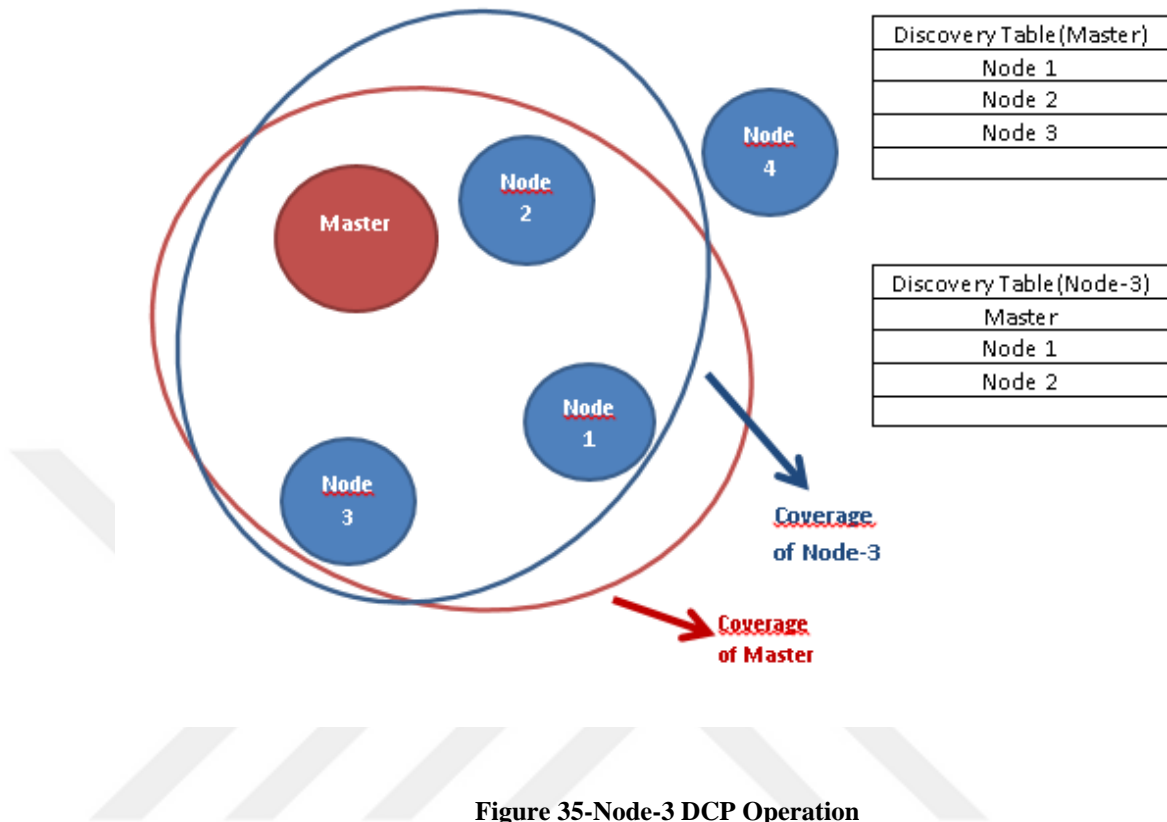


Figure 35-Node-3 DCP Operation

### 3.2.2 System Architecture

- **Software Layers**

System uses nodes as sensor points or router or both. That's why software is designed as layered architecture. Although lower layers can vary with different architectures of MCUs, upper layer designed to operate in most of the system. This kind of architecture enables users to create new systems faster since only upper layer should be ported to related MCU system.

In the bottom line, drivers of MCU are programmed such as clocks, timers, GPIO, interrupts, UART and SPI. In this layer, driver of MCU are programmed. This block is also called HAL (Hardware Abstraction Layer). This layer changes with different MCU architectures. For example, since the registers of ARM Cortex M0+ MCUs and

Texas Instruments MSP series MCUs, they need different codes. In other words, this layer changes via architecture of MCUs.

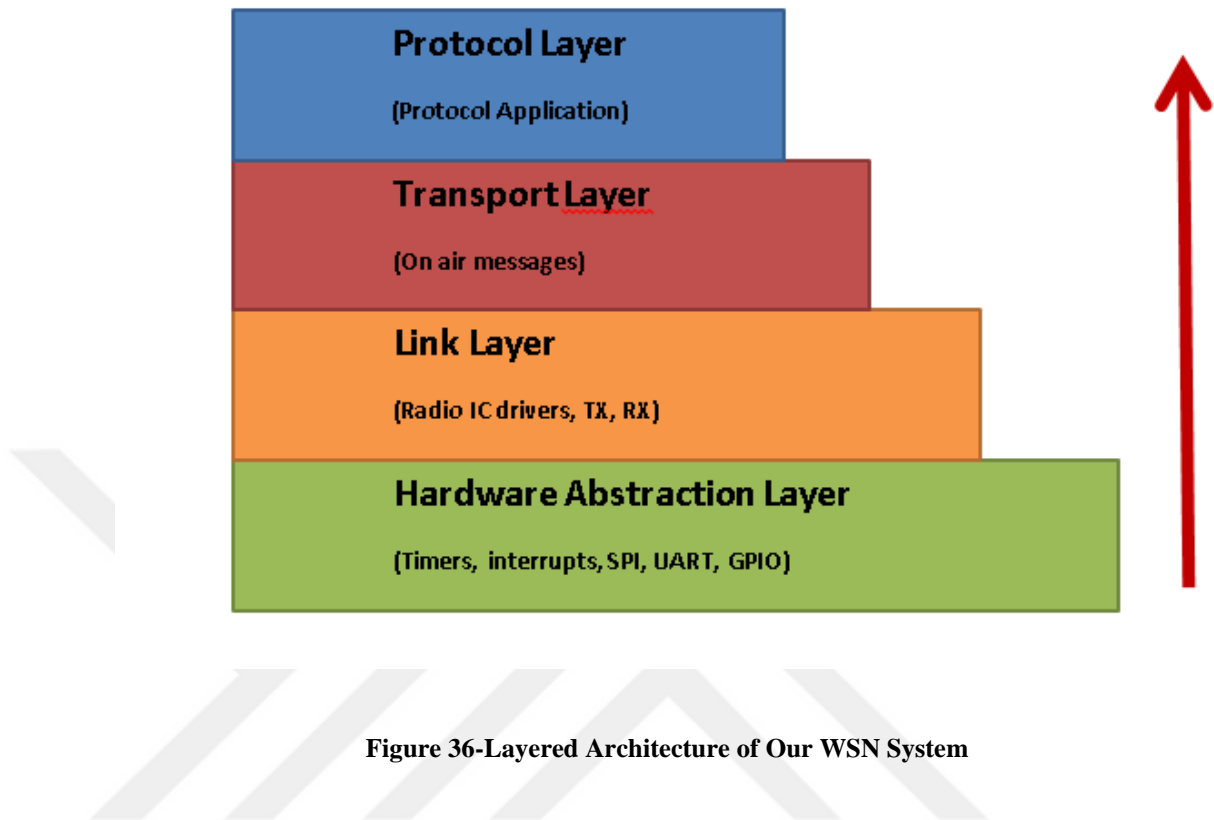
One layer above Link layer which is the driver of radio unit coded via SPI communication is placed. In this layer, radio's main functions are controlled via SPI. RX and TX transmissions, all options of radio are configured and controlled in this part. Link Layer also changes with different RF-IC brands.

So far, it can be inferred that different systems have different codes for link layer and Hardware Abstraction Layer. In order to implement this protocol created for our thesis, the upper layers is designed to be same for other systems.

Transport Layer, where Message frame structure is created, is layered above the Link Layer. In this layer, the message on the air between nodes is programmed. This driver is responsible for creating message structure. The message structure which is created in here is sent to other node via Link Layer. When data comes from link layer, data parsed and sent to upper level.

The top layer is the protocol layer which is responsible for applying our algorithm into this system. In this layer, receiving messages are parsed here. Moreover, parsed messages are processed here. Furthermore, necessary answer messages are created in this layer.

The summary of the layered architecture is explained below in Figure 36.



So far it is mentioned that the layer organization consists of 4 layers. However, in order to understand the structure in a more detailed way, the communication of two nodes should be observed. The following table explains the communication between two nodes. The messages which travels on the system are indicated in the Figure-37.

1. Protocol layer fills message frame tables according to algorithm. The command, data and status info is put into the protocol frame.
2. Message frame is created for on air communications
3. Link layer transmits the created frame (TX)
4. Message is on the air
5. RX message is received by RX Link Layer.
6. Message frame is parsed so that protocol data can be reached.
7. Protocol layer parses this message and make necessary operations on RX side

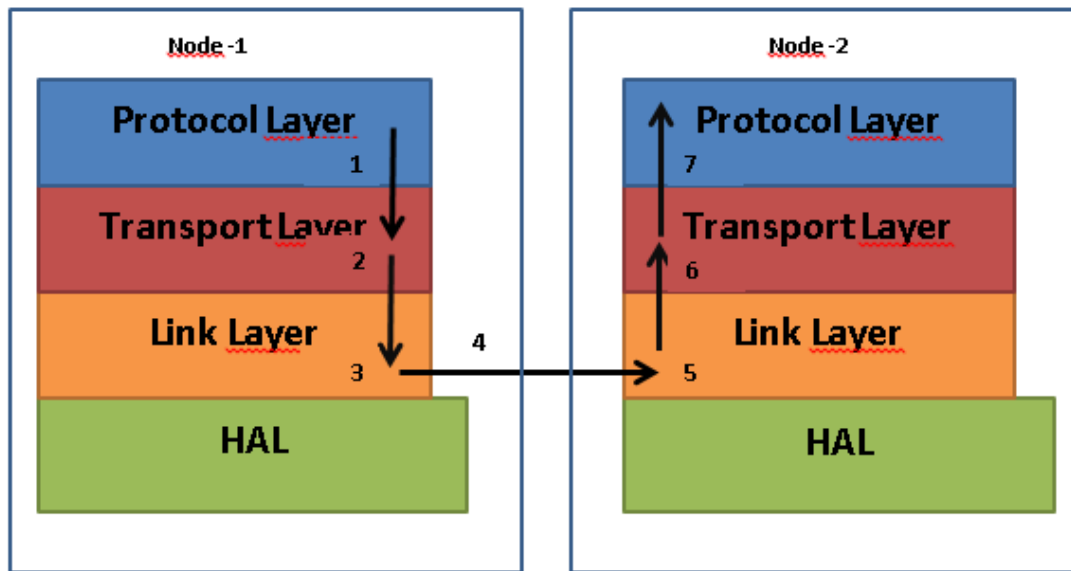


Figure 37-Layered Architecture of Messages between two nodes

- **Radio Message Frame Structure**

Before explaining about how routing operations are handled, it is best to talk about the radio message frame structure which carries messages from Master to slaves or slave to slave. This structure, handles the lower level communication.

As previously mentioned, MCU and Radio IC communicates via Serial Peripheral Interface (SPI) which is serial communication protocol. Moreover, in this configuration MCU is configured as SPI Master and Radio IC is defined as SPI Slave. Lower level components of MCU, handles SPI communication. However, in order to increase systems reusability, reliability and quality, SPI communication is also designed as layered topology.

In the bottom line, driver of SPI, interface between MCU and SPI peripheral of MCU, is placed. In this layer MCU is programmed to enable and initialize SPI peripheral. In the upper layers, raw SPI message is turned into a frame for



communication. Since SPI blocks of different MCU's are not same in terms of architecture and codes, layered architecture is important. Because, in this topology, protocol layer is planned to be applied to any MCU.

MCU commands, adjust and create frames which are used for nodes to communicate each other on air. MCU sends its frames via SPI to RCU (Radio Control Unit) Then Radio Control Unit sends these frames to other nodes. In addition, MCU reads temperature sensor placed on RF-IC. This is the sensor information used in this study.

To sum up, SPI serial communication is used for data transfer between MCU and RCU in the lowest level of the layer. After SPI communication between RCU and MCU establishes, the frames are created for radio. In other words, RCU sends radio frames which are coming from MCU to other nodes so that data delivery between sensor nodes are started. Although SPI coding and architecture varies using different MCU architectures, radio frames transmitted from RCU is one of the main focus of this thesis and these frames are independent from MCU and RF-IC.

Radio communication frames should be kept as low as possible to decrease energy consumption where battery power is limited. Because big frames need more transmitter power. Frame sizes should be decided by considering how many node count needed by the system. That's why this parameter, frame size, parametrically designed. The detailed information about components of the frame are explained below. However, it should be kept in mind that frame sizes can be selected according to size and architecture of the system.

### **1. Transport Layer Frames:**

Transport Layer carries actual data sent by other nodes. When a node receives transport frame, it parses the protocol data and send it through the protocol layer.

**Table 4-Transport Layer Frame**

Source Address	Destination Address	Direction	Frame Type	Hop Count	Frame ID	Protocol Data	CRC
----------------	---------------------	-----------	------------	-----------	----------	---------------	-----

- **Source Address:** Defines the address of the sender node. During transmission of the message frame on the network, source address indicates where actual data is coming from.
- **Destination Address:** This address shows the target node which packet is sent to.
- **Direction:** This parameter is also an address definition of the router or repeater node. When a routing is needed in order to reach data destination, the router address is written on Direction parameter of the frame. Sensor node has a routing table and direction parameter varies with destination node address.
- **Frame Type:** Frame type uses for the type definition of the frame.
  - **0x00** → Message
  - **0x01** → Start DCP: Starts DCP sequence
  - **0x02** → DCP Attach: when this message comes from neighbour node, this node is added to DCP table
- **Hop Count:** When routing capabilities of the sensor node should be used to reach destination node, data frame hops between nodes till final destination. Hop count is important since when routing table of the node prepares hop count is an indicator.
- **Frame ID:** This parameter indicates the identification number of the frame. In Discovery and Configuration state which will be explained later in this chapter. When radio message frames travel around the network there is a possibility that same messages can be received and processed. Receiver node solves this problem, which also called impulsion problem talked about in previous chapter, by looking at Frame ID.

- **Protocol Data:** Transport layer frames carry protocol data between nodes. The ingredients of protocol data are explained below in protocol frame structure.
- **CRC:** CRC, cyclic redundancy check, detects the frame whether all bits are received properly. If a data loss occurs, CRC alarm is created. When a CRC Alarm occurs, it means there is a loss of data on the air.

## 2. Protocol Layer Frames:

Protocol frames keeps main data of the sensor node. The data includes sensor readings, sensor node status. Protocol Layer data carried on transport layer messages as Protocol Data.

**Table 5- Protocol Layer Frame**

<b>Address</b>	<b>Password</b>	<b>Command</b>	<b>RSSI</b>	<b>WakeUpTime</b>	<b>Temperature</b>	<b>Alarm</b>
----------------	-----------------	----------------	-------------	-------------------	--------------------	--------------

- **Address:** Every node has an address for communication. This address is some kind of name of the node in the sensor network. Master and slaves are using addresses to reach each other. When a node wants to send a signal to another node, it puts the address info of the target. In the receiving a signal scenario, nodes are waited to frames that starts with their address. If the address matches, MCU parses the other parts of the message and takes action.
- **Password:** In today's world radio waves surrounded us. In the light of these mesh networks, in the future there are lots of networks in the same coverage area but connected to the different masters. For example, we can mistakenly add our neighbours' node into our node. When a node is connected to a master, a password is given by the master in order not to mix this node with the nodes in other networks such as neighbour networks.
- **Command:** When a node wants another node to do something, fills necessary commands to this area. If this part of the frame is 0 it means do nothing. For

instance, when a master needs the result of temperature fills this part of the frame. The information about the detailed command list is explained below:

- **0x00** → Do nothing
- **0x01** → Set Red Led
- **0x02** → Set Green Led
- **0x03** → Set Yellow Led
- **0x04** → Turn off the Leds
- **0x05** → Start Temperature Reading Routine: *Master commands slave to read its temperature sensor and sends back the result of the operation to the master.*
- **0x06** → ACK: *In some protocols, important messages should be acknowledged such as routing is necessary.*
- **RSSI:** Received Signal Strength Indication is used to measure the incoming signal power. If RSSI value is below threshold, slave wants master to make DCP actions again.
- **WakeUpTime:** For cyclic events this feature can be used. Some sensors such as temperature sensors do not need to be read in high frequency. Because temperature at home does not change very often. Master assigns this feature to the nodes. For example, master wants slave to read and send the temperature value in 10 minutes of time.
- **Temperature:** The measurement of the temperature value is sent in the frame by slave after master commands and starts reading temperature routine. After sending the result to the master, this area is written to “0”. If there is “0” in this register, either temperature value is just send or reading temperature is in progress.
- **Alarm:** normally it is “0”. If an alarm occurs this flag will be changed. For example, when the battery of the node is needed to be changed, slave sends this frame to the master. Details are explained below:
  - **0x00**→ No Alarm
  - **0x01**→ LOW\_BATTERY

- **0x02**→ LOW\_RSSI: *If this alarm flag is set, this node is prevented from using as a router.*
- **0x03**→ COMMUNICATION\_ERROR
- **0x04**→ CRC\_FAIL: *If this alarm flag is set, last message should be sent again*
- **0x05**→ SENSOR\_MOVED: This alarm flag is used to warn master that current sensor node is moved to another location.

### 3.3 Protocol Message Sequences

Figure-38 and Figure-39 show the message sequences during DCP operation and normal operation. In Chapter 3.1 it is mentioned that our system has two modes called DCP mode and normal operation. During DCP operation master node tries to reach every possible node around. Furthermore, in normal operation sensor nodes read the temperature data and send them to the master node so that master node can transmit data to PC.

In Figure-38 and Figure-39, it is assumed node-1 is in the coverage area of master node while node-2 is outside of this box. In Figure-38, using DCP sequence, master discovers node-2 and in Figure-39, master reads sensor data coming from node-1 and node-2.

In Figure-38, master node first checks whether it's "DCP\_TABLE" is empty or not. If it is empty, "DCP\_BROADCAST" signal is broadcasted to the nodes which are placed in the coverage area of the master. As previously mentioned, it is assumed that node-1 is in the coverage area. Node-1 answers with a "DCP\_ATTACH" message so that master adds node-1 into its "DCP\_TABLE". Then as protocol orders, master try to learn the neighbor nodes of the nodes recorded into "DCP\_TABLE" one by one. In this case master sends "DCP\_START" message to node-1 and by receiving this message node-1 broadcasts "DCP\_BROADCAST" signal in order to learn its neighbor nodes. Then node-1 finds node-2 by receiving "DCP\_ATTACH" message coming from node-2. After this message node-1 adds node-2 into its "DCP\_TABLE" and share

its table with master. Master compares the tables of its own and table coming from node-1 and discovers node-2. Finally, master ends DCP sequence so that normal operation can start.

In Figure-39, normal operation starts with all the nodes with a special sleep mode called “RX\_SNIFF\_MODE”. In this mode radio unit sleeps and listens whether a signal comes or not with a low energy. The “WakeUpTime” parameter determine the amount of time of “RX\_SNIFF\_MODE”. Master controls this parameter. For example, master use this parameter to tell slave node “sleep 5 minutes and then wake up and send me the data”. After “WakeUpTime” timer expires, slave node gets its temperature sensor value and sends it to the master. When master reads all the data coming from the field, this gathered data send to PC via serial terminal so that temperature sensors are monitored.

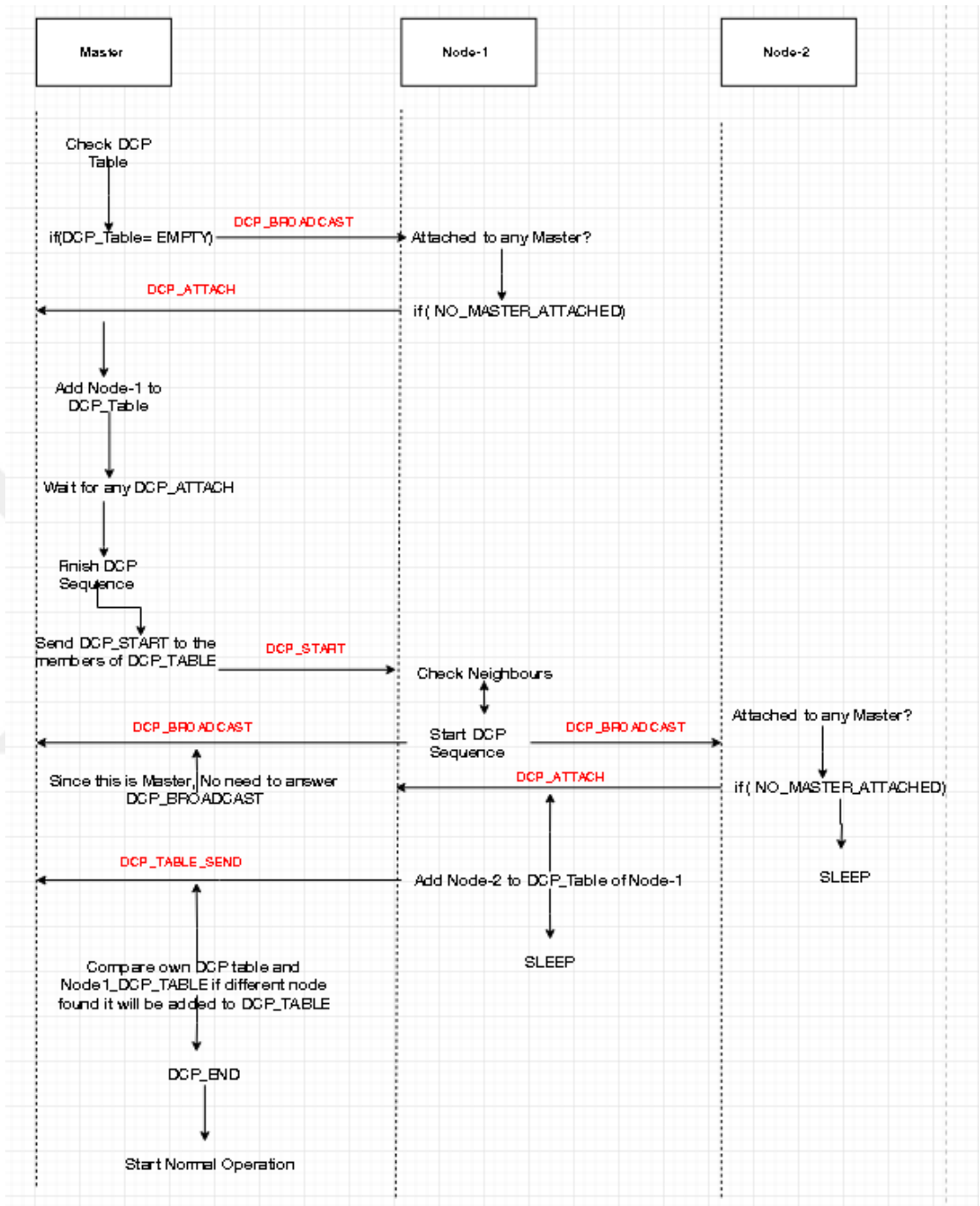


Figure 38- DCP Protocol Message Sequences

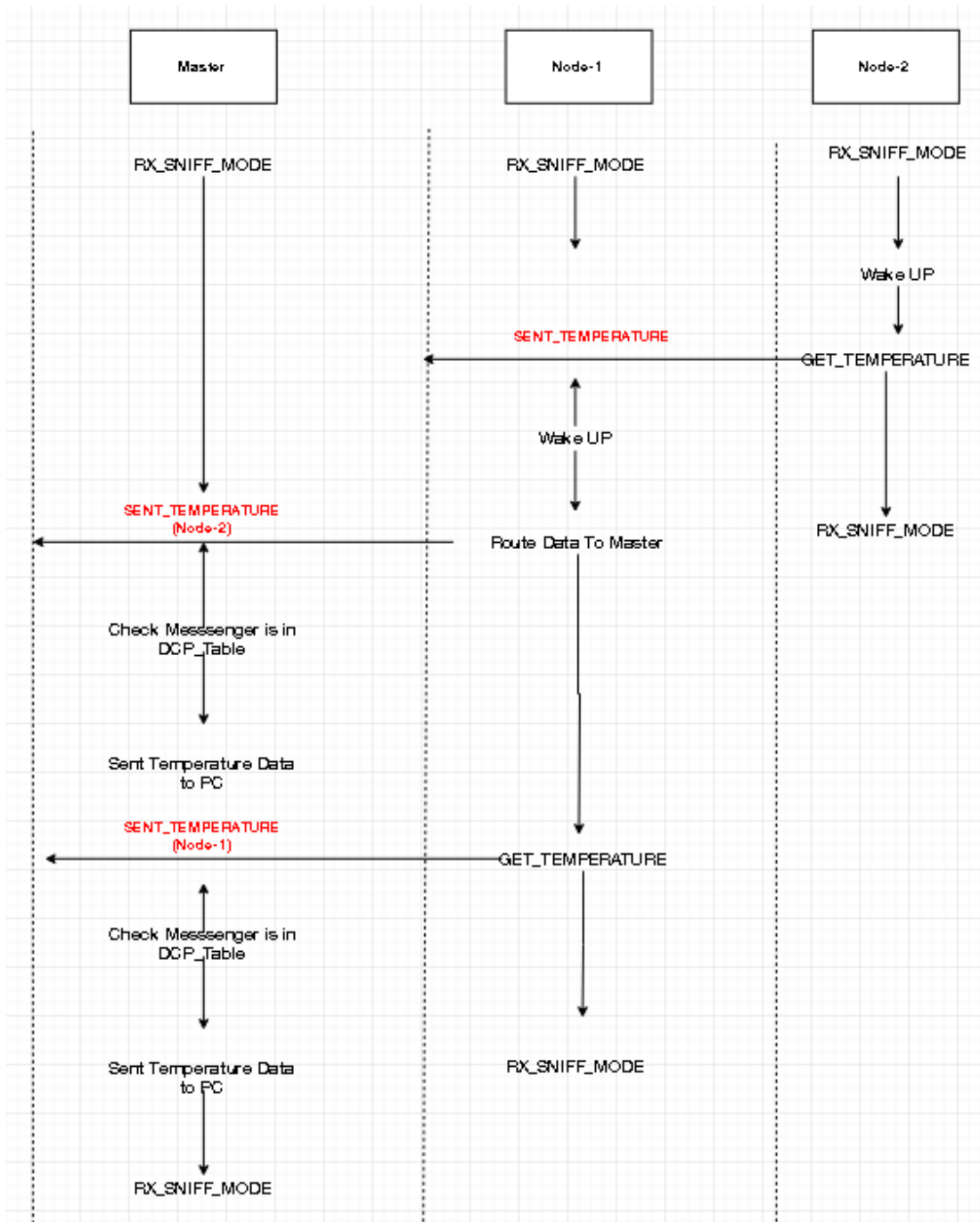


Figure 39- DCP Normal Operation Message Sequences



### 3.4 Special Cases

In the light of having a reliable system, there should be additional algorithms, since there are some cases should be considered. In the case of our protocol, the following situations considered as special cases:

- When the battery of a node is about to fail?
- When a node cannot be reached and communicated?
- What happens if a node moved to another direction?

#### 3.4.1 Special Case 1: Battery about to die

Battery power is measured on certain intervals so that if the power of the battery is close to critical level, other nodes could be notified. As a result, after battery failure, other nodes can understand why they cannot reach the failed node and they don't send any data to that node

. If other nodes try to reach this failed node, they cannot communicate with this node. In other words, when a node fails, other nodes tries to reach that node which results in waste of battery. In order to prevent this situation, when battery power is on the critical level, master node should be notified.

The algorithm for notifying the master node is to send the alarm message called "LOW\_BATTERY". When this message reaches to the master, master node should initiate "DCP\_START" process.

When low battery message comes, master node could delete this failed node from its DCP table. By doing so, the communication flow through this failed node could be prevented. However, if this node is a router node, after deleting this node on the system, some other nodes also could not be reached. That is why when a node fails, master should start DCP process from the start.

#### 3.4.2 Special Case 2: Unreachable Node

It could be happened that sometimes master cannot communicate with a node in some reason. If the "LOW\_BATTERY" message is not received by master and a node

cannot be reached 3 cycle times, this means that there is a communication error on this node.

When master detects there is an unreachable node, the user side is notified with a “COMMUNICATION \_ERROR” message. When master receives this message master starts DCP process from the beginning since this failed node could be a router node.

### **3.4.3 Special Case 3: Changing place of the node**

When a node moved from one location to another, the routing tables could also be changed. In order to protect efficient routing created by DCP, place altering should be detected.

An accelerometer sensor could be used in order to detect whether a device is moved or not. A critical level of moving should be decided considering the nature of the sensor. For example, if the sensor is responsible for window security, by opening or closing the window there is a standard movement. However, if someone moved the sensor from the window it could be detected. After reaching the critical movement level, sensor node should create a “SENSOR\_MOVED” alarm. When master gets this alarm, it sends PC that related sensor is moved to another location. Moving this sensor to another location, also cause to chance the routings. Therefore, if this case is happened, master initiates the DCP sequence.

## **3.5 Implementation of Protocol**

In this thesis study, apart from theoretical studies, there are also practical work. In order to test and validate the protocol, first it has to be implemented on a real hardware. In this section, implementation of the protocol over the hardware is explained.

In this section, selected hardware and the software implementation is concerned.

### 3.5.1 Hardware Studies

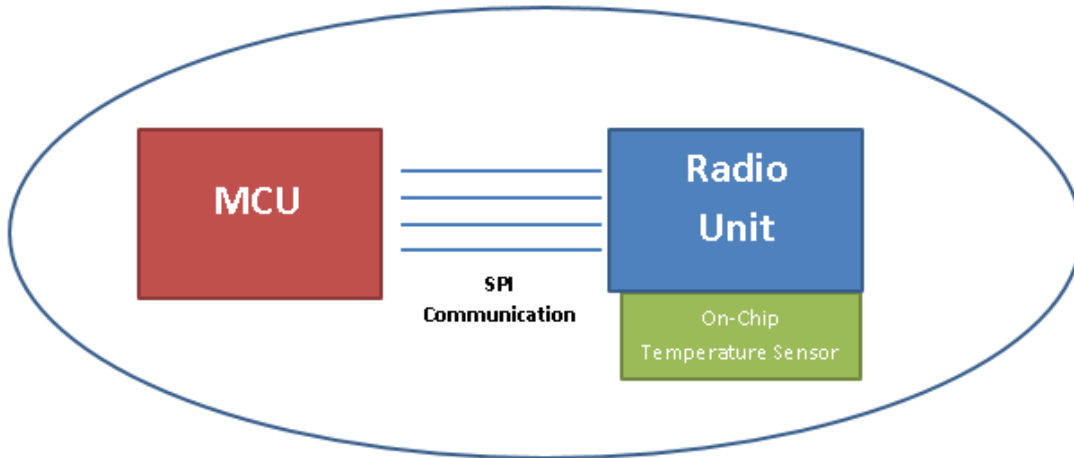
#### 3.5.1.1 Test Node Structure

As previously mentioned on Chapter 2, WSN system consists of MCU, RF unit, sensor unit and power unit. In our system, a node is consisting of a microcontroller and a radio unit. Microcontroller (MCU) uses this radio module to transmit and receive data from one node to another. In other words, MCU is the brain of the node and by speaking via radio module.

In addition, MCU and radio unit uses “Serial Peripheral Interface (SPI) for communicating between each other. In this structure, microcontroller is the SPI master while radio unit is an SPI slave.

Radio unit has an on-chip temperature sensor which is used as sensing unit. Moreover, MCU reads temperature values from Radio unit via SPI communication.

Test and validation hardware consist of NXP FRDM KL25Z and Texas Instruments TI CC1120 daughter kit. While KL25 family development kit is used as MCU, TI-CC1120 is used for both RF unit and temperature sensor. MCU communicates with RF Unit through SPI in order to send and receive RF messages. Furthermore, on chip temperature sensor on the RF kit is used for sensing unit simulation. Moreover, on chip accelerator on the FRDM-KL25z board is used for movement detection of the node.



**Figure 40- WSN Test Node**

### 3.5.1.2 MCU Kit

In the selection phase of MCU, it was logical to select a development kit, since this thesis is about the protocol rather than hardware design. Moreover, a tested hardware is better for software design. Otherwise, fault detection becomes more difficult.

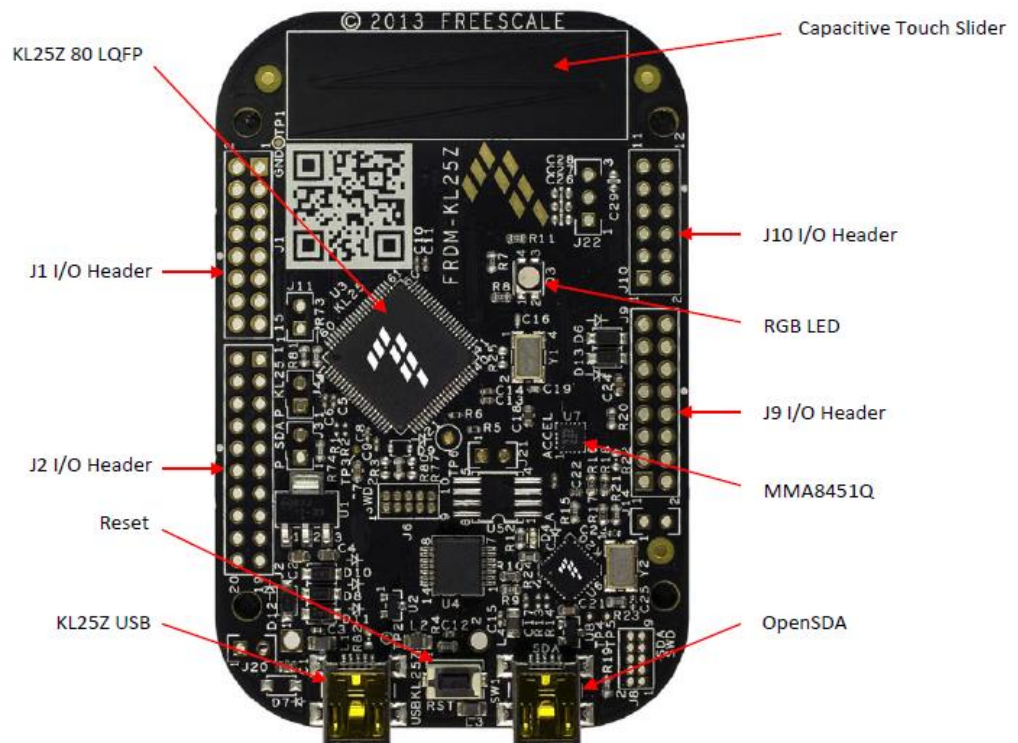
Before selecting the kit, the architecture of the MCU should be decided. Considering cost, performance and low power consumption, a MCU with ARM Cortex-M architecture is selected. ARM Cortex-M has “M7”, “M33”, “M4”, “M3”, “M23”, “M0” and “M0+” architectures according to ARM company. These models categorized into 3 sections which are “highest performance”, “performance efficiency” and “lowest power and area”. The following table shows the categorization of ARM Cortex-M architectures.

**Table 6- ARM Cortex-M Architectures**

Lowest Power	Performance Efficiency	Highest Performance
M23	M33	M7
M0	M4	
<b>M0+</b>	M3	

Over these architectures M0+ is selected among the other architectures due to its performance and low power consumption characteristics. FRDM-KL25z which has ARM CORTEX M0+ architecture is selected as the development kit.

As seen in Figure-41, FRDM-KL25Z kit has enough I/O's with serial peripherals, LEDs, accelerometer and USB connection. Moreover, this kit has power outputs which can be used to feed the RF unit. Moreover, USB port can be used for programming and debugging which prevents making a debug circuit.



**Figure 41- FRDM-KL25Z Kit**

### 3.5.1.3 RF Development Kit

Texas Instruments CC1120 daughter board is used as RF unit. This development kit has also an on-chip temperature sensor.

For licence issues on RF spectrum, working frequency of the device should be in ISM band. This board uses as 868 MHz frequency for communication. Moreover, input power range of CC1120 is suitable for output of FRDM-KL25z board. It can be controlled over SPI communication. One of the mains reason why this IC is selected is that CC1120 has a mode called “RX sniff mode” which is a function with low RX power algorithms.

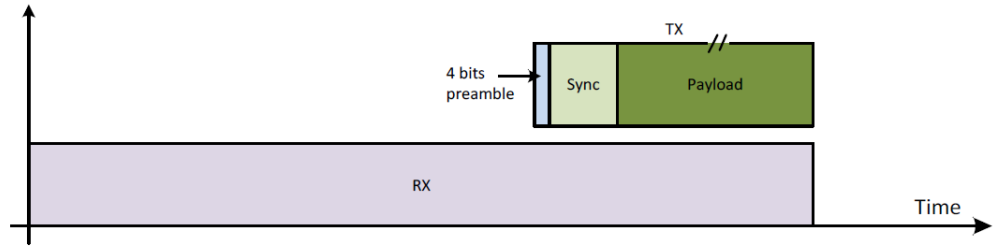


**Figure 42- TI CC1120 RF Kit**

For a better understanding algorithms for minimizing RX current used in this chip, ordinary RX mode and RX Sniff mode is explained in detail.

- **Ordinary RX Mode**

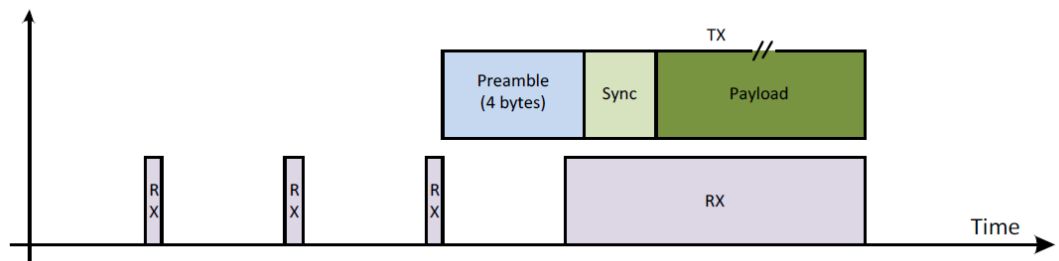
In ordinary mode, the radio packet is consisting of 4 bits of preamble, sync word and the payload. User should poll the RX FIFO whether data is received or not. Following figure explains the details of ordinary mode:



**Figure 43- Ordinary RX Mode**

- **RX Sniff Mode**

In the RX Sniff mode, preamble is increased to 4 bytes. The chip wakes up on intervals and checks that at least 4 bits of preamble is received then go back to sleep. Using this approach chip consumes less power by sleeping in the certain intervals. For a deeper understanding following figure could be used:



**Figure 44- RX Sniff Mode**

According to datasheet of the product following table indicates the current values of RX Sniff mode and ordinary RX mode:

**Table 7- CC1120 RX Modes**

Mode	RX Current(mA)
Ordinary RX Mode	22(peak)
RX Sniff Mode	2

### 3.5.2 Software Studies

In this section, software design and protocol implementation is explained in a more detailed way. Refer to the section System Architecture (3.2), the software is designed in layered architecture in for modularity. In that section it is mentioned that there are 4 layers which are HAL, Link Layer, Transport Layer and Protocol Layer.

For a better understanding, the written code on the CD is walked through in this section. In other words, which functions of the code refer to which layer is explained.

- **HAL Layer**

This layer has the lowest layer and it has initialization functions of peripherals. Timers, interrupts, SPI, UART and GPIO configurations are defined for this layer.

- **Timers:** 1ms Tick Timer interrupt timer is used to create Delay functions.
- **Interrupts:** When RF is in RX mode and data is received, RF unit creates and interrupt to our MCU so that received data could be get. For this purpose, a hardware interrupt pin assigned. Necessary interrupt routines are handled by "*PORTA\_IRQHandler*" function.
- **SPI:** Serial peripheral Interface functions are also on the HAL layer. Using "*spi\_init*" function, SPI clocks and peripherals are initialized. Send and receive over SPI are done via "*SPI\_Send*" function.
- **GPIO:** 3 LEDs and hardware interrupt pin is configured in the "*GPIO\_Init*" function.
- **UART:** Communicating with PC and for easy debug we need to configure UART peripheral. Initialization of the I/O's , clocks, BAUD rate and parity is configured in "*USART\_Init(uint16\_t BaudRate)*" routine.

- **Link Layer**

Radio IC drivers over SPI functions are placed in this layer. SPI communication with MCU and RFU needs these link layer functions. All the data exchange happens using this layer. When a link layer function is called, it uses HAL layer to send and receive data. Following functions are used for link layer:



- *cc112xSpiWriteReg* → Write values to configuration /status/extended radio registers
- *cc112xSpiReadReg* → Read values from configuration /status/extended radio registers
- *cc112xSpiWriteTxFifo* → Write “pData” to radio transmit FIFO
- *cc112xSpiReadRxFifo* → Reads RX FIFO values to “pData” array
- *runRX* → Run RX scenario so that when receive interrupt comes, received data is get
- *runTX* → Sends TX buffer

- **Transport Layer**

So far, it is mentioned that HAL layer and link layer are the bottom layers of MCU and RFU. In other words, HAL layer and link layer are hardware dependent layers. From now on, while going upwards on the layers, transport layer and protocol layer do not depend on hardware since the code will be almost same in other hardware.

Using bottom 2 layers, data exchange on the air can be done. Now, using transport layer functions the meaning of data makes sense. Instead of communicating with raw data on the air, protocol data is exchanged over the transport layer messages. The message structure and details are explained in section 3.2.

According to radio message frame structure defined in section 3.2, Figure-43 shows the definition of the radio message structure.

```
typedef struct
{
    char Source;           //Source Address
    char Destination;     //Destination Address
    char Direction;       //Direction Address
    char Frame_Type;      //Frame_Type
    char Hop_Count;       //Hop_Count
    char Frame_ID;        //Frame_ID
    char Protocol_Data[10]; //filled with MSG_Protocol (Protocol Data)
}Radio_Message;
```

**Figure 45- Radio Message Structure Definition**

“*R\_CommandParser*” function is responsible for creating and processing radio messages. When a data is received from the link layer, “*R\_CommandParser*” processes the frame and take protocol data.

- **Protocol Layer**

In the upper layer, protocol layer, the protocol data coming from the link layer is processed. According to protocol data necessary operations handled and necessary answers are sent to the link layer.

According to protocol message frame structure defined in section 3.2, Figure-44 indicates the definition of the protocol frame structure.

```
typedef struct
{
    char Addr;           //node address
    char Password;      //password for not to mix with neighbour networks
    char Command;       //command
    char RSSI;          //RSSI value
    char WakeUpTime;    //Wakeup time for next cyclic communication
    char Temperature;  //temperature value
    char AlarmFlags;    //alarm
}MSG;
```

**Figure 46- Protocol Message Frame Structure**

“*P\_CommandParser*” routine handles the processing the protocol data coming from link layer according to section 3.2.

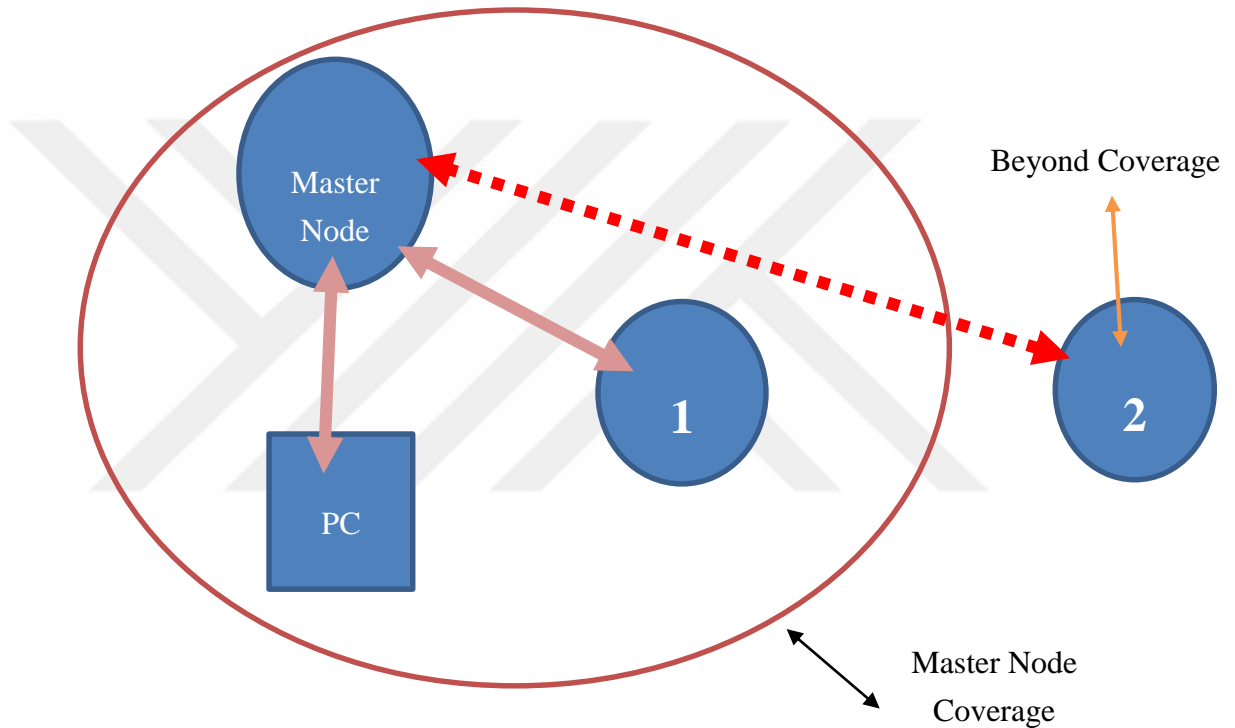
### **3.6 Test and Validation**

Definition of protocol, system architecture and implementation topics covered so far. Test setup circuit will be explained in this chapter.

In former chapters, hardware components were described. As previously mentioned that one sensor node consists of one FRDM-KL25z board as MCU, one

CC1120 kit as RCU and one battery. Apart from slave nodes, in the case of master node, an UART connection to a PC is used to see the output of the system.

Three nodes are used for validation which are placed as one master and two slaves. Master node is responsible for gathering temperature readings data from slave nodes and send this data to PC from serial port via terminal. Following figure illustrates the test and validation setup.



**Figure 47- Test and Validation Setup**

According to Figure-45, Master node, PC and other two nodes are placed for test and validation setup. Master communicates PC via UART over a serial port opened on PC. A terminal program managed this communication. When master gather data, it sends data to PC over serial communication. Moreover, node-1 placed in the reach of master whereas node-2 is placed beyond the range of master.

In the beginning, Master checks its DCP table as mentioned in Chapter 3.2.1.1, at first the DCP table is empty. Therefore, master initiates DCP sequence. When master broadcasts a DCP signal, it is expected that master finds Node-1 and cannot reach Node-2. Then Master adds Node-1 into its DCP Table.

After filling DCP Table of Master with Node-1, Master commands Node-1 to search its nearby nodes. When Node-1 starts DCP sequence, it would find Node-2 and Master Node. In the light of this information, Node-1 creates its DCP Table. Node-1 sends its DCP table to the Master Node. Then Master compares its DCP table with the one coming from Node-1. After comparison of Master's and Node-1's DCP Table, Node-2 is added to the Master's DCP table. Thus, Node-2 where is placed beyond the reach of Master, is discovered by Master. Detailed operation is explained in Chapter 3.

Now, Master knows that there is a node out of its reach. Node-1 will send messages coming from Master to Node-2. Thus, coverage of Master node is increased via this method.

So far Master learned its nearby and connectable nodes. The second part of this system is gathering data from sensor nodes and sends it to the terminal. Following figure shows the communication log coming from master.



**Figure 48-Communication Log Between Master and PC**

Power consumption of the test setup measured in the following way

- Node current of one TX sequence with the max output power is measured
- Current consumption of the node is measured in the RX interval.

RX and TX power of one node is measured and the result are shown in the table below:

**Table 8- Measured Currents of Different Modes**

Sequence	RX Current(mA)
RX (ordinary mode)	10
RX (Sniff mode)	3
TX	30

Considering “WakeupTime” parameter which defines the interval of sensor monitoring is defined as 5 minutes, following four scenarios applied on the test setup shown in Figure-47. Furthermore, one-hour energy consumption of whole test setup of 4 scenarios are measured. The results can be seen on Table-9.

**Table 9- Energy Consumptions of Test nodes for 4 Scenarios**

Scenario	1 Hour Energy Consumption (mAh)
Flooding + Ordinary RX mode	450
Flooding + RX Sniff Mode	345
DCP + RX Sniff Mode	270

During the measurement phase following cases should be taken into consideration:

- Measured energy consumption value is the total energy consumed by all nodes on the test setup
- Master node always on in order to communicate with PC
- Slave nodes Node-1 and Node-2, apart from RX and TX sequences they are at sleep phase
- 1-hour total consumption value shows the whole system power consumption
- All LEDs on the board should be use in order to understand the phase of the nodes during measurements.



## 4 CONCLUSION AND FUTURE WORK

In this thesis, wireless sensor network systems are presented. Moreover, contents of a WSN node, basic wireless communication topics and methodology of this study is covered. It is empirically illustrated that using our approach on WSN networks, the coverage of Master Node is increased. In addition, related protocols are examined.

Prior work is done to apply and create our Discovery and Configuration Procedure in order to increase the coverage of the system with self-routing configuration in gateway controlled WSNs. In order to create such a system, current protocols and approaches are carefully studied.

All the analysis is simulated by using test nodes which are composed of FRDM-KL25 development kit and TI-CC1120 daughter kit. For simulating whether our protocol is working or not, sensor node hardware is programmed and tested on the field.

Result of this study indicates that Discovery and Configuration Procedure extends the coverage of the master node. Then, configuration process organizes how nodes communicates each other by deciding routing. Finally, in the normal mode all the data gathered from sensor nodes on the field is sent to the PC application by master node.

To sum up, it is observed that Discovery and Self Configuration Procedure increases the communication range of the master node and consumes less energy compared to flooding technique.

At the beginning of the thesis, it was mentioned that for this research the priority of the range extension of master node is higher than the energy consumption. As future work, more energy efficient routing algorithms could be researched while increasing the coverage of the master node.

## REFERENCES

**Santra, S., & Acharjya, P. P. (2013).** A Study And Analysis on Computer Network Topology For Data Communication. *International Journal of Emerging Technology and Advanced Engineering*, 3(1).

**Arulmozhi and G., Nadarajan, R.,** 2003, *Mathematical and Computational Models*, Allied Publishers, 542-544.

**Stankovic, J. A. (2008).** *Wireless sensor networks*. computer, 41(10).

**Akbas, A., Yildiz, H. U., Tavli, B., & Uludag, S. (2016).** joint optimization of transmission power level and packet size for WSN lifetime maximization. *IEEE Sensors Journal*, 16(12), 5084-5094.

**Tekkalmaz, M. (2013).** *Power-source-aware adaptive routing in wireless sensor networks* (Doctoral dissertation, bilkent university).

**Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., & Pister, K. (2000).** System architecture directions for networked sensors. *ACM SIGOPS operating systems review*, 34(5), 93-104.

**Nivedhitha, V., Baranidharan, B., & Santhi, B.** *A Survey on Coverage Control Protocols in Wireless Sensor Networks*.

**Wang, B. (2011).** Coverage problems in sensor networks: A survey. *ACM Computing Surveys (CSUR)*, 43(4), 32.

**Razavi, B., & Behzad, R. (1998).** *RF microelectronics* (Vol. 1). New Jersey: Prentice Hall.

**Akyildiz, I. F., & Vuran, M. C. (2010).** *Wireless sensor networks* (Vol. 4). John Wiley & Sons.



**Tan, H. O., Korpeoglu, I., & Stojmenovi, I. (2011).** Computing localized power-efficient data aggregation trees for sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 22(3), 489-500.

**Berker, B. (2008).** E-sense: a wireless sensor network testbed and system for monitoring inbuilding environments (Doctoral dissertation, bilkent university).

**Karl, H., & Willig, A. (2005).** Architectures and Protocols for Wireless Sensor Networks. Chichester.

**Intanagonwiwat, C., Govindan, R., Estrin, D., Heidemann, J., & Silva, F. (2003).** Directed diffusion for wireless sensor networking. *IEEE/ACM Transactions on Networking (ToN)*, 11(1), 2-16.

*Figure 2:* EM Spectrum. adapted from <http://www.ti.com/lit/ml/slap127/slap127.pdf>

*Figure 3:* Simplex Mode Communication adapted from <http://mjwavesofenergy.weebly.com/wireless-networkscommunications.html>

*Figure 4:* Half Duplex Communication. adapted from <https://upload.wikimedia.org/wikipedia/commons/b/b3/HalfDuplex.JPG>

*Figure 5:* Full Duplex Communication. adapted from [https://en.wikipedia.org/wiki/Duplex\\_\(telecommunications\)#/media/File:FullDuplex.JPG](https://en.wikipedia.org/wiki/Duplex_(telecommunications)#/media/File:FullDuplex.JPG)

*Figure 11:* Amplitude Modulation. adapted from [https://upload.wikimedia.org/wikipedia/commons/8/8d/Illustration\\_of\\_Amplitude\\_Modulation.png](https://upload.wikimedia.org/wikipedia/commons/8/8d/Illustration_of_Amplitude_Modulation.png)

*Figure 18:* Point-to-Point Topology. adapted from - <http://www.infiniteinformationtechnology.com/internet-things-network-topology>

*Figure 19:* Bus Network Model adapted from -

<https://upload.wikimedia.org/wikipedia/commons/4/47/BusNetwork.svg>

*Figure 20:* Ring Network Model. adapted from -

<https://upload.wikimedia.org/wikipedia/commons/7/75/RingNetwork.svg>

*Figure 21:* Star Network Topology. adapted from -

<http://www.infiniteinformationtechnology.com/internet-things-network-topology>

*Figure 22:* Mesh Network Topology adapted from -

<http://www.infiniteinformationtechnology.com/internet-things-network-topology>

*Figure 24:* Gossiping. adapted from –

<http://sensors-and-networks.blogspot.com.tr/2011/10/gossiping.html>

*Figure 43:* Ordinary RX Mode adapted from -

<http://www.ti.com/lit/ug/swru295e/swru295e.pdf>

*Figure 44:* RX Sniff Mode. adapted from –

<http://www.ti.com/lit/ug/swru295e/swru295e.pdf>

*Table 7:* CC1120 RX Modes. adapted from –

<http://www.ti.com/lit/ds/symlink/cc1120.pdf>

