DESIGN OF A WIRELESS MESH SENSOR NETWORK FOR A HOUSING COMMUNITY

John Maloco

M.EngSc **2010**

NUI MAYNOOTH

Ollscoil na hÉireann Má Nuad

DESIGN OF A WIRELESS MESH SENSOR NETWORK FOR A HOUSING COMMUNITY

A thesis presented to the National University of Ireland, Maynooth

by

John Battista Maloco

for the degree of Masters of Engineering Science by Research

September 2010

Department of Electronic Engineering

Faculty of Science and Engineering

Supervisor: Dr. Séamus McLoone
Head of Department: Dr. Seán McLoone

ABSTRACT

Wireless mesh sensor networks are typically a cluster of intelligent radio nodes which transfer data between each other directly in a hop, or indirectly through two or more hops via adjacent nodes. These nodes contain one or more sensors. Wireless mesh sensor networks provide a solution in monitoring and controlling the physical world around us and offer far reaching potential applications. This thesis presents a design and prototype development of one such potential application, namely the use of a wireless mesh sensor network to monitor the events and activities in a housing community environment.

The first part of this thesis examines wireless mesh sensor networks in detail. It looks at the technology behind these networks and the methods employed in transferring data between wireless nodes.

The second part of this thesis focuses on the system design, implementation and prototype realisation of the wireless mesh sensor network for a housing community. It shows how an application specific approach can simplify the design of the system. In addition it presents two novel MAC protocols for the transfer of data from transmit-only sensor nodes to fixed infrastructural mesh nodes.

ACKNOWLEDGEMENTS

First, I would like to thank my supervisor Dr. Séamus McLoone for his help, guidance and command of the English language. I would also like to thank the staff of the Electronic Engineering department at NUI, Maynooth, for their encouragement and support, especially Prof. John Ringwood, Dr. Sean McLoone, Denis Buckley and James Kinsella.

I would also like to extend my thanks to Human Resources at NUI, Maynooth for their support, especially Ms. Mary Kelly.

Finally, thanks to friends and family for their support throughout. Thanks especially to my wife, Suzanne and my son Ben for their patience during the last few months.

This thesis is dedicated to my wife and son, to my late father, Alfredo and to my mother Lena.

DECLARATION

I hereby declare that this thesis is my own work and has not been submitted in any form for another award at any university or other institute of tertiary education. Information derived from published and unpublished work of others has been acknowledged in the text and a list of references has been provided.

Signed: _____

Date: _____

Table of Contents

List of Figures

NOMENCLATURE

The following is a list of abbreviations used in this thesis.

ACK	:	Acknowledgement
ADC	:	Analogue to Digital Converter
AODV	:	Ad-hoc On Demand Distance Vector
CDMA	:	Code Division Multiple Access
CSMA	:	Carrier Sense Multiple Access
CTS	:	Clear to Send
DSDV	:	Destination Sequenced Distance Vector
DSR	:	Dynamic Source Routing
DTOA	:	Difference in Time of Arrival
FDMA	:	Frequency Division Multiple Access
FIFO	:	First In First Out
GPIO	:	General Purpose Input Output
GPRS	:	General Packet Radio Service
GPS	:	Global Positioning System
GSM	:	Global System for Mobile Communications
HK	:	Housekeeping
ISM	:	Industrial, Scientific and Medical
MAC	:	Medium Access Control
MACA	:	Multiple Access with Collision Avoidance
MCU	:	Microcontroller Unit
MEMs	:	Micro Electro-Mechanical systems
MSF	:	No meaning. It is a broadcast station identification.
MSN	:	Mesh Sensor Network
PCB	:	Printed Circuit Board
RF	:	Radio Frequency
RFID	:	Radio Frequency Identification
rfPIC	:	Microcontroller with built-in radio transmitter from Microchip
ROI	:	Region of Interest
RSSI	:	Received Signal Strength Indicator
RTS	:	Ready to Send
Rx	:	Receiver
RxTx	:	Transceiver
SMS	:	Short Message Service
SOF	:	Start of Frame
TDMA	:	Time Division Multiple Access
TOA	:	Time of Arrival
TORA	:	Temporally Ordered Routing Algorithm
Tx	:	Transmitter
UWB	:	Ultra Wide Band
Wi-Fi	:	Wireless Internet IEEE802.11 standard
WLAN	:	Wireless Local Area Network
WMSN	:	Wireless Mesh Sensor Network
WPAN	:	Wireless Personal Area Networks
WSN	:	Wireless Sensor Network

1. INTRODUCTION

Wireless mesh sensor networks (WMSNs) are a collection of intelligent wireless nodes equipped with one or more sensors. These nodes work together in order to facilitate collaborative measurements. They form interconnecting mesh networks which provide data paths which can route data from source nodes to destination nodes. Wireless mesh sensor networks provide a solution in monitoring and controlling the physical world around us.

In recent years the area of low power localised wireless sensor networks (WSNs) has attracted a vast amount of research interest, mainly due to the fact that these wireless sensor networks encompass many different areas of technology, including wireless technology, networking, computation, sensors and circuitry. In each of these areas, concepts, tools and applications offer further research and development opportunities. Another driving factor for this interest in wireless sensor networks is the availability and continuing evolution of low cost hardware solutions in realising working systems. An example of this is the availability and variety of low power, low cost, radio modules operating in licence-free radio bands covered by the Short Range Device Regulatory Compliance (Loy et al. 2005). These licence exempt radio bands include the pan-European band at 868 MHz and the ISM (industrial, scientific and medical**)** band. Some of the radio frequencies covered by the ISM band include 433 MHz, 915 MHz and 2.4GHz (Loy et al. 2005).

The radio modules were originally designed as wire replacement for point to point data transfer and remote control applications, operating on the principle of digital in (transmitter side) and digital out (receiver side). The appeal of these devices is largely due to their attributes:

- They require very little power making them ideally suited for battery operation.
- They are low cost.
- Little or no radio frequency (RF) expertise is required to use them.
- They are easy to interface to other hardware such as microcontrollers.

- They are capable of transferring data up to Mbits/s and can have ranges from tens of metres to tens of kilometres.

Ongoing improvements in power consumption, performance, size and integration continues to fuel research and development in low power radio applications. The ultimate goal for this continuing research and hardware development is to develop applications which will benefit society. Wireless mesh sensor networks could be considered one such application. It could also be considered a platform from which to develop other applications, as this thesis will show.

The home and living environment is currently attracting much interest as an area for wireless applications. Research is looking at wireless technology to effectively create the smart home of the not too distant future. Wireless home automation will provide more flexible management of lighting, heating and cooling, security, and home entertainment systems from anywhere in the home. The idea of automating the living space through wireless control and sensors is on the threshold of becoming commonplace in many homes. RF wireless systems such as ZigBee (Jianpo et al. 2010]), Bluetooth (Davies 2002), Z-Wave (Gomez and Paradells 2010), RFID (Roberts 2006; Want 2006), and Wi-Fi (IEEE 802.11) (Hiertz et al. 2010) offer the means to achieve this.

While wireless home automation research is gathering momentum, this research looks at extending wireless technology beyond the house and into the housing community. This is an area which is yet to be fully exploited.

1.1 Motivation

Wireless applications such as remote meter reading and RFID tags for refuse bins have already found their way out of the house and into the community. These systems have been developed by the service providers with their interest in mind, namely cost savings and ease of service. It is fair to say that communities can benefit from these initiatives also, as service providers may choose to pass these benefits onto the consumer in terms of cost savings and quality of service.

This research examines how best to develop a wireless network to provide these and other services to a housing community which primarily benefits the community. This thesis is a report on the research, design and development of a wireless mesh sensor network to be deployed in a housing estate environment and identifies some of the benefits this type of network could offer.

Networks already exist between many houses in a housing estate. At present this is mainly through the internet protocol TCP/IP, which in most cases is an indirect link provided by Internet Service Providers (ISPs). Wireless links are also becoming more prevalent, with Wireless Local Area Networks (WLANs) based on the IEEE 802.11 (Wi-Fi) standards. Many of these WLANs have a gateway to the internet provided by wireless broadband service providers.

The direction for this research is to develop a novel housing estate network based on licence exempt, low power wireless technology, not in competition with IEEE 802.11. This system should be both affordable and beneficial to a housing community. These benefits may also extend to service providers to the housing community.

1.2 Objective

The objective of this research is to develop a wireless mesh sensor network for a housing community that is reliable, low cost and allows for easy implementation. In order to achieve this it is important that existing technology and methods are examined.

At the start of this research the focus was mainly on developing a system for the sole purpose of tracking children in a housing estate. The child would wear an active RFID tag (Roberts 2006) which would transmit a unique identification code at regular intervals. A network of radio nodes, strategically placed around the housing estate, could then monitor this tag. The radio nodes would then relay this information back to a central location to process the data to determine the radiolocation of the RFID tag.

This initial research has been expanded to design a multipurpose wireless mesh sensor network for a housing community. One of the features of this sensor network is the

ability to locate mobile sensor nodes. This retains the possibility to locate children within the network. As part of this research a number of existing radiolocation methods are examined and suggestions are made as to the method of radiolocation that best meets the requirements of the system.

The design of the proposed WMSN is based on an application specific approach, which helps alleviate the complexities of designing for generic applications. The design approach will highlight critical design issues and discuss how tradeoffs can substantially help in overcoming difficulties in reaching design goals. The design philosophy is one of simplicity. To quote Albert Einstein *"Everything should be made as simple as possible, but not simpler".* This hopefully will be evident in the coming chapters.

1.3 Contribution of Thesis

This thesis is a report on the design and development of a novel application based on wireless mesh sensor networks (Poor and Hodges 2002). The main contributions which were made by this thesis are:

1. System design of a novel housing community monitoring network based on wireless mesh sensor networks.
2. The design of a TDMA MAC protocol, synchronised by the MSF atomic clock radio signal (Maloco et al. 2006).
3. The design of a MAC protocol to support transmit-only wireless sensor nodes (Maloco and McLoone 2007).
4. Hardware and software design of a wireless mesh node and a wireless sensor node, specifically designed to meet the requirements of the system outlined in this thesis.

1.4 Outline of Thesis

The remainder of this thesis is structured as follows:

In chapter 2 information pertaining to the main areas of this research is established. The research is based on the technology of wireless mesh sensor networks. This technology is examined, breaking it down into the following topics; Mesh networking; Sensor networks; Routing algorithms; MAC protocols; Radiolocation; Energy scavenging; System deployment; Standardising wireless sensor networks.

Chapter 3 examines the requirements and applications of the proposed WMSN. It presents a high level design overview which encompasses all aspects of the system. It also discusses the reasoning behind the approach of the design. The system design concept focuses on a hybrid solution for a wireless mesh sensor network, in which wireless mesh nodes are deployed in a fixed infrastructure and transmit-only sensors are deployed wirelessly. The chapter concludes with a discussion on how the system is expected to perform.

In chapter 4 two Medium Access Control (MAC) (Ye and Heidemann 2003) protocols are proposed to ensure data is successfully transferred between wireless sensor nodes and wireless mesh nodes. The first of these protocols investigates the use of the UKs MSF (NPL 2005) atomic time signal as a synchronisation source for a Time Division Multiple Access (TDMA) MAC protocol. The second protocol adopts a ‘transmit and hope’ scheme, implementing techniques to reduce the probability of data collision (Stathopoulos 2004).

Chapter 5 and 6 presents a detailed design of both the hardware and software pertaining to the wireless sensor node and wireless mesh node respectfully.

Chapter 7 presents concluding discussions and outlines a few ideas for future work on this research.

2. WIRELESS MESH SENSOR NETWORKS

Wireless mesh sensor networks combine the advantages of wireless mesh networks and wireless sensor networks. This research is based on the application of a wireless mesh sensor network. This chapter presents a review of the technologies and techniques used in implementing such networks.

2.1 Mesh Networking

A mesh network is a communications network of inter-connected nodes and has one of two connection arrangements:

- Partial mesh topology: Every node is connected to every other node, but it may not be directly connected. Information may have to be passed between a few nodes before it reaches its destination, see figure 2.1(a).
- Full mesh topology: Every node is directly connected to every other node in the network, see figure 2.1(b).

Both the full and partial mesh topologies are reliable because they offer a measure of redundancy. If a node is damaged, information may still be able to reach its destination by being rerouted.

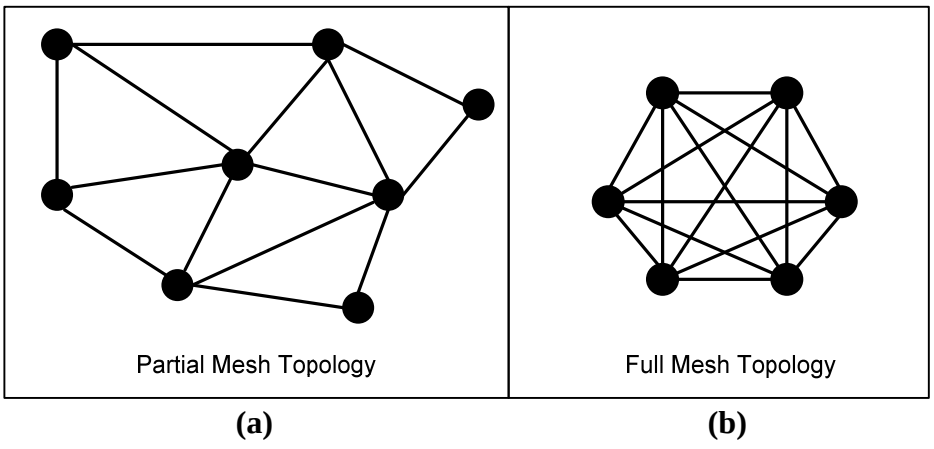


Figure 2.1: Mesh network topology – (a) partial and (b) full

Mesh networks often consist of clients, routers and gateways. In general terms, clients are the end users in the network, such as a desktop computer. Routers forward data to and from other network nodes and gateways. Gateways are portals to other networks and possibly onto the internet.

2.1.1 Wireless Mesh Networks (WMNs)

Mesh networks can be expensive to implement due to the cost associated with the routing and interconnection of cables. In some cases cabling may not even be practical, or even possible, as in, for example, a harbour environment were there may be a requirement for mesh nodes to be implemented between boats.

Wireless mesh networks provide a solution to this problem. A WMN is a network created using wirelessly connected nodes rather than direct connection through cabling. Each node is capable of forwarding on packets of information to other nodes either directly or indirectly via one or more hops. The physical infrastructure of the mesh network is greatly simplified by the use of wireless nodes.

As with wired mesh networks the two main types of nodes, in a WMN, are routers and clients. The wireless mesh routers forward traffic to and from other nodes and gateways which may be connected to the Internet. Wireless mesh clients can also work as routers but tend to be the end user in the network and usually only have one wireless interface. Examples of wireless mesh clients are PDAs, laptops, cell phones and other similar wireless devices.

When designing a wireless mesh network there are a number of critical factors which need to be taken into account. These include:

- **Scalability**: The multi-hop nature of communication in wireless mesh networks can cause scalability issues. The routing protocol may have difficulty finding or managing paths as the size of the network increases.
- **Mesh connectivity**: The self-organising and managing capability of a WMN is an important feature of these networks. Topology aware routing algorithms can greatly increase the efficiency of the network.

- **Quality of Service (QoS)**: Latency in data packet delivery, data transport reliability and data accuracy are among the most important aspects to consider when looking at the QoS in wireless mesh networks.
- **Deployment:** One of the basic requirements for the deployment of any two interconnecting wireless devices is that they are within range of each other. This becomes more strategic when mesh interconnectivity is sought. Mesh topology may form a fixed infrastructure, in which case planning of mesh node positions is required. Wireless mesh networks may also be deployed randomly in an ad-hoc fashion, or consist of mobile devices, in which case nodes must self-organise.

This general description of wireless mesh networking has many applications. These networks can be large and complex, especially when networking Wi-Fi, WiMax (Koon et al. 2007) and Cellular devices, for example. The mesh nodes required in handling such network traffic are themselves complex. These mesh nodes tend to be powerful embedded computers running sophisticated algorithms.

However, wireless mesh networking can be applied to much less complicated systems. This research will now focus on one aspect of wireless mesh networking, that pertaining to localised sensor networks.

2.2 Wireless Sensor Networks (WSNs)

Wireless sensor networks are a collection of intelligent nodes equipped with one or more sensors, a wireless communications device such as a radio, and in most cases an intelligent computing device such as an 8-bit or 16-bit microcontroller (MCU).

As with many technologies the military were key drivers in the development of wireless sensor networks going back to the 1970's and 1980's (Chong and Kumar 2003). One of the target applications for the military was that of battlefield monitoring and surveillance (Tiwari et al. 2007). Wireless sensor networks are now used in many industrial and civilian application areas such as asset tracking and environmental monitoring.

A 2010 report titled "Active RFID and Sensor Networks 2011- 2021" by IDTechEx Ltd. forecasts the active RFID market to grow to 10 times its present size by 2021. This report attributes this growth to a number of factors including the development of wireless sensor networks where large numbers of active RFID tags with sensors are radio networked in buildings, forests, rivers, hospitals and many other locations. Another factor highlighted by this report is a much stronger future market demand for tracking, locating and monitoring people and things.

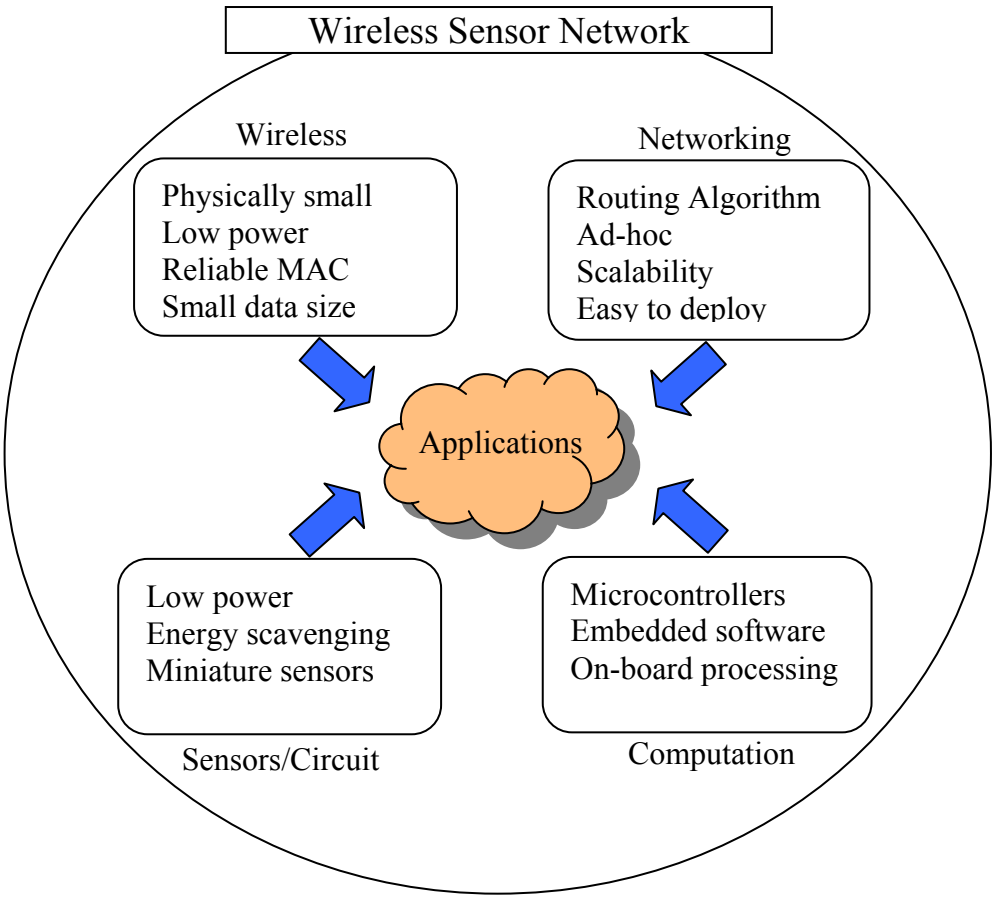


Figure 2.2: Main components of a wireless sensor network

The development of WSNs requires technologies from different research areas: circuitry and sensing, networking, wireless communications, and computing (including hardware, software, and mathematical algorithms). Thus, combined and separate advancements in each of these areas have driven research in sensor networks (Chong and Kumar 2003). Figure 2.2 shows what technologies and components are encompassed in forming a wireless sensor network.

Wireless sensor networks have the following desirable characteristics:

- **Low power:** Wireless sensor nodes tend to be battery operated devices which can be required to operate over a long period of time (1 to 5+ years) unattended. Therefore these nodes must be low power.

- **Transmit small amounts of data:** To ensure long battery life the radio transmitter is switched on for the shortest possible time. Sending small amounts of data (1 to 20 bytes) facilitates this. Short data transmissions also frees-up more channel space for other nodes to transmit.

- **Low cost:** Ideally the node should be low cost, enabling many nodes to be deployed without having a price deterrent.

- **Easy to deploy:** It should be possible to add and remove nodes simply by powering them on and off, thus deploying them in an ad-hoc fashion.

- **Reliability:** Sensor nodes may be unattended for long periods of time. Therefore they are designed to be reliable. This reliability extends to both hardware and software. This reliability also extends to a method of ensuring that data transmitted by the sensor node reaches its destination.

Very often sensor node networks are deployed in mesh configuration. Mesh nodes are often configured to use short multi-hop transmissions rather than larger single hops. This is regulated by reducing the nodes transmission range. This is more energy efficient per node, as short hops require less transmitter power than a single larger direct link. Figure 2.3 illustrates the single hop versus the multi hop transmission path.

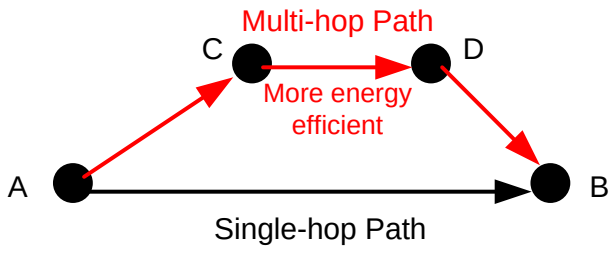


Figure 2.3: Single-hop vs. Multi-hop – energy efficiency

The data flow in sensor networks is mostly unidirectional. Most sensor networks have a single destination or data collection point. This end point can then process, store or forward the data collected from the sensor nodes. This end point can also act as a gateway to other networks, for example, connecting to the internet or a cellular network.

2.2.1 The Wireless Sensor Node

Figure 2.4 depicts a block diagram of a wireless sensor node. This node contains a microcontroller unit (MCU), a radio transceiver, one or more sensors, an external sensor interface, a power source, and memory storage.

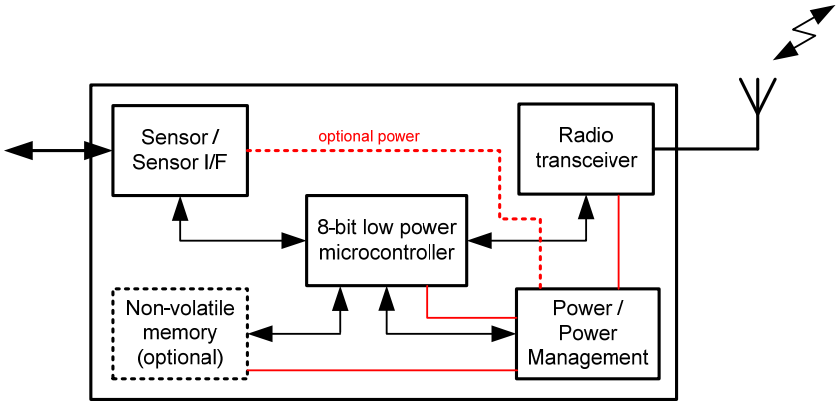


Figure 2.4: Wireless sensor node functional block diagram

Microcontroller

Most manufacturers of microcontrollers now supply a range of ultra low power 8-bit and 16-bit devices in very small form factor. These devices are ideally suited for wireless sensor network applications. Not only do these devices provide the intelligence of the wireless sensor node, they also provide many more resources through their built-in peripherals, such as:

- Analogue to digital converters
- EEPROM (flash) storage memory
- Pulse width modulation
- Timers
- Serial interfaces (I^2C; SPI; UART)
- Direct Memory Access (DMA)

Microcontrollers are programmable devices and, therefore, they are only as good as the programs they execute. This is somewhat alleviated by the availability of software templates or complete operating systems, targeting wireless sensor networks. Some examples of these include TinyOS from the TinyOS Alliance (TinyOS 2010), SimpliciTI from Texas Instruments (TI 2010), and Contiki developed by Adam Dunkels (Contiki 2010). The availability of low cost radio hardware which supports the IEEE 802.15.4 LR-WPAN (low-rate wireless personal-area network) standard, has led to software development of full layered stack protocol solutions such as ZigBee (ZigBee 2010), MiWi (Microchip 2010), and WirelessHART (HART 2007).

The idea behind these solutions is to standardise hardware and software, so as to enable quick development of low-cost, bug-free systems. However, standard solutions can be restrictive due to their generic design, and can introduce many features or overheads which are not required.

Sensors

Wireless sensor nodes typically contain one, or a combination, of sensors including switches, temperature sensors, voltage sensors, light sensors, humidity sensors, vibration sensors, accelerometers and gyros. These sensors range from a simple switch to advanced MEMs (Micro Electro-Mechanical Systems) devices such as accelerometers and gyros. The advancement in miniature MEMs technology has produced a range of very low power, extremely small, sensors.

However, miniaturisation is not always the driving factor for wireless sensor nodes. It very much depends on the application of the wireless sensor network and on the size of the node itself. In general, wireless sensor nodes can accommodate any sensor that can be interfaced to a microcontroller, as long as the power consumption of the sensor is suitable for the application of these battery powered nodes.

Sensor Interface

Many wireless sensor nodes also have the provision to have external sensors attached through a sensor interface. In most cases this sensor interface is a direct connection to the microcontroller. Most sensors can be interfaced through serial interfaces, analogue (A/D converter) inputs and digital I/O. All of these interfaces can be supported by

peripherals on-board microcontrollers. This aids in minimizing the need for any additional components, thus keeping costs low and saving printed circuit board (PCB) real-estate.

Power/Power Management

The power source for a wireless sensor node is very often supplied by a battery. Minimising the power drain on the battery is one of the prime goals in designing these nodes. The power is mainly dissipated by the radio device while it is transmitting, receiving, or just listening. All other devices also contribute to the power drain. It is therefore important to be able to manage the power to different devices in a wireless sensor node. In order to extend the battery's life, all devices must be either off, or in a low power mode, when not in use. The microcontroller provides the necessary control for the power management of these nodes.

Radio Transceiver

There are numerous radio modules available to operate in licence free bands, such as 433 MHz, 868 MHz and 2.4 GHz bands. All these modules can be easily interfaced to microcontrollers, many of which use standard serial interfaces. It is also possible to get a radio transceiver and a microcontroller in one integrated package. An example of this is Texas Instruments CC1110fx radio chip (CC1110 Datasheet 2010) which combines the CC1101 sub 1 GHz radio transceiver, capable of data rates up to 500 Kbits/s, with an industry-standard enhanced 8051 microcontroller, in a very small 36 pin QFN package 6mm x 6mm. This combination offers a very attractive solution for wireless sensor nodes.

Antennas are also an essential part on any radio system. The antenna options for wireless sensor nodes include (see figure 2.5):

- **External antenna:** This would provide the best performance. This type of antenna can add to cost and space requirements.
- **PCB antenna:** Practically no cost except for PCB real-estate. Can be a challenge to design a good PCB antenna.
- **Chip antenna:** Short range but has the advantage of being very small.

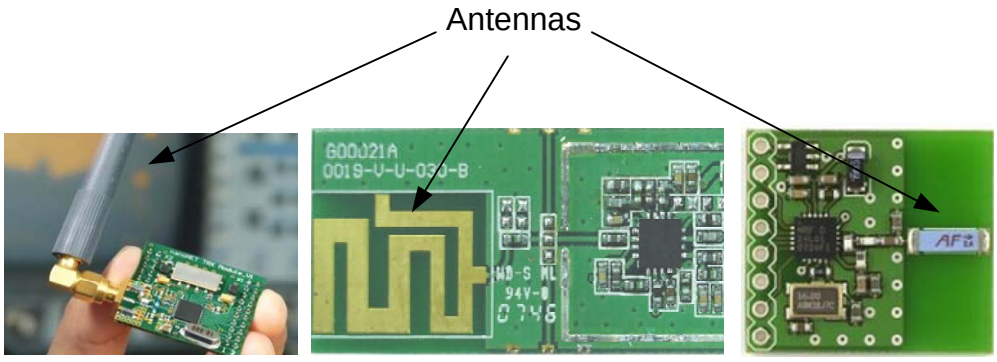


Figure 2.5: Antennas for wireless sensor networks

In some wireless sensor network applications the use of an external antenna is seen as a hindrance due to its size (see figure 2.5(a)). This has led to more use of chip and PCB antennas. Whichever type of antenna is used, it is important to ensure that the implementation and design of the antenna is done correctly, for example, in terms of impedance matching.

Most radio modules come equipped with impedance matching circuitry and, in some cases, complete with antenna as shown in figure 2.6. Single chip radios such as Texas Instruments CC1101, usually require some external circuitry to impedance match the output of the radio to the antenna. This type of information is usual supplied by the manufacturer in the product datasheet for the device.

Figure 2.6: XBee radio module complete with antenna
(Image from http://www.mobilenetx.com)

Badly designed or matched antennas can significantly reduce a radio's performance, which can lead to unnecessary additional power consumption. This would be a major concern for the low power sensor nodes.

2.3 Routing Algorithms

One of the key elements in determining the performance of a wireless mesh network is the routing algorithm adopted by the network. Routing is the process of selecting paths in a network along which to send data. Routing algorithms are used to select the best path to send the data. To do this they take into consideration things like number of hops required, time delay and communication cost of packet transmission (Razavi 2002). In this section a brief overview of a number of existing routing algorithms is presented.

There are many varied types of routing protocols available for wireless mesh networks. It is not the scope of this research to detail all these algorithms. Instead the reader is referred to (Lang 2003) which provides a comprehensive overview of a number of the currently available routing protocols. It classifies each routing protocol according to its key characteristics such:

- **Single channel versus multi-channel protocols:** Single channel protocols use just one frequency channel to communicate, whereas multi-channel protocols such as Code Division Multiple Access (CDMA) and Frequency Division Multiple Access (FDMA) use a number of frequencies, allowing for parallel data transfer. Communication is much more efficient using a multi-channel protocol, but it can be difficult to implement it in a completely mobile wireless mesh network because a controlling station is needed to assign the channels.

- **Uniform versus non-uniform protocols:** In a system where a uniform protocol is implemented, nodes have no special functions assigned to them. In non-uniform routing protocols some nodes may be assigned to be a gateway, or an end client for example.

- **Hierarchical topology/clustered routing:** Clusters are introduced to bring some structure into a dynamic system. Each cluster will have a cluster head node which is responsible for the creation and expansion of the cluster. The cluster heads build up a hierarchy of clusters and they also manage the communication within the clusters. Gateway nodes are responsible for the communication between the node clusters. However, they can cause bottlenecks for the flow of data between the clusters.

- **Position based protocols:** These protocols require no routing tables to be maintained. Information is sent in the direction of the destination and therefore there is no overhead required to find or update routes. Based on the geographic position of a packet's destination, each node knows only its own position and the position of its one-hop neighbours in order to forward data packets (Mauve et al. 2001).

- **Pro-active versus on-demand routing (re-active) protocols:** In proactive routing a routing table is maintained detailing the routing information to every node in the network. Updates to the table can be event driven (i.e. only when a change is recognised) or they can be periodic. On-demand protocols however do not maintain a routing table. A route is only calculated when it is needed.

- **Full versus reduced topology protocols:** In full topology protocols all the topology information is distributed, whereas in reduced topology protocols only some of the information is distributed.

- **Use of source routing:** In this type of protocol the route depends on the source of the data. The source puts all the routing information into the header of the data packet and the forwarding nodes use this information. Under certain circumstances, such as a node no longer existing, the forwarding node can change the routing information.

- **Use of broadcast messages:** There are various types of broadcast messages that a routing protocol may employ:

- **Local Multicast:** Only broadcast to some nodes in the transmission distance.
- **Local Broadcast:** Transmit to all nodes in the transmission distance.
- **Network wide Broadcasting:** Flood the whole network.

2.3.1 Popular Routing Algorithms

There are four routing protocols which are widely discussed and compared (Mittal and Kaur 2009; Bouhorma et al. 2009; Esmaeili et al. 2007; Geetha et al. 2006; Chenna and ChandraSekhar 2006). These are DSDV, DSR, TORA and AODV (Broch et al. 1998) and are summarised here for the convenience of the reader.

- **DSDV – Destination Sequenced Distance Vector:** This is a proactive protocol that updates routing information on a regular basis. To avoid routing loops, destination sequence numbers have been introduced. Broch et al. (1998) shows that DSDV does not perform well against DSR, TORA and AODV in high mobility networks. However, in static or low mobility network this routing algorithm performs equally as well as the others. Figure 2.7 shows comparative results for this.

- **DSR – Dynamic Source Routing:** This is an on-demand reactive protocol that uses source routing. Each packet must carry its complete route to its destination in its data header. Routes must be discovered using a route discovery mechanism. Once discovered they can be saved in routing tables. If broken links are detected a route error message is sent throughout the network and a route maintenance mechanism takes over to try and repair the route.

- **TORA – Temporally Ordered Routing Algorithm:** TORA is a source initiated protocol and can provide routes between any source/destination pair. It supports on-demand routing for networks with a large degree of mobility and proactive routing for networks with less mobility. TORA assigns *height* values to links and data may only flow from nodes with higher heights to nodes with lower heights. By doing this the protocol builds a loop-free, multipath routing structure. TORA ensures that all nodes maintain up-to-date routing information about adjacent

(one-hop) nodes. When performing on-demand routing TORA does three basic functions, namely route creation, maintenance, and deletion (Pirzada et al. 2005).

- **AODV – Ad-hoc On Demand Distance Vector:** This is an on demand reactive routing protocol. If a route to a destination is unknown, a route discovery process is initiated. This consists of broadcasting a route request packet in an expanding ring search technique. If a destination sees a request it will reply with a route reply packet. Research shows that, AODV gives the best overall results for dynamically changing networks were the mobility may change from highly mobile to static (Chenna and ChandraSekhar 2006; Lang 2003).

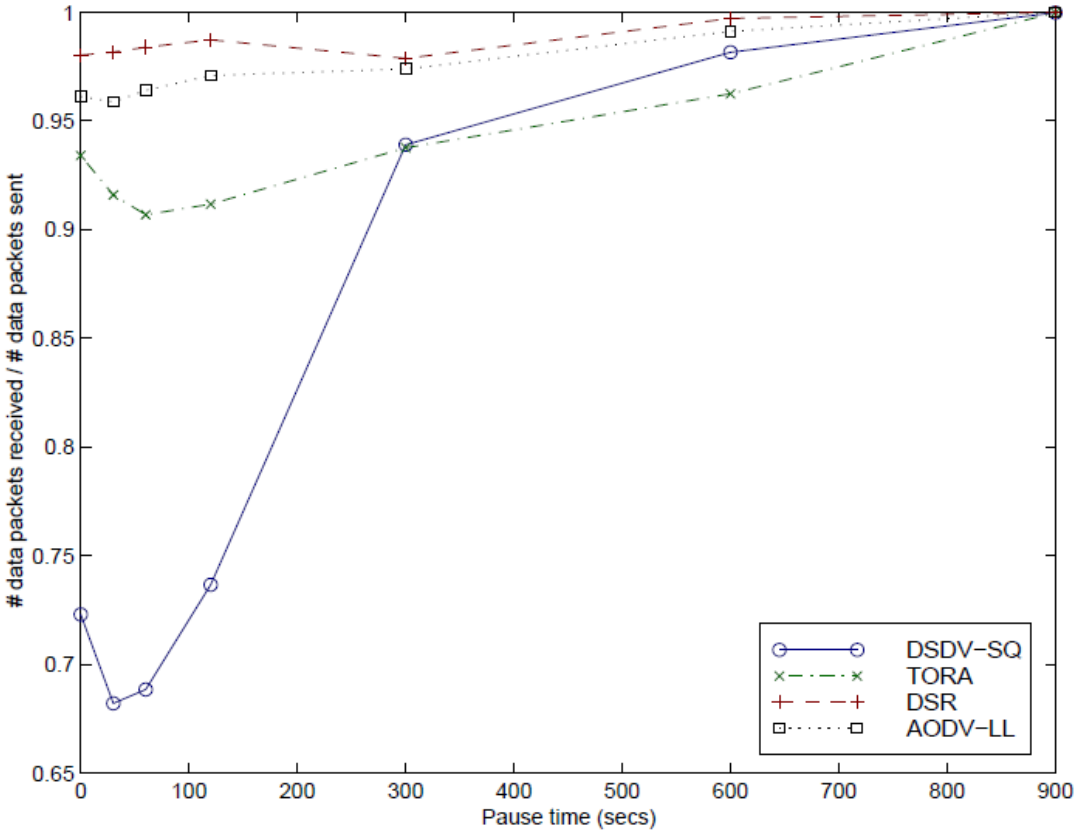


Figure 2.7: Comparison between the four protocols of the fraction of application data packets successfully delivered (packet delivery ratio) as a function of pausetime. Pause time 0 represents constant mobility. (Broch et al. 1998)

2.3.2 Simplifying the routing issue

In an attempt to simplify the selection of a routing protocol, suitable for an application as described in this thesis, the protocols are broadly divided into proactive and

reactive types. Proactive protocols have stored routing tables which rarely change. Reactive protocols have dynamic routing tables or no routing tables at all.

When the mobility of wireless nodes in a network is high, reactive protocols out perform proactive ones. This is mainly due to the constant changing of routes. Reactive protocols calculate or discover the required route on demand so routing tables are not necessary. This makes them ideal for high mobility node networks.

However, nodes in a wireless sensor networks are not always mobile. In many cases wireless sensor nodes are strategically placed in a fixed infrastructure to perform tasks, such as environmental monitoring. The routes between these nodes are then known and fixed. Routing using proactive look-up routing tables is then easy to implement and maintain. For this reason the DSDV routing protocol is examined in a little more detail.

The destination sequenced distance vector protocol or DSDV is a proactive protocol that updates the routing information on a regular basis. To avoid routing loops, destination sequence numbers have been introduced. Each node maintains lists of all the available destinations, information about adjacent nodes to reach destinations and the number of hops required to reach each destination, in a routing table. The routing entry is tagged with a sequence number which is originated by the destination station. Every time a route is updated a new incremental sequence number is associated with it. For any particular route, nodes should ensure they use the most up-to-date one, i.e. the route with the highest sequence number associated to it. In order to maintain consistency, each node transmits and updates its routing table periodically. The packets being broadcasted between nodes indicate which nodes are accessible and how many hops are required to reach them.

The advantages of DSDV include:

- Protocol guarantees loop free paths.
- The protocol algorithm is easy to implement.
- Complexity and maintenance is reduced significantly if all nodes have one destination.

- Performs well against other routing algorithms when the mobility of nodes is low.
- DSDV only maintains the best path information rather than information on all the paths to the destination. This reduces the amount of space required to store the routing tables.

The disadvantages of DSDV include:

- Does not perform well against other routing algorithms when the mobility of nodes is high.
- DSDV doesn't support multi-path routing.
- The larger the network the more difficult it is to maintain the routing table information, particularly when any node can be the destination. This is because each node must maintain an entry detailing how to get to each other node.

In summary, the DSDV or a variation based on DSDV would be a very good choice for a proactive routing protocol as long as the node mobility is low and there is a single destination in the network.

2.4 MAC Protocols

The **Media Access Control** (**MAC**) provides addressing and channel access control mechanisms that make it possible for several network nodes to communicate within a multi-point network.

The most typical way to transfer data between two wireless devices is to establish a two-way communication path. In order for nodes to send and receive data they require both radio transmitters and receivers (transceivers). With two-way communications any transfer of data can be acknowledged by the recipient giving the sender confirmation whether the data was received successfully or not. Unsuccessful confirmation would enable the sender to resend the data. Unsuccessful data transfer is often caused by data collision. Data collision is when two wireless devices transmit at

overlapping times on the same radio frequency channel. The data from the two devices effectively collide at the receiver, corrupting both data transmissions.

Having transceivers in all nodes, a number of protocol options for transferring data are possible. The protocols presented here are both basic and relatively easy to implement. Some protocols are designed to recover from collisions such as Pure Aloha and Slotted Aloha. Another type of protocol is the collision avoidance protocol. Three such protocols are CSMA (Carrier Sense Multiple Access), MACA (Multiple Access with Collision Avoidance) and TDMA (Time Division Multiple Access)

2.4.1 Aloha and Slotted Aloha

Aloha, also known as pure Aloha, is basically sending packet data when available and waiting for an acknowledgement. If no acknowledgement is received the data is resent after a random amount of time.

A slight improvement to this protocol is Slotted Aloha. This is a synchronous system which introduces discrete timeslots. The size of the timeslot is determined by a fixed packet transmission time. Data is only sent at the beginning of the next timeslot. This means that packets overlap completely or not at all. In order for this to work timeslots must be synchronised between all transmitting nodes. This method reduces the number of collisions compared to pure Aloha. However, the difficulty with Slotted Aloha in wireless networks is the synchronising of all radio nodes so that transmissions occur at the start of a timeslot.

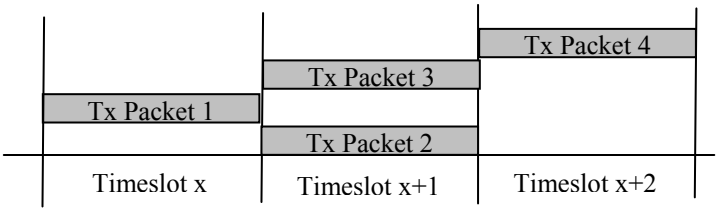


Figure 2.8: Discrete timeslots

Figure 2.8 shows three discrete timeslots in which data packets may be transmitted. This represents the discrete transmission slots as in Slotted Aloha. Timeslots are not reserved for single transmissions and, therefore, multiple transmissions can occur in the same timeslot. In the scenario of figure 2.8 there is a potential for a data collision between Packet2 and Packet3 as they both occupy the same timeslot during transmission. This is only a potential collision as it can depend on the location of nodes and the transmission range, as illustrated in figure 2.9.

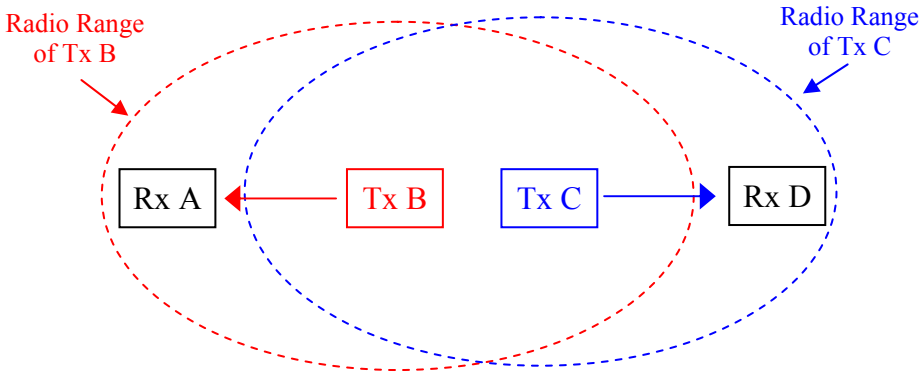


Figure 2.9: Collision potential - exposed terminals

In figure 2.9 transmitter B (Tx B) sends data to receiver A (Rx A) and transmitter C (Tx C) sends data to receiver D (Rx D). If both Tx B and Tx C transmit in the same timeslot no data collision will occur. This is because Rx A is out of range of Tx C and Rx D is out of range of Tx B. Therefore data at the receivers will not be affected by the other transmitter, even though the transmissions occur at the same time.

2.4.2 CSMA

CSMA is a *listen before send* protocol. CSMA listens for a radio frequency carrier signal to determine whether or not the radio channel is busy. Data is sent when the radio channel is available, thereby reserving the channel while sending data. If the data channel is busy CSMA waits a random amount of time before re-checking the status of the channel.

The scenario represented in figure 2.9 can be a problem for CSMA. This problem is known as Exposed Terminal (Adere and Murthy 2010). Even though both Tx B and Tx C can successfully transmit simultaneously to Rx A and Rx D respectfully, CSMA will prevent this from happening. This is because Tx B and Tx C are within range of each other and will be able to sense each others RF carrier. Therefore if either transmits then this will prevent the other from transmitting.

CSMA is also susceptible to the Hidden Terminal Problem (Adere and Murthy 2010). An example of the Hidden Terminal Problem is when two radio nodes, out of reach of each other, transmit data simultaneously to a common node, as shown in figure 2.10.

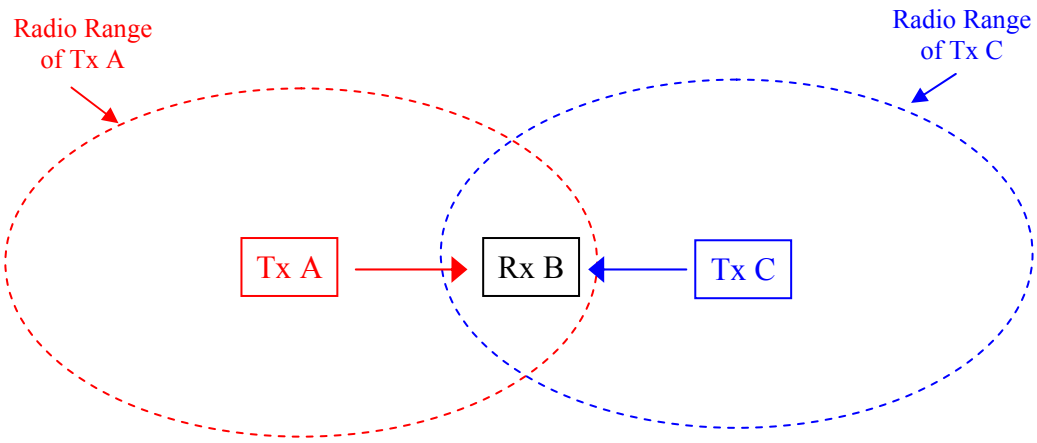


Figure 2.10: Collision potential -hidden terminal problem

If both Tx A and Tx C transmit to Rx B at the same time, neither Tx A or Tx B will be able to sense that the channel is busy as they are out of range of each other, therefore a collision cannot be avoided at Rx B.

In order to combat the hidden terminal problem, CSMA employs the use of an acknowledgement (ACK), i.e. all data sent should be acknowledged by the recipient. This will verify the successful transfer of the data. In the case of no acknowledgement due to data collision caused by a hidden terminal, the collision can be recovered by resending the data. Since wireless communications can't detect collisions, it can try to avoid them. CSMA does this by reserving a free radio channel, before transmitting, using short pulses of data. This is known as CSMA with Collision Avoidance (CSMA/CA) This data has no meaning other than to inform other devices that a

transmission is imminent. This then prevents all other devices from using the radio channel, leaving it free for the reserving device to send its data.

2.4.3 MACA

MACA (Multiple Access Collision Avoidance) implements a simple RTS/CTS (Request To Send/Clear To Send) handshaking protocol (see figure 2.11).

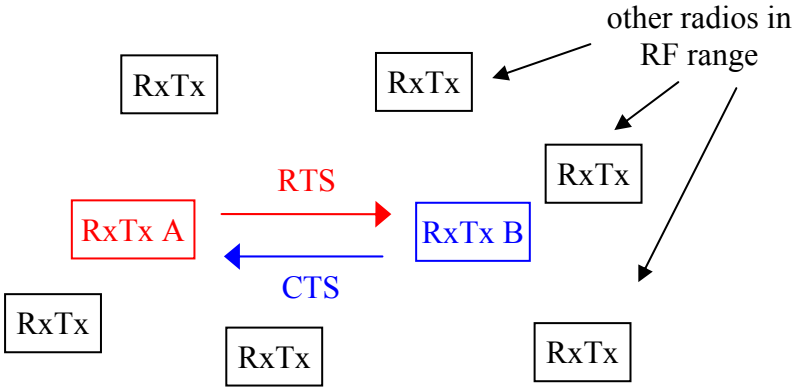


Figure 2.11: RTS/CTS protocol

Radio device A (RxTx A) in figure 2.11 wants to send data to radio device B (RxTx B). In order for this to happen, radio A must send a RTS to radio B. On receiving the RTS, radio B will send a CTS signal back to radio A if it is ready to receive data. On receiving the CTS, radio A will transmit its data to radio B. On hearing RTS and CTS, other radio devices in RF range (labeled in figure 2.11 as RxTx) will refrain from any transmissions until the communications between radios A and B are complete.

2.4.4 TDMA

TDMA (Time Division Multiple Access) is a multiplexing technique that allows transmission from several sources to access the same communication channel. TDMA applies division in the temporal domain. TDMA differs from Slotted Aloha in that TDMA allocates a unique time slot for each source. This time slot is a period of time for a device to transmit its data. In this time period all other devices refrain from transmitting, thus guaranteeing an interference free channel.

In theory TDMA would appear to guarantee collision free data transfer and could therefore support transmit-only devices. This is true for all devices adhering to the same protocol. This does not, however, account for collision from other wireless systems, within RF range, transmitting on the same radio channel. This type of collision could be considered as RF interference.

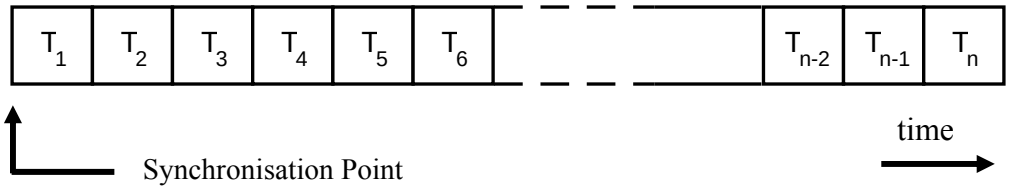


Figure 2.12: Diagram of general TDMA frame

TDMA does require a radio receiver in order to operate correctly. This is to synchronise the start of the TDMA sequence with all other nodes. This is shown in figure 2.12 as the synchronisation point. It is crucial that all nodes are synchronised at this point. The better the accuracy of this synchronisation between all nodes, the better performance can be achieved from the TDMA protocol.

In figure 2.12, time is divided into discrete timeslots, T_1 to T_n. Each radio node will be assigned a unique timeslot. During this timeslot the node can transmit data, confident that no other node is transmitting.

The basic implementation of TDMA uses a fixed number of timeslots of a fixed duration (static TDMA frame). Therefore it is easy for the node to calculate the appropriate time to transmit. For example, if a Node A is allocated timeslot 3 (T_3) and each timeslot period is 100ms, the start of timeslot T_3 will occur at 200ms, i.e. two timeslots after the synchronisation point.

A disadvantage of static TDMA frames is that the timeslot is reserved regardless of whether a node wants to transmit or not. This can be overcome by using Dynamic TDMA frames. These can be dynamically configured i.e. the number or width of time slots can be altered depending on the number of active devices, or the amount of data they have to transmit. This requires that each device has a receiver in order to listen to

other devices and to receive configuration data. However, this does add complexity to the overall protocol.

Static TDMA frames do not use the channel bandwidth as efficiently as their dynamic counterparts but one of the main advantages of TDMA is that once a good synchronisation point is obtained, it is a simple and reliable protocol to implement.

A final, important feature of TDMA is guard-bands. These are transmission free periods padding the time slots as shown in figure 2.13. They guard against a possible drift in synchronisation. They also cater for a tolerance in the timing between different devices. However, guard-bands increase the duration of the time slot, increasing the overall latency for the system.

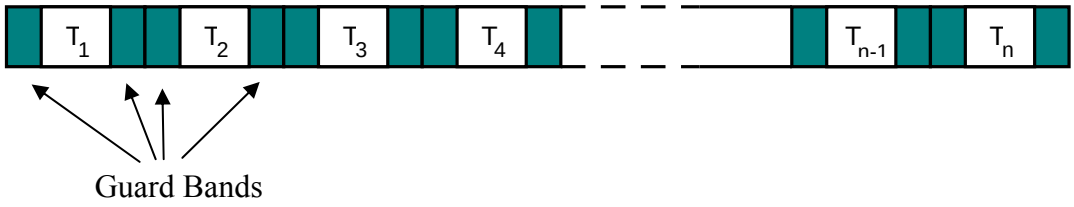


Figure 2.13: TMDA guard bands

2.5 Radiolocation

Radiolocation is the ability to locate individual radios within the specified network area, enabling the tracking of assets and children. This typically uses some form of measurement from the RF signal to resolve location. This can be the receiver signal strength indicator (RSSI), the angle or time of arrival of the RF signal, or some form of directional system. However, radiolocation is not possible without a fixed reference point (a known location).

Radiolocation can be based on transmissions from the radio node to be located. A typical example of this is the cellular network. When a signal from a mobile phone is

received by one or more antenna masts then the position of the phone can be inferred, see figure 2.14. Reception by a single antenna can indicate a rough proximity to the antenna based on signal strength. A more accurate location measurement is possible when multiple antennas (3 or more) receive the phones signal. The multiple signals can be used to triangulate the position of the phone.

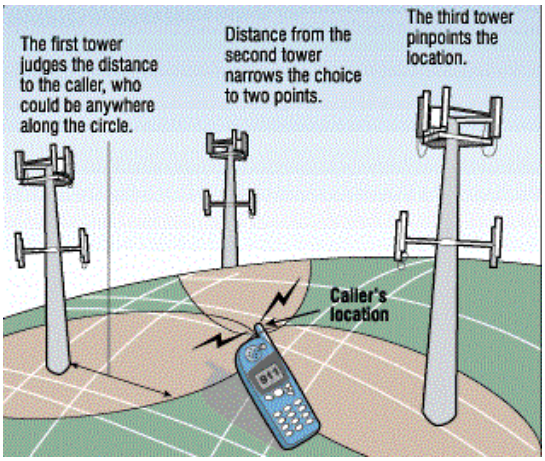


Figure 2.14: Diagram of cellular triangulation
(Image from http://www.al911.org/)

However, nodes can also discover their own location. Global Positioning Systems (GPS) provides a solution for this. Once a node knows its own location it can then use this information, for example, in a GPS Satellite Navigation device. Other applications may require the device to report its location. An example of this would be fleet vehicle tracking where the nodes location would be radioed back to a central station, typically via a cellular network.

GPS is also used for the application of locating children. There are a number of devices on the market, two of which are the Amber Alert GPS Child Locator (Amber Alert 2010) and the Nu.M8 GPS Child Locator (Nu.M8 2010). Both these devices are worn by the child. The Amber Alert, figure 2.15(a), can be worn on a wrist, on a belt, or in a pocket. The Nu.M8 is in the form of a wrist watch, see figure 2.15(b). They both incorporate a GPS receiver for position and a GSM/GPRS modem to send this location information to its destination.

The main advantages of these devices include:

- The accurate global position reporting.
- Used as a single stand-a-lone device, i.e. no need for additional equipment.
- The GSM/GPRS modem can be used for additional features such as emergency calls.

These GPS trackers do however have a number of disadvantages. The information sent by these devices is GPS longitude and latitude coordinates. These coordinates must be used with mapping software in order for the user (parent or guardian) to make sense of them. To facilitate this, the devices report their GPS coordinates to a central monitoring station which then posts the position on a map, such as Google Maps, which can then be accessed over the internet. This therefore means that the user must have access to the internet.

(a) **(b)**

Figure 2.15: GPS Child Locators – (a) Amber Alert (b) Nu.M8
(Amber Alert 2010; Nu.M8 2010)

Other disadvantages include:

- There is usually a requirement to pay a monthly subscription to a service provider for these devices
- In order to incorporate all the necessary equipment, i.e. the GPS receiver and GSM/GPS modem, these devices tend to be uncomfortably big for small children to wear on their wrists, as in figure 2.15(b).
- Battery life is short, in the order of a few days
- Interference and lack of coverage is also a problem with GPS receivers. Signals are often unable to penetrate through objects such as buildings.

Even though the GPS and Cellular networks employ very sophisticated radio systems, the basis for radiolocation remains the same for low powered radio networks, such as the wireless mesh sensor network described in this thesis.

2.5.1 RSSI

The RSSI (Received Signal Strength Indicator) is an attractive option to use in radiolocation because of its ease of implementation. However, it is limited due to its poor performance in range measurements. The RSSI output is not always a linear scale, in practice, for a number of reasons. Many low end radio devices implement a stepped response to signal strength offering little accuracy in terms of linear distance measurements. Another factor effecting RSSI accuracy is physical obstructions in the path of the RF signal, which also reduces the RSSI. It is very difficult to then determine if this reduction is due to distance, or in fact an obstruction. A radio device attached to a person will encounter many obstructions when transmitting to a receiver due to the mobility of the device. The person's body itself will become an obstruction at times depending on orientation to the receiving point.

2.5.2 Time of Arrival

The time of arrival of a signal (TOA) is a much more accurate measurement of distance. However, as radio signals travel at the speed of light, accurate measurement require fast processing speed at the receiver.

GPS receivers use this technique to calculate their positions. They require communication with at least three satellites to triangulate latitude and longitude position, and a fourth if altitude is required. To have an accuracy of 1 meter, the GPS receiver must be able to resolve the time of arrival of signals from each satellite to an accuracy of just over 3ns.

Trying to implement this technique with low end 8 bit MCUs would be difficult. GPS requires a clear signal path between the receiver and the satellites. Implementing ground level time of arrival measurements in built up areas would also have to contend with signal reflections which can cause multipath distortion of the signal.

A more recent development in tracking for indoor and built up areas is the use of Ultra Wide Band (UWB) transceivers. UWB is a technology for transmitting information spread over a large bandwidth (>500 MHz). UWB uses very short pulse signalling over a very wide spectrum of frequencies of this large bandwidth. This enables the receivers to measure TOA of a signal to sub nanosecond precision.

Reception by three or more receivers permits accurate 2D localization, while reception by four or more receivers allows for precise 3D localization. If only one or two receivers can receive a transmission from a mobile device (typically referred to as a Tag), proximity detection can also be readily inferred.

Figure 2.16 shows an example implementation of tracking using UWB radios. Four base stations are strategically positioned to provide cover for a desired area or cell. The position of the four base stations are fixed and known. The position of a mobile unit (Tag) can be triangulated by the difference in time of arrival (DTOA) of the signal from the tag to the base stations. In order for this to work the base stations must be accurately synchronised and share the DTOA with each other.

The Tag may also triangulate its own position in the cell by calculating its distance from at least three base stations.

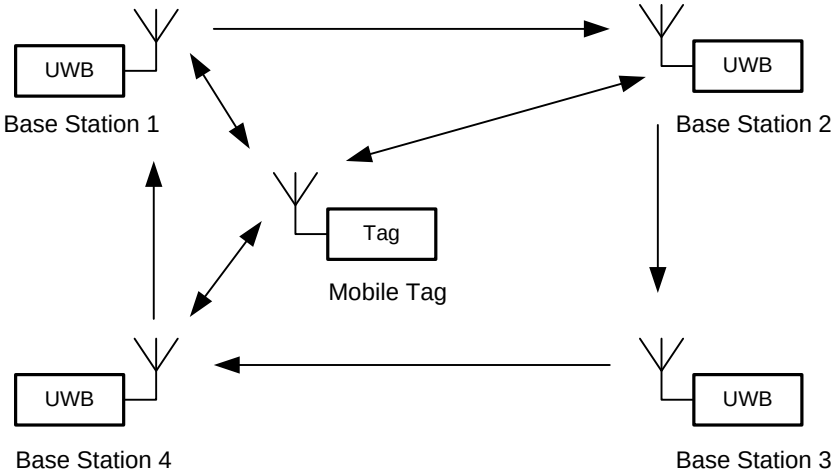


Figure 2.16: Diagram of UWB tracking setup

One of the advantages of UWB is its tolerance to multipath distortion in built up areas. It accomplishes this by suppressing the short pulse signal reflections, which arrive at the receiver after the direct signal, as shown in figure 2.17.

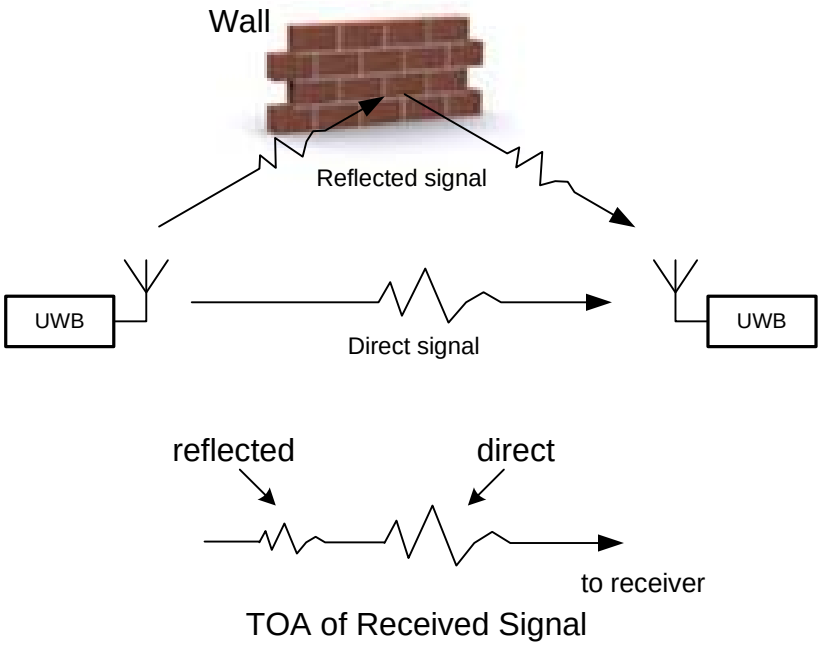


Figure 2.17: UWB TOA of direct and reflected signals

Radiolocation may also be accomplished by using a combination of direction and signal strength. The signal strength gives a rough estimate of distance while directional antennas or antenna arrays enable the direction of the signal to be obtained.

Some radiolocation techniques do not require that the location of the radio is obtainable at all times. The use of radio bounded (or fenced) and exclusion areas only require that the systems knows when a radio device is inside or outside a designated area. Other systems use short range radio systems, placing receivers at fixed positions. The location of a device is known when it passes one of these fixed positions. Some examples of these will now be discussed.

2.5.3 Asset tracking and stock management

RFID (radio frequency identification) uses radio waves to identify individual items. There are two types of RFID tags, passive and active. Passive tags do not have an internal power source. Instead they are activated by a reader which induces a small current into the tag which in turn powers the device. A passive tag is shown in figure 2.18. Once powered the passive tag sends a unique RF encoded identification to the reader.

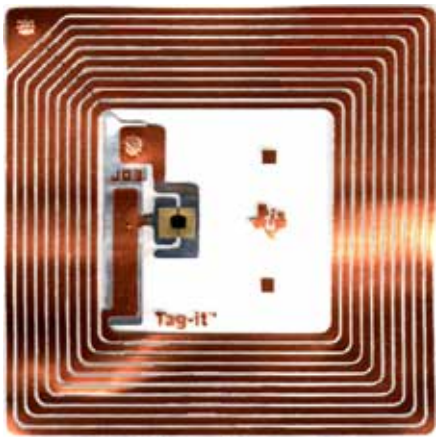


Figure 2.18: Picture of Texas Instruments Tag-it Passive RFID Tag
(Image from http://www.sagedata.com/)

Passive RFID has a typical operating range of a few centimetres. Due to their very low cost and paper thin dimensions, passive RFID tags are set to be a replacement to barcode identification. Their advantage over optically read barcodes is that they do not need to be optically visible to the reader. Passive RFID can be made to operate up to a maximum distance of a couple of meters. This may be required if passive RFID tags are to be detected while passing through a doorway. To achieve this, the RFID reader must emit a powerful RF signal to energise the RFID tag. When greater distances are required for RFID then Active RFID tags can be used.

Active RFID tags are self powered devices capable of transmitting up to a couple hundred meters. They are in effect low power licence exempt radios. These tags make it possible to monitor the presence and quantity of items in a location such as a

warehouse. This may not be practical however due to the relatively high cost of the active tag compared to the passive tag. A more typical application of Active RFID is for barrier-free electronic tolling of roads and bridges. Figure 2.19 shows a picture of an electronic tolling device placed on the windscreen of a car. This device is activated when it comes into proximity of the tolling point. Once activated it transmits a unique code associated to the vehicle it is assigned to.

Figure 2.19: Active RFID electronic road toll
(Image from http://www.thefullwiki.org/RFID)

Radio fence

These systems use radio signals to set an invisible wireless boundary. They operate by having a central stationary radio unit monitor one or more mobile units. While the mobile units are within range of the central unit, they report there presence. This can either be on a timed regular basis, or by the central unit polling each mobile unit for a response. If a mobile unit fails to report its presence, then some action is usually taken, e.g. an alarm can be activated.

These radio systems are typically omni-directional, giving 360 degree coverage. Therefore the position of the central unit is important and should be at the centre of the desired coverage area. These systems can cover areas up to 100m to 300m in diameter, depending on the radio range. This can also be reduced to a desired smaller area as shown in figure 2.20, where the radius of the wireless fence is shown as 30m (diameter 60m).

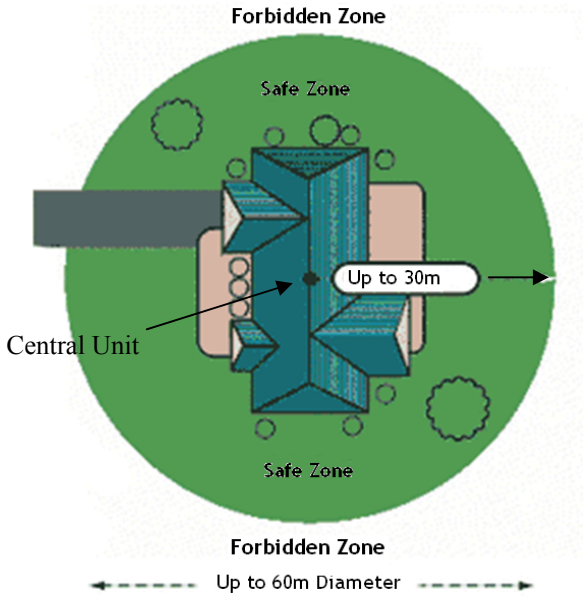


Figure 2.20: Wireless boundary fence
(Image from http://www.radiofence.com)

ionKids Child Monitor

This product is another example of a wireless boundary fence. However, it this case, both the central unit (parent unit) and the monitored unit (child unit) are both mobile.

Figure 2.21 ionKids parent and child units.
(Image from http://www.ion-kids.com)

The parent unit is a hand held device and the child unit is in the form of a wristwatch, see figure 2.21. The parent unit is capable of monitoring up to four child units at any one time. The parent unit can set a wireless boundary for the child unit up to a maximum of about 150m. This distance is based on the receive signal strength from the child's unit. When a child unit goes beyond the set boundary an alarm is sounded. The alarm will also sound if the child unit is removed without a special key.

The ionKids monitor also includes a "find mode". In this mode the parent unit switches to maximum range (beyond the boundary range) and provides directional information of where the child unit is transmitting from.

2.6 Energy Scavenging

Wireless sensor nodes are often deployed with no possibility of an external power source. They rely on batteries or some other form of energy supply, such as energy scavenging, or a combination of both. As energy scavenging will be used in the final design and implementation of the proposed wireless mesh sensor network, this section provides an overview of the technology.

Energy scavenging or harvesting is the process of extracting power from the environment without having any adverse effect on the environment. This can be renewable sources such as wind and sun, or it can also be "free" resources. These "free" resources would include the use of vibrations from an industrial machine to power a sensor, for example. This sensor could then take temperature measurements from that machine. An example of such a device is the AdaptivEnergy Joule-Thief™ Module shown in figure 2.22. This miniature vibratory energy harvesting module is based on piezoelectric technology and is ideal for battery life extension or replacement in wireless machinery monitoring.

Figure 2.22: AdaptivEnergy Joule-Thief™ Module
(Image from Mouser Electronics)

Another "free" resource is the harvesting of energy from the many RF signals which surround us. Although the term energy scavenging can be applied to any scale of energy collection, when discussing wireless sensor networks it is normally associated with very low power generation. This can be in the order of milliwatts and in some cases even microwatts.

Up to a few years ago the idea of an energy scavenging micro-generator producing microwatts or a few milliwatts didn't have any applications. However in more recent years, with the advances in ultra low power technology, these micro-generators have many applications including powering nodes in a wireless sensor network.

In some cases the power produced by these micro-generators is not enough to power a device directly. In these cases the power is accumulated in batteries or capacitors until it reaches the required level. Once this level is reached the device can then activate. In the case of a wireless sensor node this activation could be the powering of the device, the sensor measurement and the transmission of data. These actions would partially or fully deplete the accumulated energy and therefore the cycle of replenishing this energy would start again. Figure 2.23 shows a block diagram of the required stages from harvesting an energy source to delivery of power to the end device.

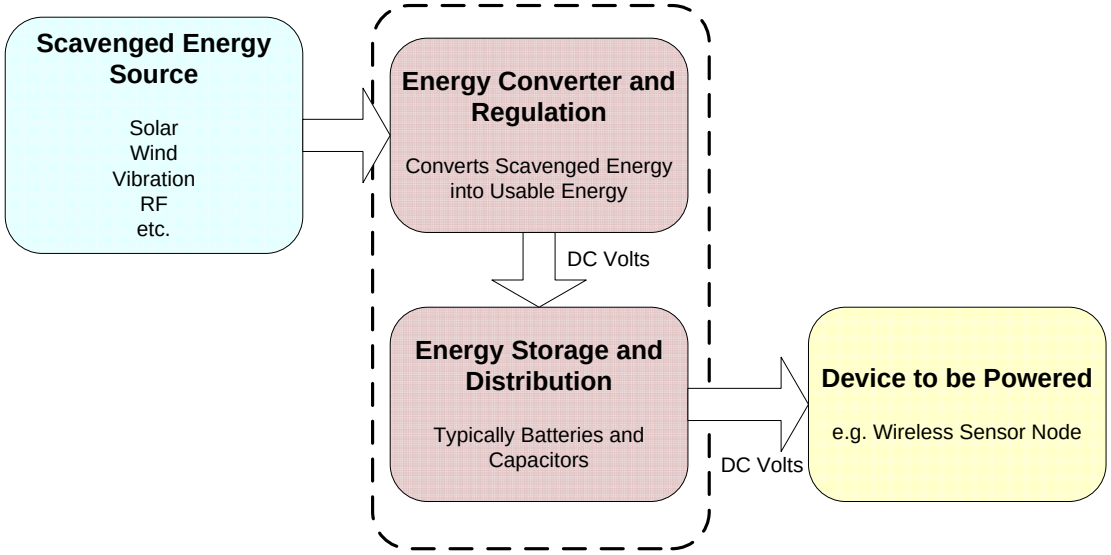


Figure 2.23: Energy scavenging block diagram

One of the most common sources of energy scavenging is the use of small solar panels. These are simple, reliable and have no mechanical moving parts. They do however require daylight. Hence at night, or in badly lit areas, these devices produce no power. Wind is another common source of renewable energy. Micro windmills are available for providing low power harvesting solutions. Unlike solar energy, wind can produce energy both day and night but only if there is wind. Energy generation by wind or solar, or a combination of both, can not guarantee a twenty four hour continuous power source. If continuous powering of a device is required then the following method is a possible solution.

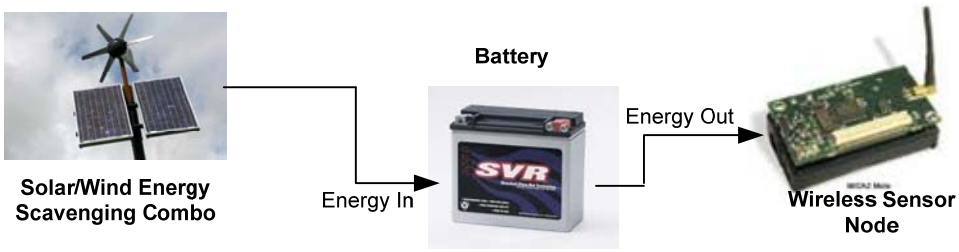


Figure 2.24: Diagram of combined wind/solar solution with charging battery while operational

In figure 2.24 a battery is charged by a solar/wind energy harvesting device. The battery then in turn provides power to a wireless sensor node. If the energy into the battery is greater than the energy required to power the sensor node, then the battery will be charged while powering the sensor node. The battery can then accumulate enough energy to continue powering the sensor node when both sun and wind are absent. If this system is designed correctly, this method can provide twenty four hour continuous power to the sensor node.

2.7 Deployment

The methods and strategies for deployment of wireless mesh sensor networks are very diverse and depend greatly on the application. Wireless sensor network deployment strategies aim in achieving maximum sensing capabilities while minimizing costs, conserving power and achieving a high level of reliability. Strategies for deployment of nodes are not only concerned with meeting the requirements of connectivity, they are also employed to meet the sensing coverage requirement of the network. They

also try to minimize the number of sensors required to satisfy the system. Therefore, sensor deployment strategies play a significant role in determining the appropriate placement of sensor nodes to meet coverage requirements (Zou and Krishnendu 2003).

In this section a general overview of two basic deployment strategies are discussed, namely, pre-planned, deterministic, deployment and random deployment of wireless sensor networks.

2.7.1 Deterministic Deployment

One of the basic criteria for deployment of wireless mesh sensor networks is that each node must be in RF range of at least one other node. However, one of the reliability aspects of wireless mesh networks is the redundant paths for data transfer. Therefore it is important to ensure mesh nodes have at least two connection paths. With deterministic deployment this can be achieved with the correct planning.

Deterministic deployment is ideally suited when network deployment remains unchanged. Research has shown that one of the optimal patterns for deterministic deployment is a triangular lattice (Bai et al. 2006). Figure 2.25 shows three deterministic deployment strategies based on grid placement over a region of interest (ROI), including the triangular lattice method.

Reducing and enlarging the grid spacing can control the level of sensing granularity. This however, can have an effect on power consumption. The further the nodes are spaced apart the larger the transmission hop which in turn requires more power. The closer the nodes are placed together the finer the sensing resolution. However, this does require a greater the number of nodes to monitor a ROI. This also can have a significant impact on cost.

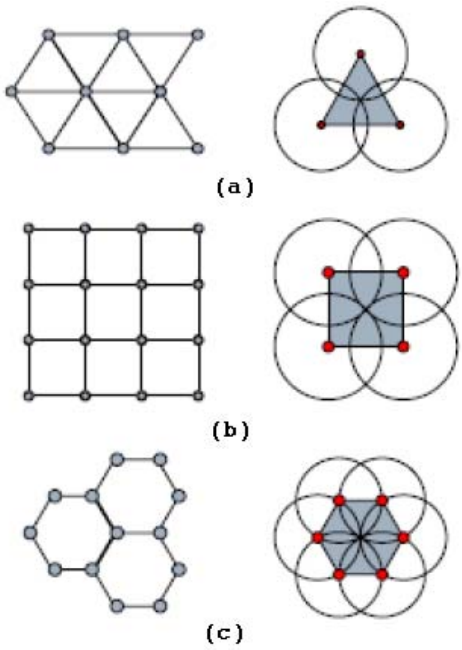


Figure 2.25: Grid deployment (a) triangular lattice (b) square grid (c) hexagonal grid (Aziz et al. 2009)

In theory grid deployment would be the best way to monitor a ROI, both from a sensing and communications aspect. In practice however, it can suffer from sensing and radio irregularities. Sensors do not always exhibit the same sensing range, and in some sensor networks individual sensor nodes may have different types of sensors on board. This can lead to irregular sensing patterns which can cause gaps in grid sensing coverage (Aziz et al. 2009). There exists a similar situation with radios. Not all radios will exhibit the same omni-directional radio range (often portrayed as a circle around a node). Irregularities due to obstructions can greatly alter the RF footprint of a wireless sensor node. Both these scenarios may require alterations in the grid deployment to fill in gaps.

The key advantages of deterministic deployment include:

- High degree of accuracy by manually placing sensor nodes in a fixed infrastructure.
- In certain situations very reliable and easy to implement.
- Evenly distributed nodes maximises coverage with the minimum amount of nodes.
- Routing tables can be static.

2.7.2 Random Deployment

Deterministic deployment is not always practical or suitable for wireless sensor networks. Hazardous and inaccessible environments may make the placement of sensor nodes in regular patterns impossible. In some cases sensor are required to monitor from the air, e.g. storm analysis. These sensors are sometimes deployed by aircraft. If these sensors are not tethered together then tight control over the distribution of these sensors is extremely difficult. Therefore, trying to formulate a triangular lattice deployment in this scenario would be impossible.

The alternative is for random deployment of wireless sensor nodes. This is a practical way in placing the sensor nodes in a ROI. However, research has shown that in cases where there is mobility of sensor nodes, random deployment can require up to seven times more sensors than deterministic deployment to provide 100% coverage (Zaidi 2008).

Random deployment is suitable when network topology changes significantly or when there is insufficient knowledge of the ROI. Self registering and configuring nodes can be applied to the ROI on an ad-hoc basis. Random deployment is also practical in military application, where wireless sensor networks are initially established by dropping or throwing (Chen et al. 2009). Randomly deployed nodes may require more complex software compared to deterministically deployed nodes in order to meet these requirements.

In the case of random deployment, a strategy for reliability is to ensure that more than one sensing node is at a point of interest to offer redundancy at that point (Balister et al. 2009). Research (Kumar et al. 2004; Wan and Yi 2006) has examined this in terms of deployment density and k-coverage. *K*-coverage is the requirement that every point in the ROI can be covered by at least k sensors at any time. If nodes were 100% reliable, then $k = 1$ would provide a robust network. As 100% reliability can not be guaranteed, ideally $k > 1$. The higher the value of k the more resilient the network is to node failure (Aziz et al. 2009).
The key advantages of random deployment include:

- Suitable for ROI which are subject to change, e.g. mobile nodes.
- Prior knowledge of coverage area not always required.
- Placement accuracy not required.
- Easy deployment, e.g. can be thrown or dropped as in military applications (Chen et al. 2009).

2.7.3 Cost of Deployment

Cost of deployment varies greatly with the method of deployment. The quantity and cost of the sensor nodes have a significant bearing on the overall cost, especially in cases where the method of deployment is low cost. In other cases the cost of individual nodes can be relatively insignificant compared to the cost of deployment. One example of this is the deployment of sensors from aircraft. Tornado and storm analysis sometimes requires that low cost disposable sensors are deployed from the air in to the storm. The cost of utilizing an airplane can be as much as tens of thousands of Euros, whereas the cost of the sensors could be as little as tens of Euros. Here the deployment can far outweigh the cost of the sensor nodes.

One of the objectives of this research is to realise a low cost system. The initial aim was to develop wireless sensor nodes for less than five Euros each which could be deployed at no extra cost. The cost of deployment and the actual cost of the final sensor node design will be dealt with in chapter 7.

2.8 Standardising Wireless Sensor Networks

Wireless networking is still an emerging technology with many different configurations and implementations. It is for this reason that there are so many routing algorithms currently employed, each one tailored for a different hardware platform and network scenario. Some attempts have been made to provide a global standard in wireless sensor networks. Probably the biggest consorted effort in achieving this is the ZigBee standard.

ZigBee was launched in 2004 (ZigBee 2004) by the ZigBee Alliance, a group of organisations who wanted to standardise a platform for low power ISM radio devices.

Many of the major chip manufacturers are members of this Alliance, including Philips, Motorola, Intel, HP, Texas Instruments and Microchip.

ZigBee is based on the IEEE 802.15 standard for wireless personal area networks (WPANs), in particular the IEEE 802.15.4 standard of 2003. The WPAN standard was originally developed for applications such as short range wireless headphones. As Bluetooth, also based on IEEE 802.15, had already being developed and looked likely to corner the market in products such as wireless headsets, ZigBee was targeted towards low cost, low data rate and low power applications, not in competition with Bluetooth. This made the ZigBee standard ideally suited for sensor networks. The ZigBee standard has been slow to establish itself and it is only in the last couple of years that ZigBee is gaining real momentum.

The ZigBee protocol standard is constructed as shown in figure 2.26. The ZigBee specification contributes the network layer and application layer while the IEEE 802.15.4 standard is responsible for the physical layer and the medium access control (MAC) layer.

ZigBee offers a number of network topologies, including point-to-point, star and mesh connectivity, for its networks. Of these, mesh topology has the advantage of being able to extend the range beyond that of a single radio device.

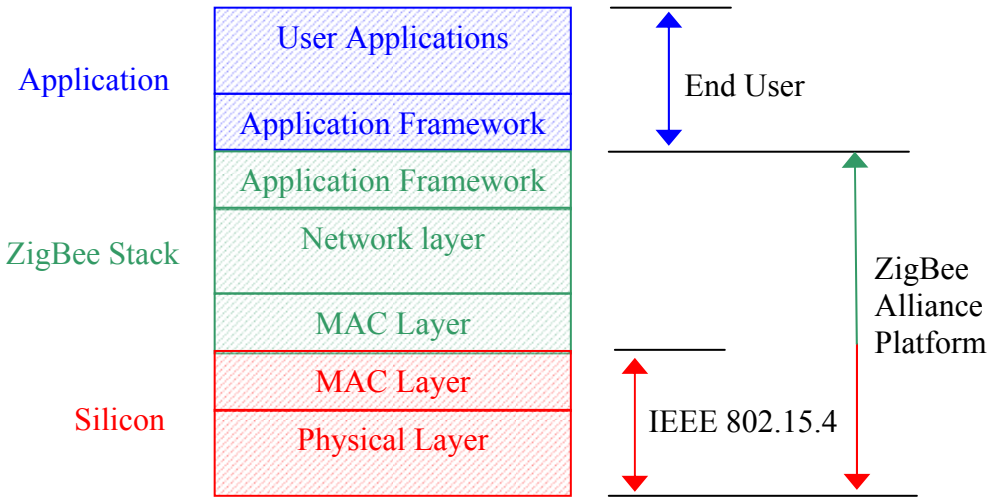


Figure 2.26: Diagram for ZigBee layered protocol stack

ZigBee mesh networks consist of three types of nodes as shown in figure 2.27:

- **Coordinators:** A ZigBee network contains one coordinator node which organises and controls the network and maintains routing information.

- **Routers:** Based on 16-bit addresses it is possible to have over 65,000 routers (and End nodes) in a single ZigBee network. Routers are capable of communicating with all other devices in the network and therefore can route data in any direction.

- **End nodes:** These devices are effectively reduced function routers. They can communicate with the coordinator and router nodes, but not with other end nodes. The advantage of the End nodes is that they can remain in low power mode (sleep) until they are required to send data, therefore consuming less power than the other devices.

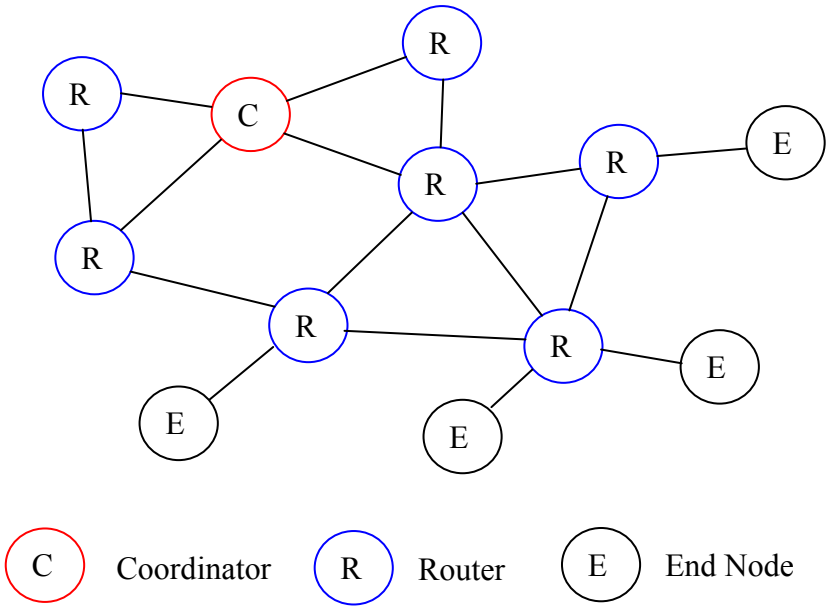


Figure 2.27: ZigBee network configured in a mesh topology

ZigBee routing is based on Distance Vector (DV). Each ZigBee router maintains a routing table entry for each route it can perform. This table stores the "logical

distance" to the destination and the address of the next router in the path to that destination. Routes are established on-demand using a route discovery process (Daintree Networks 2010).

The ZigBee standard has been developed to meet many sensor network requirements. The adoption of a distance vector routing algorithm is an example of this. This type of algorithm is the best compromise for all network configurations and deployments, suitable for both static and mobile networks.

While the ZigBee standard exists, the proposed WMSN avoids using this or any other standards for two main reasons. Firstly to avoid having redundancy that standardisation would introduce. Secondly to obtain a flexible, streamline solution, for the system design. The next chapter will now present an overview of the system design.

Chapter 2 has provided a general overview of wireless sensor networks, wireless mesh networks, MAC protocols and routing algorithms. It has also presented background information on radiolocation, energy scavenging and deployment of wireless sensor networks. This chapter has concluded with a look at a significant attempt to standardise wireless sensor networks with the ZigBee standard. The remaining chapters of this thesis now focus on the design and implementation of the proposed wireless mesh sensor network.

3. SYSTEM DESIGN OVERVIEW

The proposed housing community wireless mesh sensor network is presented here. This chapter discusses some of the applications and benefits this system could support. This chapter examines the requirements of the system and outlines a design to meet these requirements. The main part of this chapter presents a high level overview of the main building blocks of the system. Detailed design of these building blocks will be presented in later chapters.

3.1 Targeted Applications and Benefits

The proposed WMSN will be able to perform the following tasks:

- **Oil tank monitoring:** Oil level sensors can be deployed to report low levels of home heating oil in tanks. This data is then relayed to the base station. The base station can then make this information available to the house owner via SMS or to an oil supplier over the internet.

- **House alarm notification:** A sensor node can be used to detect when a house alarm is activated. This information can then be passed to the house owner or to a nominated third party.

- **Radio Tracking:** The system can be used for locating assets and people, for example the location monitoring of a child. Details of the tracking accuracy will be discuss in later chapters.

- **Refuse services:** Some refuse collection services already employ RFID tags to identify bins while they are being emptied. Having prior knowledge of weight, or whether a bin needs collecting, would enable the service provider to manage the refuse collections more efficiently.

- **Personal aid notification:** Some sensor nodes may be used to signal the need for personal aid, particularly in the case of the disabled and elderly.

- **Community lighting:** Public lighting of a housing community is normally overseen by a local governing authority. Sensors could be deployed to detect a faulty light which could then be reported directly to the local authority.

More traditional environmental data can be monitored with the appropriate sensing device. These include:

- **Temperature:** The system will support temperature measurements, for example, greenhouse temperature.

- **Moisture:** Soil moisture can also be monitored in order to determine whether or not a lawn requires watering.

These are a few examples of the applications and benefits the system can bring to a housing community. The proposed system is intended as an addition to existing security or alarm systems and not to replace them.

3.2 System Requirements

Formulating the system requirements is an important stage in any system design cycle. Knowing what is required of a system can greatly improve the design approach and choices. Outlined below are the system requirements.

The system design is based around a wireless sensor network. As mentioned in chapter 2, wireless sensor networks tend to have the following common requirements. They should be low power, contain a sensor or sensor interface and transmit small amounts of data. They should also be low cost, easy to deploy and reliable

Additional requirements for the proposed system include:

- **Radiolocation:** The system should be able to identify the location of any wireless sensor node. The accuracy of the radiolocation should be capable of determining the location to within a single property or a single location in a housing estate.

The single property would include a house and garden. The single location could include a playground or playing area; a community shopping centre; or a *no-go* area.

- **Single Destination point for data:** All sensors send their data to one central point, the base station. This will greatly simplify the requirements of the routing algorithm.

- **Ease of maintenance:** Maintaining the system should be achieved centrally, therefore the base station must be capable of determining if maintenance is required. Individual householders should not be required to monitor the system for maintenance. If maintenance is required the base station will take action or inform the appropriate party.

- **Scalability:** The system should cater for a range of housing estate sizes, from small estates comprising of tens of houses, to large estates with hundreds of houses, without having a detrimental effect on the system's performance.

- **Extend the RF range beyond that of a single radio device:** In order to transfer data over varying distances and objects, wireless nodes should be able to relay data to a destination. A partial mesh network is used for this.

- **Easy access to sensor data:** The base station will store all sensor data. Access to this data will be via SMS or Web Access.

3.3 Design approach

The design methodology adopted for this system is that of an application specific approach. The main advantage of an application specific approach is designing a system to solve one particular task and not designing a generic system which can be

applied to number of varied system applications. By taking this approach the design becomes more focused on solving the task at hand.

The design should also allow for software and hardware modifications to any aspect of the system. This approach requires, as far as possible, a discrete implementation of the system, avoiding major standards. Adopting standards such as Wi-Fi, Bluetooth, ZigBee or RFID will introduce features and performance overheads that are surplus to requirement. They will appear as black boxes in the system design, with no possibility of modifying their internal operations.

The adopted design approach incorporates proprietary licence exempt radio modules. The design will ensure that these modules are easily interchanged with other compatible modules in order to maintain flexibility in the system configuration and implementation. The processing and control will be provided by microcontrollers and embedded software. Together the radios and microcontrollers form the main building blocks of the system, namely the wireless mesh nodes and the wireless sensor nodes.

3.4 System Topology

Figure 3.1 below depicts a typical network topology of a wireless mesh sensor network deployment, arranged in a partial mesh configuration. It should be noted that the inter-connecting lines are representing wireless radio paths.

Like most wireless sensor networks the sensor is integrated directly into the wireless mesh node, or associated with a particular node through the use of an electric tether. The configuration of the system presented in this thesis is somewhat different. The system consists of both wireless mesh nodes and wireless sensor nodes (see figure 3.2). The sensor nodes are intelligent wireless devices capable of sending data to any/all mesh nodes in radio range, thus allowing for greater flexibility in sensor deployment.

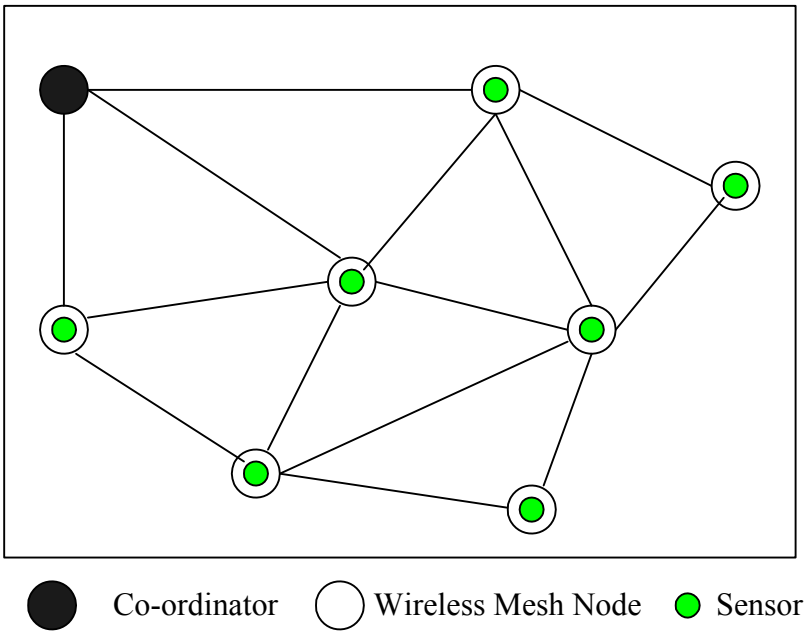


Figure 3.1: Typical sensor network topology

Unlike typical mesh sensor networks, where the sensor is part of the mesh node and thus have inherent bi-directional radio communication, these wireless sensor node devices have transmit-only capability for data. The directional lines in figure 3.2 represent the transmit-only radio links between the wireless sensor nodes and wireless mesh nodes.

3.5 Mesh and House Nodes

The mesh and house nodes form the wireless mesh network. A set of wireless mesh nodes form a fixed infrastructure, giving full coverage of the region of interest (ROI), the housing estate. Additional house nodes may be added and removed on an ad-hoc basis. These additional nodes can be used for extending the coverage area, or for more accurate coverage of the area with regard to radiolocation. These ad-hoc additional nodes will act as end clients and do not route data packets from mesh nodes.

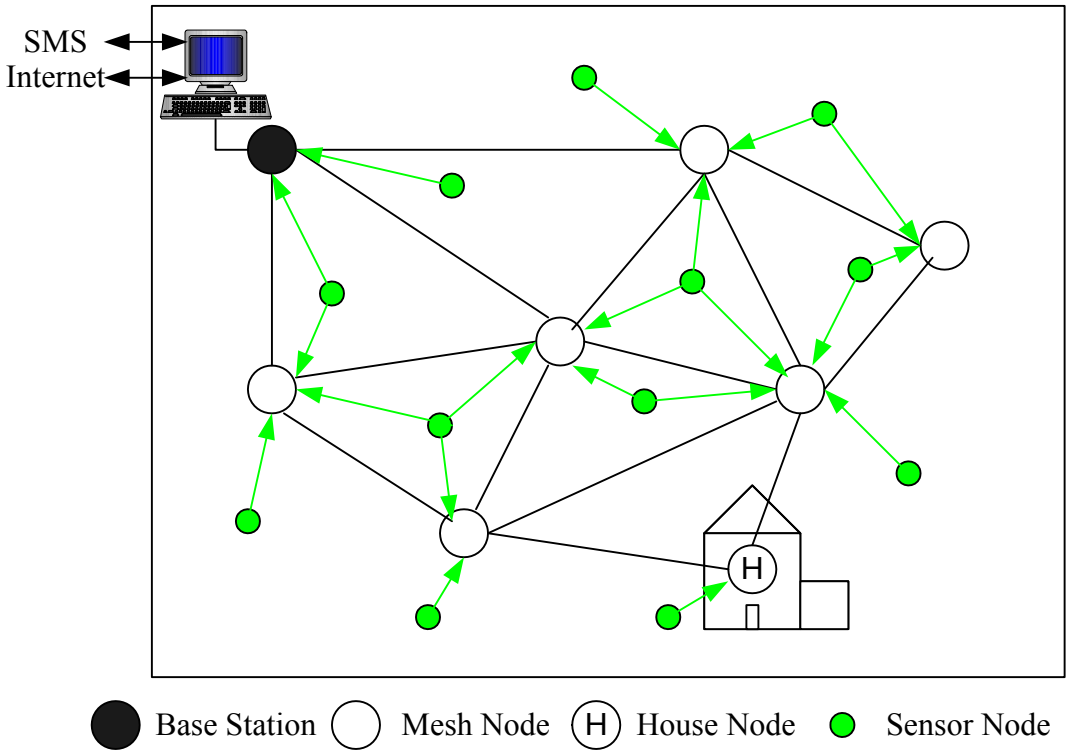


Figure 3.2: Proposed sensor network topology with wireless sensors

The intelligence of these nodes is provided by the software/algorithms running on microcontrollers. Each node also contains a radio transceiver. The frequency chosen for interconnecting mesh nodes is the licence exempt pan-European 868 MHz band. A more popular choice of radio frequency is, arguably, the 2.4 GHz band. However, with many various radio devices already operating at the 2.4 GHz band, including Wi-Fi, it was decided to opt for this less used radio frequency, in order to reduce the possibility of radio interference. The design of the mesh and house nodes allow for easy substitution of radio modules so that the system is not fixed to one frequency.

The mesh node also contains a dedicated radio receiver for the sole purpose of receiving data from the sensor node. This receiver will operate at one of the licence exempt ISM frequency bands, e.g. the 433 MHz band. Figure 3.3 shows a block diagram of a mesh (/house) node.

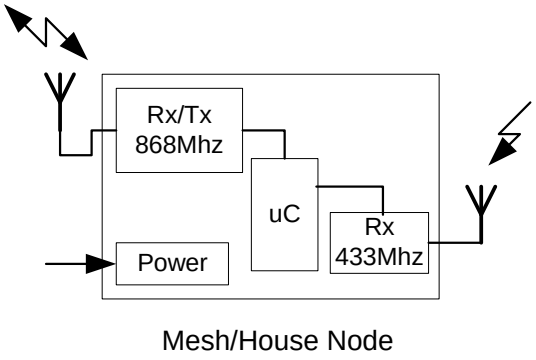


Figure 3.3: Mesh node block diagram

The main purpose of these nodes is to collect data from the sensor nodes and pass this data to the base station (the single destination in the network) in the most efficient and reliable way. Only data which is needed to be relayed will be sent by a wireless mesh node, all other data will be stripped off. Periodically, the wireless mesh node will be required to send its own housekeeping data in order for the base station to monitor the status of the node. An overview of the data packet structure and routing will be presented later in this chapter.

3.5.1 Physical Deployment of the Network Infrastructure

The layout of housing estates and communities are, in general, conducive to a deterministic network deployment. It is proposed to mount infrastructural mesh nodes on rooftops and high-up on lamp posts. This greatly reduces physical obstruction to radio communications. In addition, large open areas in housing estates have little or no electrical radio interference. It should therefore be possible to deploy the nodes in some form of a regular grid pattern.

Mesh nodes do not contain a sensor, so sensing range in not an issue. The placement of these nodes is only concerned with RF range. One aspect to the placement of these nodes is to ensure that each node is in RF range of at least two other nodes. This is to provide the option of alternative routing paths to the base station, if needed. A more critical aspect to wireless mesh node placement and one that has a significant effect on mesh node density (or granularity), is the placement in relation to wireless sensor nodes. The strategy here gives rise to a number of trade-offs.

Coarse granularity of infrastructural mesh nodes results in larger distance between the nodes and has some of the following advantages:

- Fewer nodes required for the ROI.
- Less cost.
- Less physical effort in deployment of mesh nodes.
- Lower data latency due to fewer hops.

Fine granularity of infrastructural mesh nodes results in smaller distance between the nodes and has some of the following advantages:

- Better radiolocation resolution.
- Shorter distance between nodes requires lower transmit power between mesh nodes.
- Continuous mobile sensor node coverage possible.
- Sensor node range can be reduced, saving power.

A model for a housing estate with the following specifications is adopted for the purposes of illustrating a system deployment.

Approximate size of housing estate	:	300m x 300m
Number of houses	:	~220
Mesh node grid deployment separation	:	50m
Number of Mesh Nodes	:	49
Number of sensor nodes (6 per house)	:	~1320

Figure 3.4 depicts a grid deployment of mesh nodes spaced at 50m apart with the base station deployed at any point on the grid. This would be a good compromise in terms of transmission distance and routing options between mesh nodes.

Figure 3.4: Regular grid pattern deployment of Mesh nodes

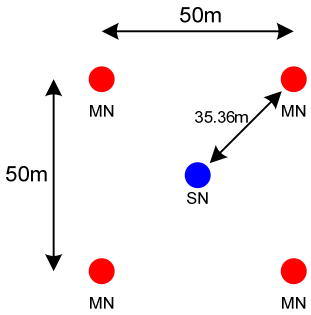


Figure 3.5: Maximum distance of sensor node (SN) from mesh node (MN)

The grid deployment of figure 3.4 ensures that the maximum distance between a sensor node within the grid and a mesh node is approximately 35.36m as shown in figure 3.5. In this case, static sensor nodes are required to have a transmit range of greater than 35.36m. If continuous monitoring of mobile sensor nodes is required then

these also must have the same transmit range. This guarantees that sensor nodes will be in range of at least two mesh nodes at any time, once they are within the grid.

In practice, precise grid deployment may not be practical or even possible. Not all housing estates are uniformly laid out. Available mounting points for mesh nodes may not be conducive to a grid pattern deployment. Furthermore RF range is never a constant.

To verify the proposed system as described in figure 3.4 would require 49 mesh nodes. The final implementation adopted two schemes in order to reduce this required number of mesh nodes. A system consisting of 4 mesh nodes and a base station was set up in a housing estate. These mesh nodes were deployed approximately 50m apart as in figure 3.5. This system was primarily used to test radiolocation aspects of the system. The second scheme consisted of 8 mesh nodes and a base station and was deployed in the Electronic Engineering building at NUI Maynooth. This network served as the main test platform for the verification of the system. Further details of the implementation and testing of the system will be presented in chapter 7.

3.5.2 Mesh Routing Algorithm

The mesh nodes route the sensor data back to the base station. These nodes have little or no mobility as they will be deployed in a fix infrastructure. Therefore the system is suitable for implementing a simple proactive routing strategy. The nodes will maintain routing tables. These tables will be ordered in terms of the best route to the base station, determined by the number of hops required. As the nodes have no mobility, once the route is determined it will always be the same for individual nodes, while all mesh nodes operate correctly. If a route is blocked, the next route from the table will be taken.

The routing tables are established once all mesh nodes are in place. The nodes are set to a ‘discovery mode’. Once in this mode, a broadcast is sent by the base station to all nodes in range. The nodes which receive this broadcast set their hop count to 1. These nodes then rebroadcast the signal. This is done at slightly different times in order to avoid data collision. The nodes that receive this broadcast (and don’t have a hop

count) set their hop count to 2. This continues until all nodes have a hop count. Figure 3.6 depicts this scenario. The numbers in the boxes indicate the hop count to the base station (BS). The circle around each wireless mesh node (WMN) represents the RF range of that node. All nodes with the same hop count are represented by the same colour. Once done, all nodes report back to the base station with their hop count number in order to verify the creation of the mesh network.

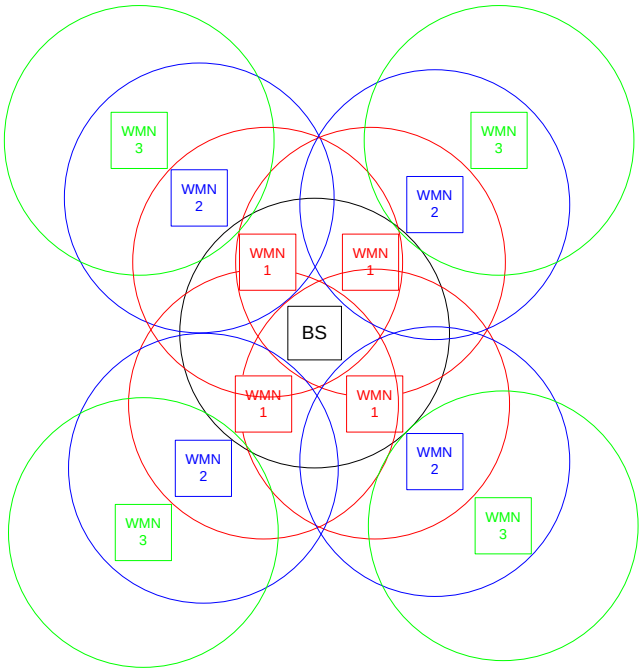


Figure 3.6: Diagram of mesh node hop allocation

This facilitates a very simple routing method. With the information about adjacent nodes stored in tables, data is simply sent to an adjacent node with the lowest hop count. If this route is blocked the next route in the table is used.

3.5.3 MAC Protocol

The MAC protocol for the mesh nodes is based on CSMA. Figure 3.7 shows a basic flowchart for the proposed MAC protocol.

The MAC protocol here is very simple. When a mesh node wants to send data it uses the receiver signal strength indicator (RSSI) from its radio to determine if any other mesh node within radio range is currently transmitting. If the radio channel is clear the mesh node starts transmitting immediately. This then reserves the radio channel for

the complete transmission of its data. Once the data has been transmitted the mesh node waits a finite time for an acknowledgement from the receiving node. The transmission sequence ends when the acknowledgement is received. If no acknowledgement is received after three attempts, the failed flag is set and this will alert the node to try an alternative route next time.

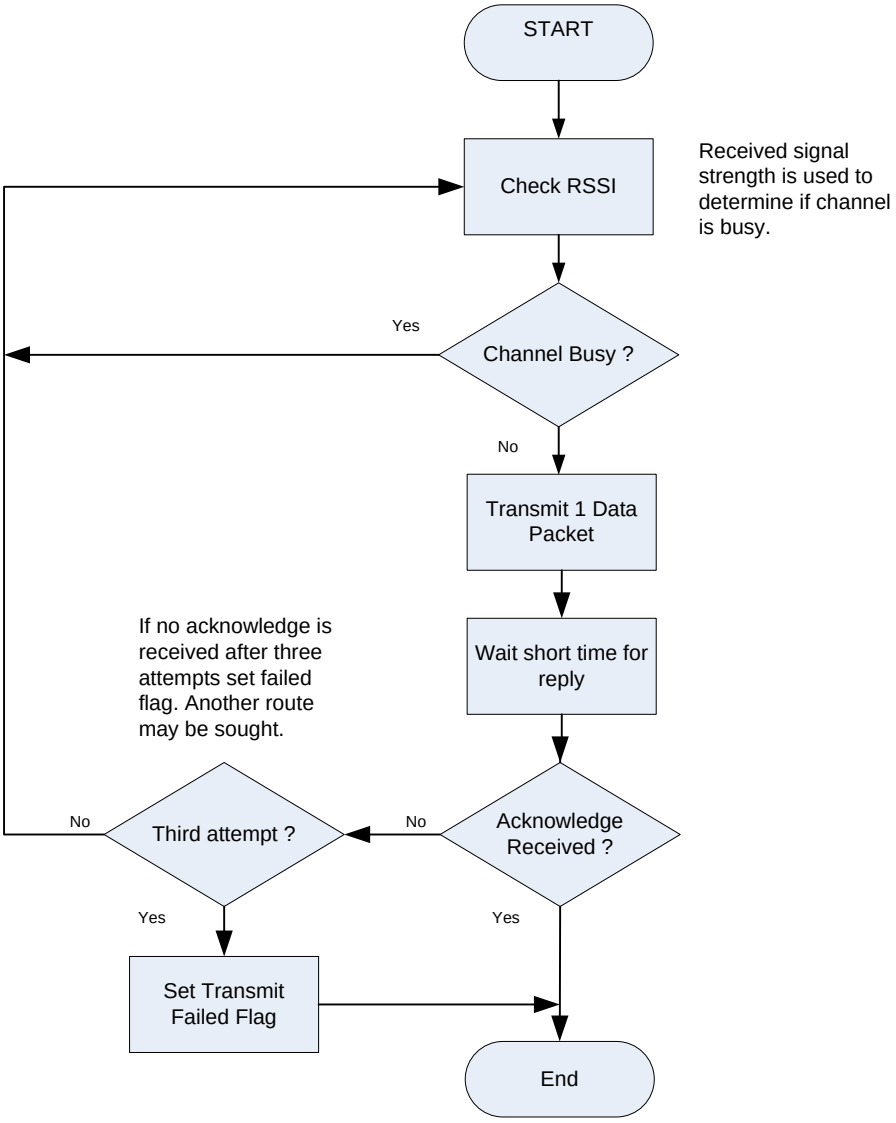


Figure 3.7: Mesh Node MAC protocol

3.5.4 Power

The wireless mesh nodes are required to be powered continuously 24 hours a day. Mains power will not be available for outdoor infrastructural mesh nodes. therefore these nodes must be powered by a combination of rechargeable battery and energy scavenging. The positioning of the mesh nodes on roof tops and on lamp posts, make them ideally sited for scavenging power from natural resources such as sun and wind.

The design of these nodes, allow for the use of solar and wind as a supplement power source. The design of this power source for the mesh nodes requires careful consideration. The power system must be designed to cater for the worst case scenario, i.e. the continuous powering of the device during short winter days with little or no wind. Extensive testing has been carried out on the use of solar scavenging. The results of this testing will be presented in chapter 7.

The house nodes, due to their proximity to the house electricity supply, are intended to be powered by domestic supply. They also contain a rechargeable battery to ensure the device remains operational in the event of a loss of power.

As part of their housekeeping data, both mesh and house nodes report the status of their batteries.

3.6 Wireless Sensor Nodes

The wireless sensor node is a battery powered single channel wireless device. The main function of this device is to read sensor inputs and transmit the results to a mesh node. The sensor node contains an rfPIC12F675 transmitter (rfPIC Datasheet 2010). The rfPIC12F675 is both a microcontroller and an RF transmitter integrated into one package. This device provides the intelligence and radio transmitter capabilities of the sensor node in a very small footprint.

The wireless sensor node may incorporate on-board sensors. It also includes a sensor interface to enable external sensors to be attached. This node can also be deployed as an active RFID tag. In this case the wireless sensor node will transmit a unique identification code only. Transmitting this information alone is sufficient for the purpose of radiolocation. For this reason there are two variants of this node, namely a mobile device used mainly for radiolocation and a static device used to monitor sensors at fixed locations (see figure 3.8).

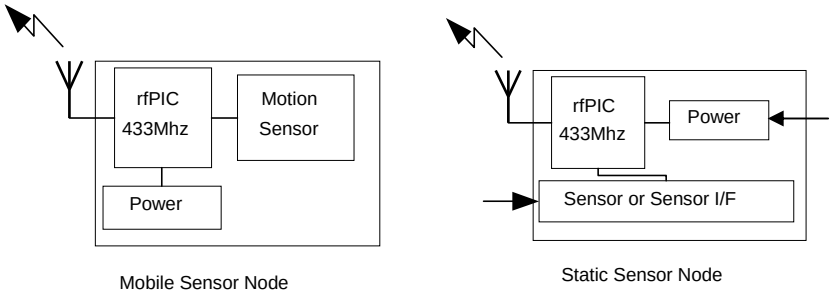


Figure 3.8: Block diagrams of both mobile and static sensor nodes

The two variants of the wireless sensor node are based on the same hardware platform. The differences between the two are given in table 3.1 below.

Feature	**Mobile Wireless SN**	**Static Wireless SN**
Activation	Movement Only	Event driven, Timed
Low Power Mode	Turned Off	Sleep Mode
Power Source	Battery Only	Battery, Mains, Energy Scavenging
Sensors	Motion Sensor Only	Various Sensors

Table 3.1 Wireless Sensor Node Variants

3.6.1 Power

Power for the mobile sensor node is provided by a button cell battery (CR2032 or similar). This sensor node is designed to operate normally from a single battery for more than 5 years. This is mainly achieved with the device being either off, or in very low power sleep mode, when not transmitting.

The static sensor node has a number of options depending of its physical deployment location. It may be powered by battery (in the same way as its mobile counter part). This device may also be powered by mains if located in or around a house. It may also be powered by scavenging energy from natural resources such as solar or wind, depending on its application.

3.6.2 Physical Deployment

The mobile wireless sensor node needs to be attached to mobile targets such as children, pets, bicycles, or refuse bins, for example. This device is deployed by simply powering it on. It is required to have a unique address (id). A single bit in this id can be used to distinguish between mobile and static devices. It is useful for the base station to be able to distinguish between the two types of devices as it can ignore the data field from a mobile sensor node data packet, as this data is not used.

The static sensor node is deployed in a fixed location, for example, in a green house for measuring temperature. Static sensor nodes must register their usage, and in some cases their position, with the base station. This device may require external sensors and/or an external power source, so its physical placement may be influenced by these factors.

If the deployment of mesh nodes is of a low granularity then the placement of a static sensor node will need to ensure that they can communicate with mesh nodes. Here the house node can play a part. The addition of an ad-hoc house node can act as a relay, receiving data from one or more static sensors and forwarding this data to the mesh nodes.

Alternatively, the static wireless sensor node can be configured to increase its transmission range in order to ensure it can send data to mesh nodes. Two ways of achieving this is to increase transmit power, or to connect an external antenna.

3.6.3 Sensors

The wireless sensor node is designed to accommodate a single on-board movement/vibration sensor. This sensor should be low power, low cost and have the ability to detect movement in all directions. It should also be able to activate the sensor node from a low power mode such as sleep.

If the wireless sensor node is required to sense anything other than movement or vibration then it will need to incorporate an external sensor. The wireless sensor node provides a digital and analogue interface for external sensors. A possible addition to

the on-board sensors would be a low battery level sensor. Currently this is not implemented in the design.

3.6.4 MAC Protocol

A MAC protocol is required in order to ensure that data sent by the 'transmit-only' wireless sensor nodes is reliably received by the infrastructural mesh nodes. The design of this MAC protocol is one of the key areas in order for this sensor node design to be viable. This research has produced two solutions for this MAC protocol. These will be presented in detail in Chapter 4.

3.7 Base Station

The base station consists of both a base station node (a mesh node with the sensor node interface replaced by a USB PC interface) and a PC. Even though the base station node, shown in figure 3.9, utilises the same basic hardware design as the mesh and house nodes, the base station node's primary role is that of an interface device between the mesh network and a PC. The base station is the single destination point for data in the network. All data is processed by the PC. The base station also acts as the gateway to the internet and to a cellular network. This requires both internet connectivity and a GSM modem for cellular connectivity.

The base station can provide information regarding the sensor network in four ways:

1. An internet web page will be updated with the current information.
2. A SMS text message will be sent signalling an event to a person or persons who have registered for that event.
3. An email will be sent signalling an event to a person or persons who have registered for that event.
4. The base station will respond to SMS text queries.

Details of the implementation of the base station and PC software will be provided in chapter 7.

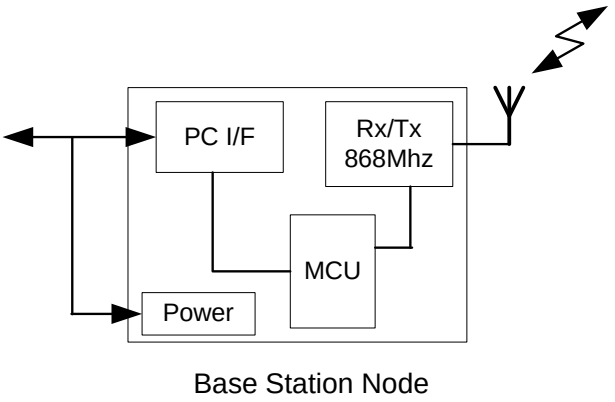


Figure 3.9: Base Node Block Diagram

The base station contains all the information regarding positions of mesh and house nodes. As these nodes are static and therefore information will only have to be updated when a new node is added or an existing node replaced.

Regarding sensor nodes, the base station must be able to distinguish between mobile nodes and static nodes. A single bit in the address of the sensor nodes can be used for this purpose. When the first data is received from a mobile sensor node the base station will register the device and store its location. Static sensor nodes will have to register their usage in order for the base station to interpret their data content. For example, the base station will require knowing if the node's data is a temperature reading or simply a switch state, or some other information. Once known, the base station can then process this information and make it readily available.

The base station should be deployed indoors in a house or community building. It will require mains supply and internet connectivity. Ideally the base station should have connection to two or more mesh nodes. If the base station is only connected to one mesh node then this node could become a bottle-neck for data traffic or a single point of failure.

The base station is required to be powered continuously. The PC will be powered from a domestic supply while the base station node will be powered from the PC via the USB interface.

3.8 Data Packet Structure and Propagation

Once the methods and techniques for routing and passing data packets between sensor nodes and mesh nodes have been established, it is also necessary to consider the structure of the data packet and the propagation of a source data packet to its destination.

3.8.1 Data Packets

Data packaging is the sending of data along with some additional information about the data, all encompassed in one data block. In wireless sensor networks figure 3.10 could be considered a general format for a data packet.

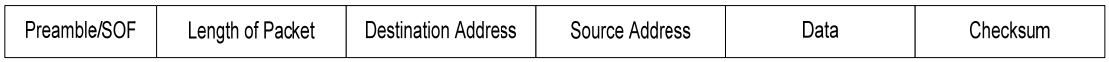


Figure 3.10: Typical Sensor Network Data Packet

- **Preamble/SOF:** The preamble is transmitted in order for the receiver to lock onto the RF signal. The preamble is often a series of alternating bits. The SOF (Start Of Frame) indicates the start of the data packet. This must contain a unique bit pattern so that the start of the packet can be identified. The end of the preamble can be combined with the SOF to produce this unique bit pattern.

- **Length of Packet:** Data packets can be of fixed or variable length. If the packets are of variable lengths then it is necessary to know how long the packet is. The length of packet data contains this information. If the packet is of fixed length then this data may not be required.

- **Destination Address:** This is to indicate the packet destination.

- **Source Address:** This is to indicate the packet origin.

- **Data:** The data contained in the packet.

- **Checksum:** Checksum or some other method of error checking the packet contents.

The design of the proposed system, has two main data transfer parts and therefore two data packets, the sensor node data packet and the mesh node data packet. Each of these has its own data packet structure.

A general structure for the sensor node data packet is show in figure 3.10. The aim of the design is to keep the packet size as small as possible without too much compromise. It is proposed to use a fixed length data packet. This immediately eliminates the need for a length byte. Also, as this packet is broadcast to all mesh nodes in range, there is no need for a destination address. This leaves the data packet structure in figure 3.11.

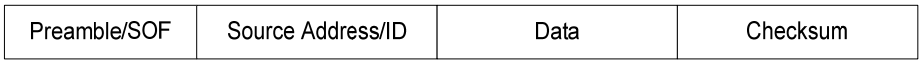


Figure 3.11: Proposed Wireless Sensor Node Data Packet

The following design parameters have being allocated to each part of the sensor node data packet:

- Preamble should have just enough bits to synchronise the receiver.
- The SOF should be established in the minimum amount of time.
- Source Address/ID should be in the range of 12 to 16 bits. This translates into approximately 4000 to 65000 unique IDs.
- The data content of the packet will be 8 bits.
- The Checksum will be 4 to 8 bits.

The mesh node data packet is also a fixed length packet. One of the advantages of fixed length packets is that they are easier to handle and quicker to process. This is of great benefit in a multi-hop network where nodes have to read in packets, process

them and forward them on. The mesh node data packet structure is shown in figure 3.12.

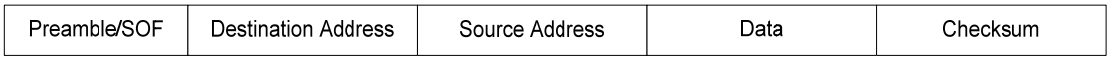


Figure 3.12: Proposed wireless mesh node data packet

It is worth noting that many of the radio transceivers suitable for the inter-mesh communication, for example the Texas Instruments CC1101 (CC1101 Datasheet 2010), have built-in preamble and SOF detection. As a result user control over the *Preamble/SOF* is limited.

The *Destination Address* is the address of the mesh node to transfer data to, according to the routing tables. The *Source address* is the address of the transmitting mesh node.

Figure 3.13 shows the content of the mesh node data. This data will contain the sensor data, which in this case constitutes both the *Source Address* and *Data* parts of the sensor node data packet. This will be a maximum of 24 bits. The mesh node data will also include the identification of the mesh node which originally acquired the sensor node data. This is particularly important with regard to radiolocation.

Occasionally sensor data will be replaced by housekeeping (HK) information origination from a mesh node allowing for the general upkeep and monitoring of the mesh network.

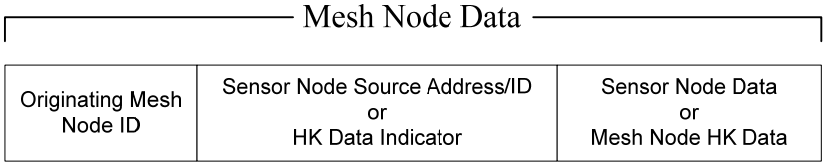


Figure 3.13: Data content of wireless mesh node data packet

3.8.2 Data Propagation

The following is a typical sequence of events where a sensor node is activated and transmits data:

1. The sensor node will broadcast one or more identical data packets for a single event.
2. Mesh nodes receiving this data will verify and process all data received from the sensor node.
3. On verifying the data packet the mesh node will retain the *Source Address/ID* and the *Data* and discard the *Preamble/SOF* and *Checksum*.
4. This retained data, together with the identification of the mesh node which originally acquired the sensor node data, now becomes the new *Data* of the mesh node data packet.
5. The mesh node data packet is then sent in the direction of the base station either directly or indirectly via a number of hops depending on its routing table.
6. Each packet is acknowledged as it makes its way to the base station.
7. At the base station, once the data packet is verified, only the mesh node data is retained and the rest is discarded.

3.9 Radiolocation

A key requirement of the proposed WMSN system is to implement a simple, effective and reliable radiolocation method.

One of the practical issues with the mobile sensor node is that its RF range will be affected by movement and RF obstacles. If the transmit range is increased to combat these effects then this will introduce other issues such as power consumption and increased data, at times, in the network. The increased data would be due to an increased number of mesh nodes simultaneously receiving the stronger signal from the sensor node. All mesh nodes receiving this would then try route this data back to the base station, resulting in an increase in network data traffic. One positive outcome

of the increased transmission power (range) is that the base station can infer radiolocation by triangulation if three or more mesh nodes report back data from the same sensor node at approximately the same time.

A more simple method, and the one implemented in the final design, is to reduce the transmit range of the mobile sensor nodes to 20m for example. If a mesh node receives data from a mobile sensor node then this node must be within 20m of the mesh node. Once the base station receives a data packet containing mobile sensor node data, it need only look at the source (mesh node) of this single packet to know the approximate location of the mobile sensor node. This is a simple radiolocation method based on proximity. This could be further enhanced by also looking at the RSSI value for a more accurate proximity analysis. This would require the RSSI value to be included in the data packet. The RSSI was not used in the final implementation of the system.

This method is extremely simple to implement. However, the trade-off here is that with the shorter transmit range mobile sensors may not be in coverage at all times, so location could mainly depend on last know location. It is also possible that mobile sensors may pass through the grid deployment without being detected so deployment strategy plays an important role here to ensure this can not happen.

House nodes may also adopt this proximity radiolocation to great effect. A typical scenario here would be a group of children playing in one house. There are two possibilities on how the house node might operate. Firstly, the house node could provide coverage for the entire house, so when a child enters the house he/she will be detected by the house node. The problem with this is how to ensure the whole house is covered and that the house node will not detect mobile sensors passing outside the house. The second solution is again a simple one. By reducing the range between the mobile sensor node and the house node to a couple of meters, a child would have to register their presence in a house by going within 2m of the house node. This reduction in range down to 2m is accomplished by reducing the sensitivity of the house node and not the transmit range of the mobile sensor node. The disadvantage with this approach is that it requires the cooperation of individuals to register their devices.

3.9.1 Tracking

Accurate tracking for radiolocation is only possible if mobile sensor nodes are constantly in range of mesh nodes and transmit at frequent intervals, or transmit every time they move. Accurate tracking also requires that the sequence of radiolocation events arrive at the base station in the same order as they were detected. Neither the sensor nodes nor mesh nodes time stamp their data packets. It is the base station which time stamps the packets as they arrive in. As mentioned in the previous section the method of radiolocation adopted relies on proximity to mesh nodes and may not provide the possibility of real-time continuous tracking and will rely on the last-known-location reported by mesh nodes in range of the mobile sensor node. A child's movement in a housing estate will generate a sequence of last-known-locations which can then be used to infer location and direction.

In terms of radiolocation in a housing estate a radiolocation interval of one minute could be deemed acceptable. An update of a child's location in the estate every minute, while the child in moving, may well satisfy the radiolocation requirements of the system. In this case accurate tracking may not be required.

This chapter has presented a system design for the proposed WMSN for a housing community. The next chapter will investigate one of the key aspects to this research namely, a suitable MAC protocol for transferring data between sensor nodes and mesh nodes. The outcome of this chapter will determine the final design implementation for the wireless sensor node, which will be presented in detail in chapter 5. This will be followed by a design presentation of the wireless mesh node which provides the backbone of the system.

4. A MAC PROTOCOL FOR TRANSMIT-ONLY SENSOR NODE SYSTEM

The wireless sensor nodes, in the proposed housing community WMSN, are effectively transmit-only devices with respect to data, i.e. 'transmit and hope'. They have no possibility of knowing if their data has been received correctly. It is therefore the responsibility of the system to ensure the highest possible success rate for sensor data to arrive at its destination, the base station. Before data can be transferred to the base station it must first be received by the mesh nodes. This requires the implementation of the wireless MAC protocol between sensor nodes and mesh nodes to reliably transfer the sensor node data. Once the mesh node has received a sensor node data packet it will attempt to transfer this data to the base station using an alternative MAC protocol based on CSMA. This is possible because the mesh nodes are equipped with transceivers. This inter mesh node MAC protocol is addressed in this chapter in regard to system scalability but will be described in detail in later chapters.

This chapter details two approaches on how to transfer data reliably from the sensor nodes to the mesh nodes using transmit-only sensor nodes. The first is a novel approach which utilises a wireless protocol based on TDMA and uses the MSF atomic time broadcast as a synchronisation signal for the TDMA sequence. The second approach is based on a 'transmit and hope' scheme. While 'transmit and hope' is not a novel approach this second approach implements a set of techniques to minimise data collision and maximise successful data transfer.

In order to choose the appropriate wireless MAC protocol for the sensor nodes the following issues must be addressed in conjunction with the overall scheme of the system:

- **Collision avoidance:** The primary task of a wireless protocol is to ensure that data transmissions do not interfere with each other. Some wireless protocols are tolerant of low levels of collision. These normally have a contingency to resend collided data (e.g. Aloha). In order for this to work, a node must contain a radio

receiver. As the proposed sensor nodes are transmit-only devices, total collision avoidance is desirable.

- **Minimum Power Consumption:** In wireless sensor networks the main power drain for nodes are the radio components, the transmitter and receiver. Some sensor nodes transmit at regular intervals based on a timing scheme. Other nodes respond to events. They transmit data only after an event has occurred. These events may rarely occur, extending the lifetime of the battery considerably. Therefore, wireless protocols should ensure that the radio transmitter is used efficiently.

- **Scalability:** This depends on the application, particularly in relation to the number of nodes required. The wireless protocol should be designed to meet the scalability requirement of the application. Furthermore, it should allow for the ad-hoc deployment of the sensor nodes.

- **Data Latency:** Latency, in this case, is the time delay from when a sensor node has data to send until the data is received by a mesh node. Acceptable latency depends on the application. There is additional latency associated with sending data from a mesh node to the base station. A suitable protocol should provide an adequate compromise between scalability and latency.

4.1 TDMA Synchronisation using the MSF Time Signal

As detailed in chapter 2, TDMA is a multiplexing technique that allows transmission from several sources to access the same communication channel by allocating individual time slots. Time slots may also include guard-bands, which are simply time spaces between slots. They guard against a possible drift in synchronisation and also cater for a tolerance in the timing between different devices. However guard-bands do give rise to additional latency.

Once the width of the time slot and the total number of slots are known, the maximum expected latency can be calculated by multiplying the number of TDMA slots by the width of the slot. This formula can also be used to establish trade-offs in the system

performance. The system can be designed to meet a short latency requirement by reducing either the time slot width or the number of slots i.e. the number of sensor nodes. Alternatively a large number of sensor nodes can be accommodated by either reducing the slot width or accepting an increase in the maximum latency. Thus, for example, designing the system to have up to 2000 sensor nodes and a maximum acceptable latency of 30 seconds would require a maximum allowable TDMA slot width of 15ms.

A possible format for the data packet transmitted by the sensor nodes is shown in figure 4.1 below. This packet is 32 bits in length. A transmission rate for the sensor node is set to 20kbit/s, resulting in a bit duration of 50μs. Hence, the total time required to transmit the entire data packet is 50μs x 32 = 1.6ms.

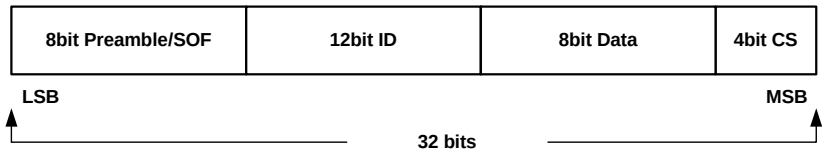


Figure 4.1: Sensor node data packet

4.1.1 TDMA SYNCHRONISATION

In order to implement the TDMA based protocol, every sensor node must be synchronised at the start of the TDMA transmission sequence, see figure 4.2.

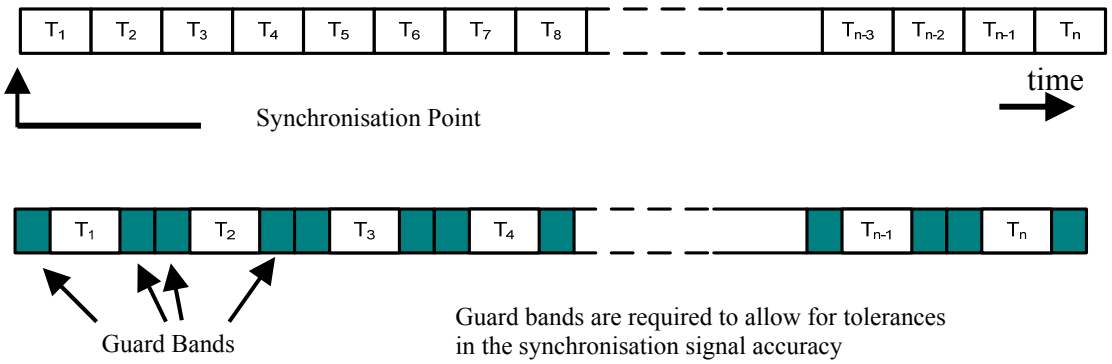


Figure 4.2: Diagram of TDMA with guard bands and synchronisation point

In order to achieve this, the first sensor node design incorporated a radio receiver capable of receiving the MSF radio transmission. This 60kHz broadcast is a Time Signal sent from Anthorn (formely from Rugby), UK. These receivers are readily available, for example the EM2S receiver module (Galleon 2010) and the CME6005 receiver (C-Max 2010).

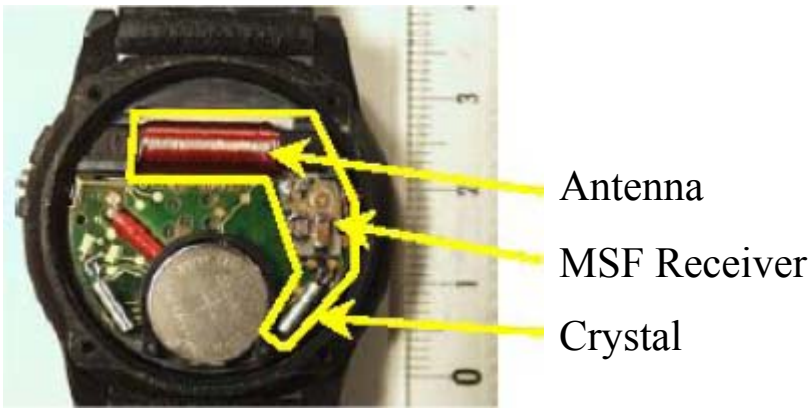


Figure 4.3: Radio controlled wrist-watch
(Lombardi 2003)

Figure 4.3 shows an example of a wrist watch which is synchronised to the MSF time (Lombardi 2003). The components required for receiving the MSF signal are a MSF receiver, which are readily available as a single chip solution from a number of suppliers, a crystal and an antenna. The antenna tends to be the largest component due to the low frequency of the signal. The MSF receivers are low cost and low power, typically 50μA when active and only 0.1μA when in stand-by mode. They are also physically very small, as can be seen from figure 4.3.

Figure 4.4 below shows block diagrams of the wireless sensor node and wireless mesh node. The sensor node contains a dedicated 60 kHz receiver for the MSF signal. It also contains an accurate low power timer to maintain the synchronisation time. Power for the sensor node is supplied by a battery. An rfPIC is used for both the radio transmissions and the on-board intelligence. In the mesh node a dedicated receiver is used for receiving data from sensor nodes.

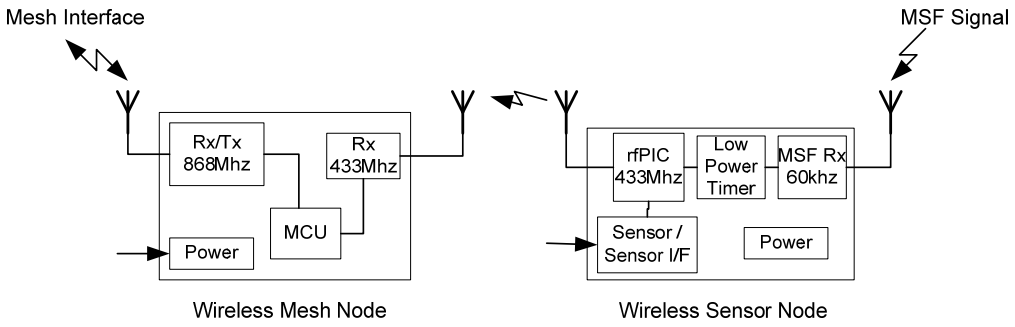


Figure 4.4: Block diagrams of the mesh and sensor nodes including the use of the MSF signal

It should be noted that the MSF signal in intended for coverage of the British Isles. However, other similar signals, provide good coverage throughout Europe and the US. The German DCF77 signal (PTB 2010) and the North American WWVB signal (NIST 2010) are two such examples.

4.1.2 MSF Time Signal

The MSF timing signal is a radio broadcast signal of the atomic clock held at the NPL (National Physics Laboratory) Anthorn, England. This signal is a modulated 60 kHz carrier wave which transmits a time signal every minute.

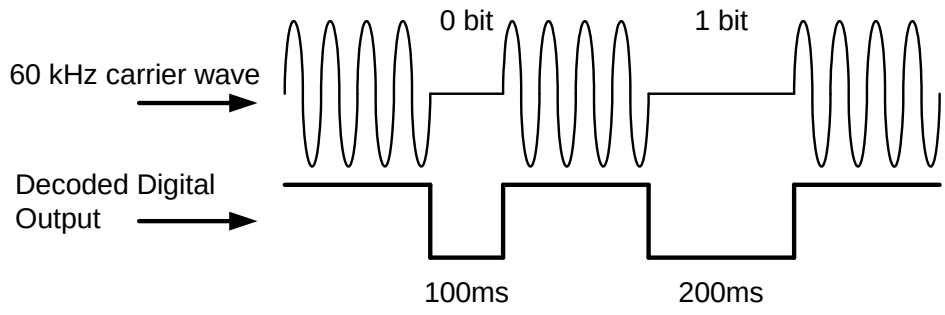


Figure 4.5: MSF modulation and encoding of '0' and '1' bits

The time information is sent in a bit stream at a rate of 1 bit/s. Bits are represented by on-off carrier modulation. A '1' and '0' bit are represented by switching the carrier

wave off for 200ms and 100ms respectively, as shown in figure 4.5. The accuracy of the one second interval between bits, transmitted from Anthorn, is better than +/- 1ms (NPL 2005). A complete one minute time frame is shown in figure 4.6.

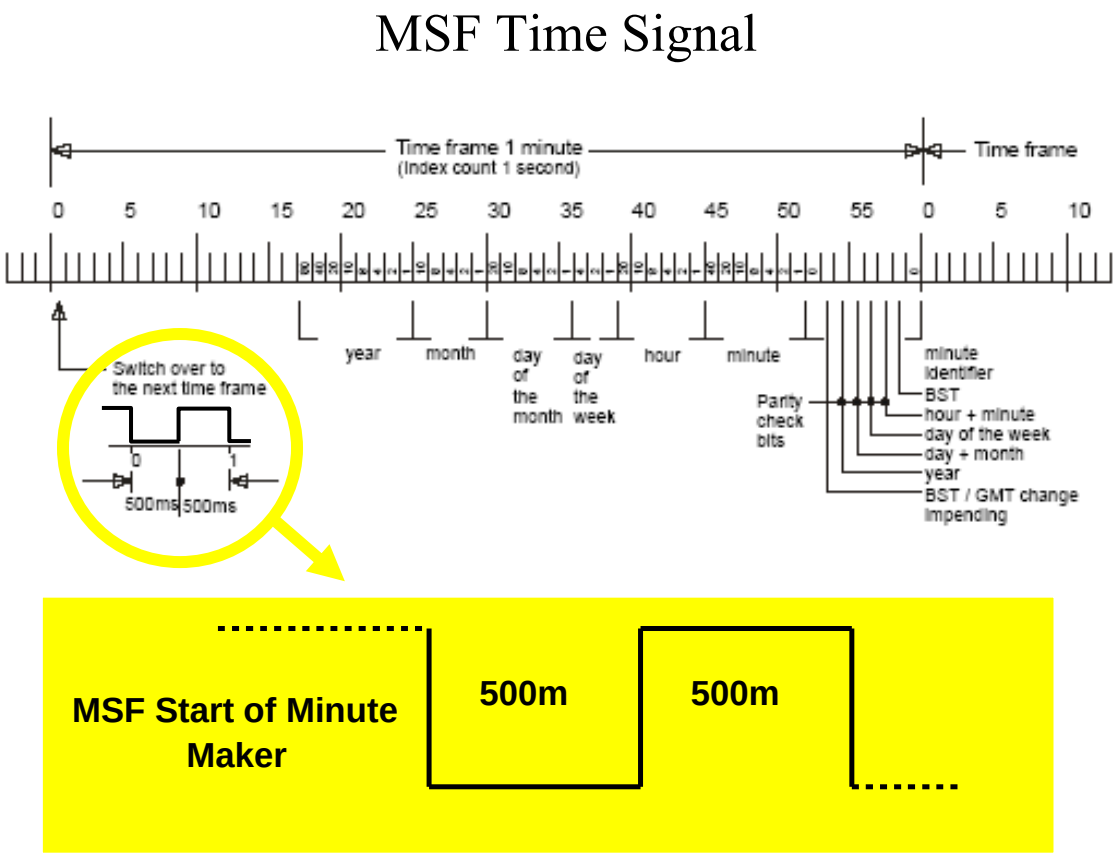


Figure 4.6: MSF 1 minute time frame

To utilise this ever-changing signal a unique bit pattern must be identified. This could then be used to determine the synchronisation point. It is also necessary that this unique pattern is repeatable at regular intervals. The pattern selected from the broadcast signal is the *start of frame* (SOF) identifier. Repeated every minute, the SOF signature comprises a 500ms low pulse followed by a 500ms high pulse, as shown in figure 4.6.

The sensor nodes contain a Galleon Systems EM2S MSF receiver module (Galleon 2010) that has a pulse width tolerance of +/- 30ms. This results in a maximum tolerance between different sensor nodes of +/- 60ms. This tolerance is mainly due to interference on the received MSF signal and not the EM2S module. It was mentioned previously that a system containing 2000 sensor nodes with a latency of 30s required

a TDM slot width of 15ms. Therefore, the MSF appears, at first glance, to be a poor choice for synchronisation. However, this is not necessarily the case. The tolerance of +/- 60ms is based on the 500ms pulse width. A significantly smaller, and more useful, tolerance can be obtained by using consecutive falling edges.

The proposed synchronisation method is to sample the MSF signal to locate the SOF signature. If the two 500ms pulses are both within a certain tolerance, the signal is accepted as a valid SOF. Anything outside this tolerance is discarded. The falling edge of the second pulse is then used to establish the synchronisation point at $t_1 + t_2$, as shown in figure 4.7 below. Ideally, $t_2 = 0$, but for practical software related reasons, t_2 will be set to a few milliseconds.

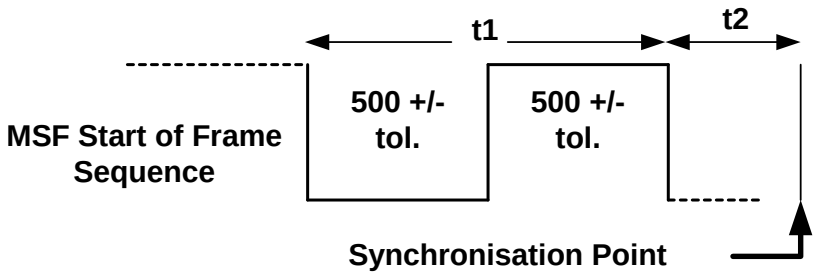
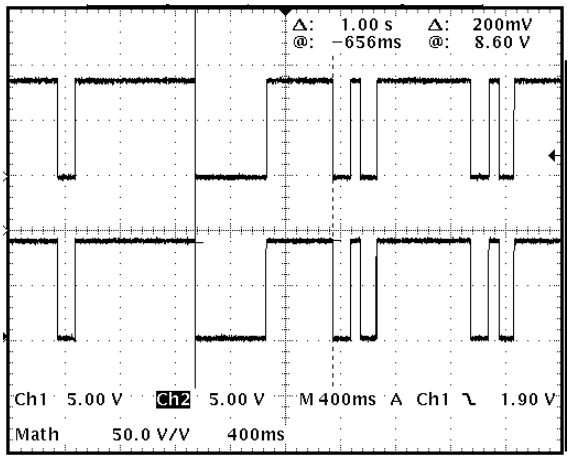
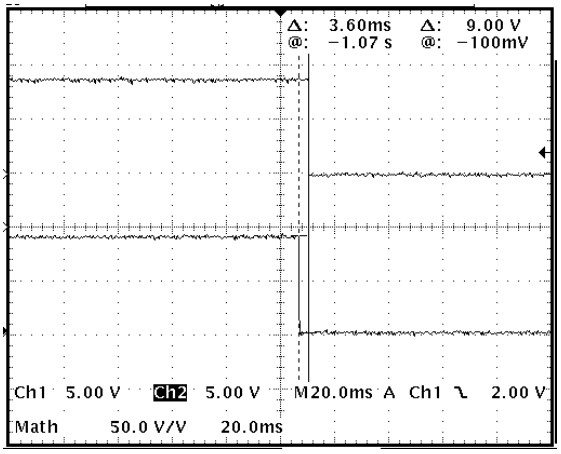


Figure 4.7: Determining the synchronisation point

In order to validate the accuracy of the chosen synchronisation point, the outputs of three MSF receivers were compared, to see how closely these points aligned. The 500ms pulses had to be within a +/-20ms tolerance limit, otherwise the SOF signal was not used. Figure 4.9(a) shows the SOF signal captured from two of these MSF receivers. It was observed that the accuracy of the falling edge of the 1s SOF signal was within a few milliseconds. Furthermore, this was not dependent on the accuracy of the two individual 500ms pulses within the +/- 20ms tolerance. Figure 4.9(b) shows a magnified view of the synchronisation point of both MSF signals. This shows the deviation between the two points to be 3.6ms.



(a)



(b)

Figure 4.9: (a) MSF SOF signal and (b) synchronisation accuracy of SOF.

This test was repeated for 1,000 continuous samples of the MSF signal. In all instances, a synchronisation accuracy of better than +/- 3ms was obtained, thus validating the proposed TDM synchronisation approach. Furthermore, as a point of interest, in approximately 20% of samples this deviation was less than 1ms.

It is worth stating that maintaining the pulse width tolerance of +/- 20ms has proven to be important. Pulse widths outside this tolerance are normally caused by interference. This interference has resulted in synchronisation errors of up to 20ms in the falling edge of the 1s SOF signal.

To further test the accuracy and suitability of using the MSF signal, three MSF receivers were setup in a housing estate for a one month period and all data logged. In this time over 24,000 samples of the signal were taken. Table 4 shows the results of this test.

The results in table 4.1 show a significant fall-off between +/-3ms and +/-2ms. There is even a greater fall-off between +/-2ms and +/-1ms. It was decided that +/-3ms, with its high percentage of success, was a good compromise for this system.

Results of the Start of Frame accuracy taken from 24,041 samples over a 1 month period

% of bad samples (not used)	**:**	**2.5%**
% of samples within +/- 5ms	**:**	**99.65%**
% of samples within +/- 4ms	**:**	**98.97%**
% of samples within +/- 3ms	**:**	**97.47%**
% of samples within +/- 2ms	**:**	**92.75%**
% of samples within +/- 1ms	**:**	**75.49%**
Standard Deviation	**:**	**1.3ms**

Table 4.1: Synchronisation accuracy of SOF over 1 month period

With a synchronisation accuracy of +/-3ms figure 4.10 shows that the TDMA time slots can be calculated at 7.6ms, 1.6ms for the data packet and 6ms for the guard bands.

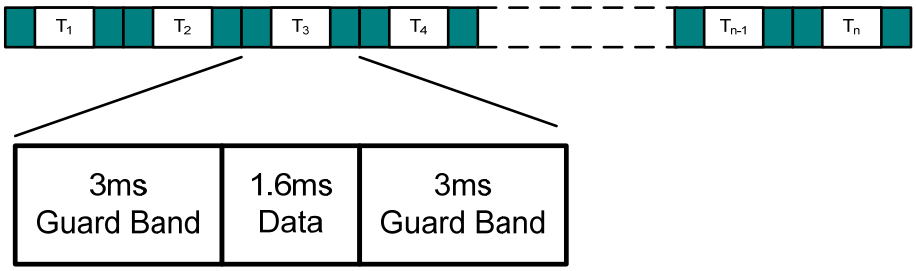


Figure 4.10: TDMA time slot with guard bands

It is also now possible to determine the performance of the system in regards to latency versus number of sensor nodes, as shown in figure 4.11. The scalability of the system is limited by the maximum acceptable latency. With a maximum latency of

30s, up to 4,000 sensor nodes could be accommodated. For the proposed housing community mesh sensor network, a maximum latency of 30s is deemed acceptable for static sensor nodes. However, for mobile sensor nodes, while 30s is acceptable for last know location, it can limit the monitoring quality. For example sensor node data packets received by mesh nodes may not be delivered to the base station in the same order as acquired due to the sequencing of the TDMA. It would then be difficult to infer the direction of a mobile sensor node.

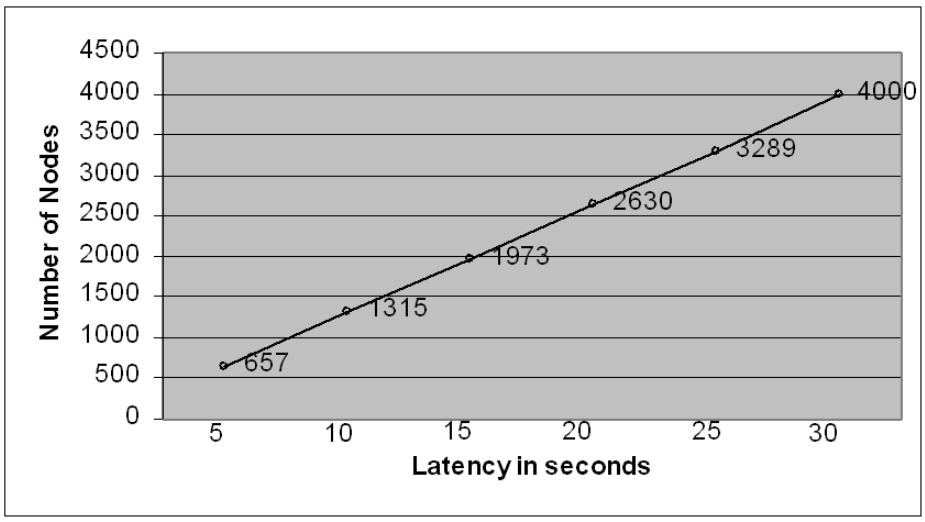


Figure 4.11: Latency vs. number of sensor nodes

The use of the MSF signal as a TDMA synchronising signal is a novel way of satisfying the requirement of this MAC protocol. However, this method was not adopted as the final solution in solving the communication protocol between the wireless sensor node and the wireless mesh node, because of the following reasons:

1. Scalability is limited.
2. Latency could be an issue when approaching large numbers of sensor nodes and especially mobile sensor nodes.
3. TDM structure should be dynamically changeable so that only active sensor nodes would require a timeslot. This would require quite complex software.
4. Unreliable MSF signal reception, especially in the vicinity of switch mode power supplies.
5. The necessity in including a dedicated Rx for the MSF signal.
6. The additional software required to decode the MSF signal.

In an attempt to alleviate some of these items, an alternative method was explored, this was the "Transmit and Hope" MAC protocol.

4.2 Transmit-Only Protocol – "Transmit and Hope"

The MAC protocol described in the previous section referred to the wireless sensor nodes as transmit-only devices. However, in order to satisfy the synchronisation of the TDMA protocol they included a dedicated receiver for the sole purpose of receiving the MSF signal. Hence the wireless sensor nodes can be referred to as transmit-only devices with regard to data. Here, a second MAC protocol is proposed to enable sensor nodes to transfer their data successfully to relevant mesh nodes without the use of any receiver.

This approach must contend with data collision. With transmit-only devices it is impossible to achieve total collision avoidance when these devices are in range of each other and share the same radio frequency channel. Therefore the MAC protocol proposed here must be tolerant of collisions, but these collisions must be kept to a low level in order to preserve system performance and to achieve a high level of confidence in successful data transfer.

4.2.1 Minimising Data Collision

The following are some areas which have been explored in minimising the effect of data collision: data rate; transmission packet length; receiver requirement for consecutive packet separation, and rate of transmissions.

Data Rate

The data rate is an obvious factor in avoiding data collision. The faster the data can be sent the less time is required for the transmission, thus reducing the probability of a data collision. The maximum data rate for the rfPIC in ASK mode using Manchester encoding is 20Kbps.

Transmission Packet Length

The transmission packet length should also be kept to a minimum. The longer the data packet the more time is taken up on the single wireless channel. This then leads to the greater possibility of data collision between two or more packets. Figure 4.12 outlines the data packet frame suitable for this system.

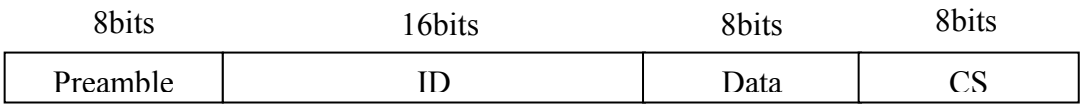


Figure 4.12: Sensor node data packet

Preamble: The preamble normally consists of ones and zeros. This data is used as padding allowing time for the transmitter to switch on, including time for the transmitter oscillator to build up and for the phase lock loop (PLL) to lock on to the oscillation. In the case of the rfPIC this time has been measured to be approximately 600μs. It is important, both in terms of packet length and power consumption, to keep the preamble as short as possible. The transmitter oscillator will start as soon as the transmitter is enabled. By keeping the data line low for the first 600μs, this guarantees that no carrier is transmitted for this time. Effectively the start up time is removed from the preamble. This therefore allows other nodes to transmit during this start up period. The proposed preamble is shown in figure 4.13.

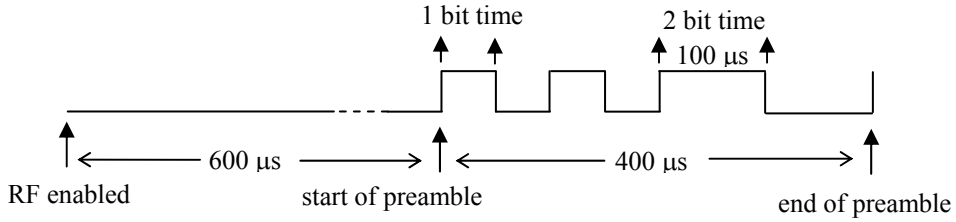


Figure 4.13: Sensor node transmission preamble

In this system it is important that the preamble is a unique pattern as it also identifies the start of the data packet. The data pattern in figure 4.13 is unique, as this pattern will not appear in the normal Manchester encoding of ones and zeros. The 400μs preamble is equivalent to 8 bits in terms of overall packet size.

ID: The ID is set to 16 bits allowing for over 65,000 unique IDs.

Data: Data is an 8 bit field reserved for sensor node data/status.

CS: This is an 8 bit checksum used to verify the packet..

The total number of bits including the preamble is 40 bits. At 20Kbps, this translates into a transmission time for the entire packet of 2ms.

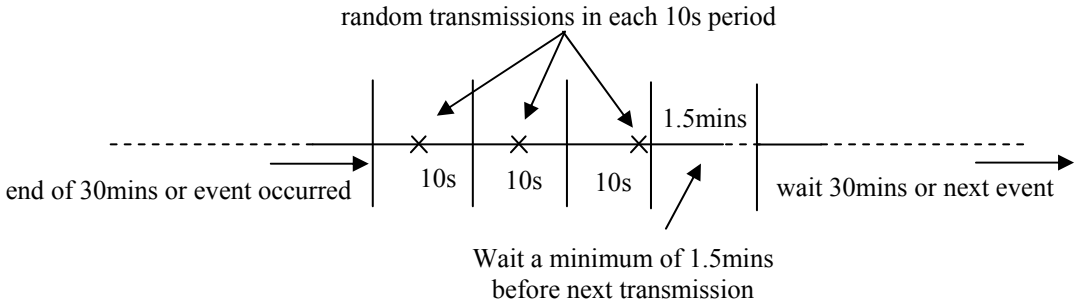
Consecutive Packet Separation

In order to calculate an accurate time for the transmission of data packets from the sensor node, we must also consider the receiver in the mesh node. If a receiver is to accept two consecutive packets there is a certain amount of time required for the receiver to finish receiving/processing one packet, store it or forward it, before it can receive the next. Preliminary tests have shown this time to be one bit time. This in effect adds 50μs to the 2ms packet transmission time. This is relatively a small amount, at just 2.5% of the total packet transmission time, giving a maximum total time of 2050μs.

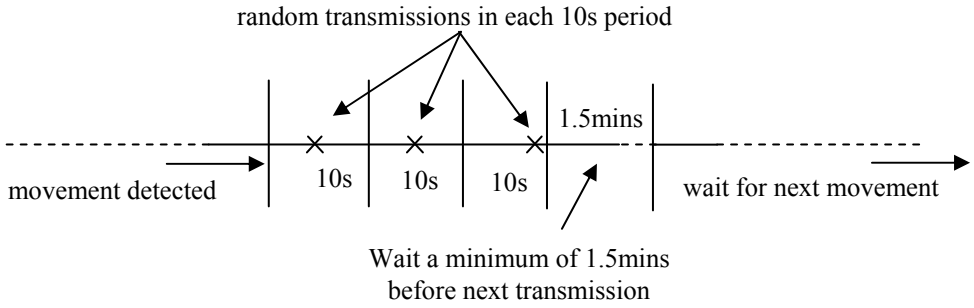
Rate of Transmissions

The period between individual sensor node transmissions is a major factor in the performance of the system. Reducing the number of transmissions in any one period is a major contributor to successful data transfer. The following scheme has been adopted. Static sensor nodes transmit at 30 minute intervals if no event has occurred. After each 30 minutes the node transmits 3 data packets in three consecutive 10 second windows. These transmissions occur randomly within each 10 second period, as shown in figure 4.14. Event driven transmissions only occur after an event has taken place. Again this data transmission consists of 3 data packets in three consecutive 10 second windows. Mobile sensor nodes adopt the same transmission scheme, treating a movement as an event. Additional movements on the same node will only be processed 1.5 minutes after the 30s transmission window has elapsed. This ensures a 2 minute interval between transmissions from the same node. It should

be noted that this transmission interval scheme is application specific. As such, the outlined times between transmissions is deemed acceptable for the proposed system.



(a)



(b)

Figure 4.14: Wireless sensor node transmit schemes for (a) static node (b) mobile node

In general, due to the distributed nature of the system, not all nodes will be competing for the same radio space during any 10s period. This is particularly the case for static nodes. Static nodes have a relatively even distribution over the housing estate. Mobile tags however, can congregate in large numbers in small areas of the estate. For this reason the mobile tags only transmit when they move position.

4.2.2 Analysis of Data Collision

To analyse the "Transmit and Hope" MAC protocol, proposed in the previous section, with regard to data collision avoidance, the probability of successful data transfers is estimated.

The probability of collision for T nodes transmitting in the same zoned area can be derived from equation 4.1 (Cerpa and Estrin 2002):

$$P_{collision} = 1 - P_{success} = 1 - \left(\frac{S-1}{S}\right)^{T-1} \qquad (4.1)$$

where S is the number of time slots in one transmission window.

This formula shows the basic relationship between node density and data packet collisions. However this formula is intended for single point events or slotted transmissions where data is sent from the start of a time slot or not at all, as in the case of Slotted Aloha. The scheme presented here does not fall into either of these categories. In our case, data is transmitted randomly and can collide anywhere during a transmission, as illustrated in figure 4.15. However, the formula above can still be used if we assume the size of the time slot to be twice that of the data packet. This idea will now be explained further.

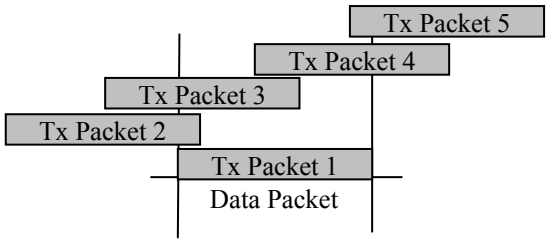


Figure 4.15: Data Packet Collisions

In slotted schemes there are a finite number of time slots reserved for a single transmission. Transmissions are synchronised to be sent at the start of the slot. The time slot need only be the length of the data transmission (data packet). Transmissions occupying the same slot will most likely collide.

In order for the proposed "transmit and hope" scheme to meet a criteria so that it can make use of equation 4.1 the following assumptions are made.

A slot is a period in time where one transmission starts and ends. If no other transmission starts in this slot then there will be no collision. For this to be true in the

proposed system a slot is required to be twice the duration of a fixed data packet. Figure 4.16 shows a data packet (*Tx Packet 1*) with a fixed transmission length of 2050μs and a starting point at Sp. In order for this packet to be transmitted with no possibility of collision, no other data packet can start transmitting 2050μs before Sp or 2050μs after Sp. This then results in a transmission window of 4100μs (or twice the data packet length). As stated above, if no other transmission starts in this slot then there will be no collision.

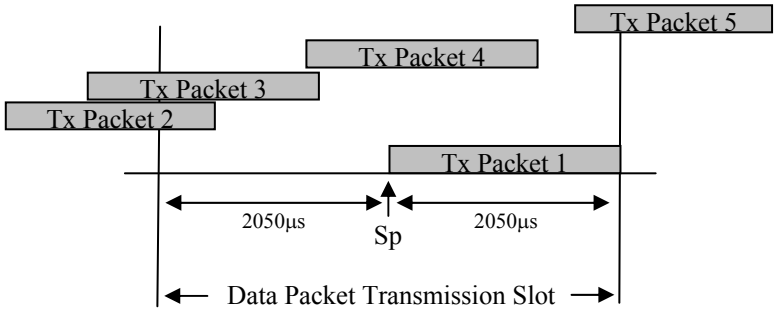


Figure 4.16: Transmission slot for one data packet (*Tx Packet 1*)

In figure 4.16 a time slot has been allocated for a data packet (*Tx Packet 1*) to be transmitted. *Tx Packet 2* and *Tx Packet 3* will not collide with *Tx Packet 1* as their transmission starting points are outside the transmissions slot (Sp +/-2050μs). However, *Tx Packet 4* and *Tx Packet 5* will collide with *Tx Packet 1* as their transmission starting points are within Sp +/-2050μs.

Equation 4.1 does not take in account the synchronised starting point associated with a slotted protocol. It simply determines if two transmissions overlap in time. In the case of slotted protocols this overlap will be 100% or not at all due to the synchronised starting point. In the case of the proposed protocol this over lap may be only partial as the starting point is random.

In order to further support the use of equation 4.1 in determining the probability of data collision, a Matlab simulation was performed.

This Matlab simulation simulates 200 sensor nodes transmitting in one 10s period to a single mesh node. This simulation assumes that all sensor nodes are within radio range of each other. The simulation tests the transmission of one sensor node against

the probability of this transmission colliding with a transmission from one of the other 199 nodes.

The transmission time for one data packet is set to 2050μs. This simulation generates 200 random transmission start times in the 10s period with a resolution of 1μs. One transmission start time is then compared to the other 199 with a tolerance of +/- 2050μs. If the chosen start time is within this period a collision is said to have occurred.

This is repeated 1000 times to establish an average and this data is logged. This simulation is then repeated a 100 times to be able to look at the deviation of individual simulations. It also then provides an overall average from these 100 simulations. The results from this simulation provided an average collision probability of 7.9% and, hence, an average probability of success of 92.1%. The Matlab code for this simulation is provided in Appendix III

Assuming that this use of equation 4.1 is correct for the proposed "transmit and hope" scheme, the same data can now be applied to the equation.

The probability of collision for 200 transmitting nodes in one zoned area is calculated as follows:

Given:

Packet duration = 2050μs therefore, Slot size = 4100μs

Then:

S = Number of Slots in 10s period = 10,000,000 / (4100) = 2,439

Hence:

$$P_{collision} = 1 - \left(\frac{2438}{2439}\right)^{199} = 7\% \qquad \text{or} \qquad P_{success} = 93\%$$

This result of $P_{success} = 93\%$ is comparable with the simulated results presented above. Using this equation figure 4.17 shows the correlation between the probability of successful transmissions and node density in any zoned area.

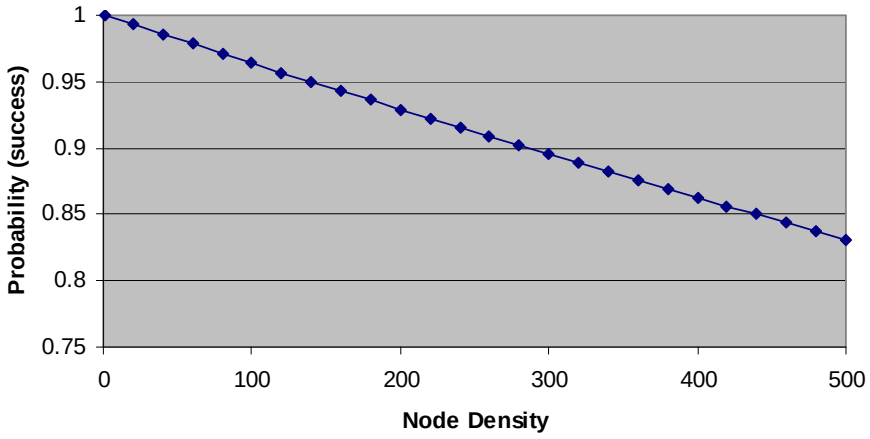


Figure 4.17: Correlation between probability of successful transmissions and node density

This figure shows that a data packet sent by a sensor node is likely to avoid data collision. However, it should be noted that this analysis allows for the worst case scenario. The system, in practice, should perform much better than this analysis suggests. The correlation between the probability of successful data transfer and node density above assumes that every sensor node is attempting to transmit data during a single 10s window. This is not the case as explained previously. It is more likely that only a small percentage of the nodes will ever be competing for any one 10s transmission window. This low contention rate greatly increase the probability of success. Furthermore, as sensor nodes will transmit to all mesh nodes in range, there can be multiple paths for the sensor node to transfer its data. Therefore a transmission colliding at one mesh node may be received successfully by another mesh node within range. The probability is also increased by repeating each transmission three times in three consecutive 10s periods.

The Matlab simulation was extended to examine the probability of successful transmissions, from a sensor node to a mesh node, taking into account the three consecutive transmissions one in each of the 10s windows. The simulation was performed for one to one thousand nodes attempting to transmit data to a single mesh node.

Using the first Matlab simulation a set of collision values were obtained for numbers of nodes ranging from 1 to 1,000 in steps of 50. This produced the graph in figure

4.18(a), a plot of the probability for a sensor node to successfully transmit data to a single mesh node, against the number of sensor nodes transmitting in a single 10s window.

By using a measure of probability the likelihood of a transmission colliding which is sent in the first 10s window and then repeated in the second 10s window is given by:

$$(\text{Probability of Collision in one 10s Window})^2$$

The probability of collision is further reduced with the introduction of a third 10s window by:

$$(\text{Probability of Collision in one 10s Window})^3$$

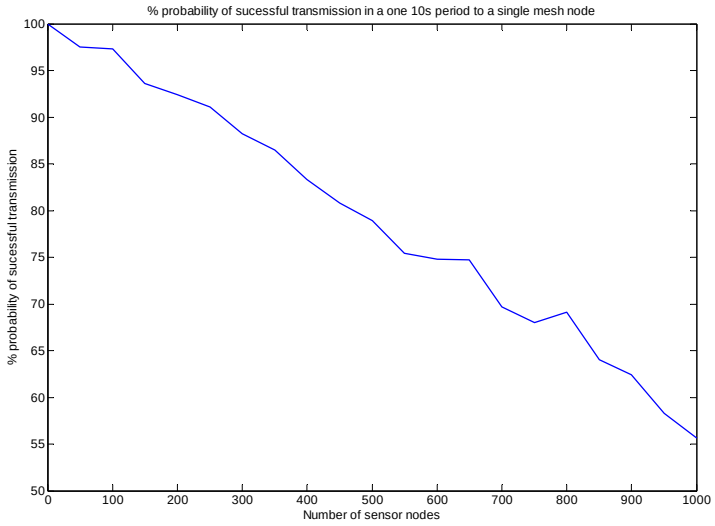
As an example, using the same criteria of 200 transmitting nodes in one zoned area with a $P_{success} = 0.93$ gives a $P_{collision} = 1 - 0.93$. The probability of at least one successful transmission, using three consecutive 10s transmission windows, is increase to:

$$1 - (1 - 0.93)^3 = 0.9996$$

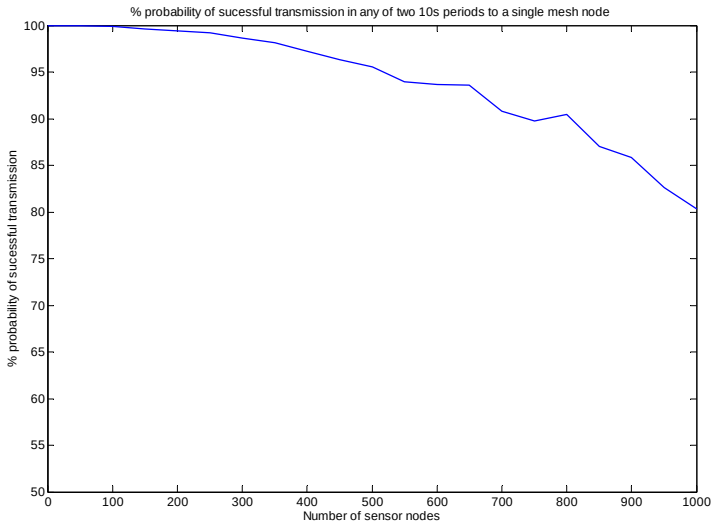
Clearly, the proposal of using 3 consecutive 10s transmission windows is vindicated in the sense that the success rate is significantly higher than for a single 10s transmission window.

Figure 4.18(b) is a Figure 4.18(c) plot the probability for a sensor node to successfully transmit data to a single mesh node, against the number of sensor nodes transmitting in two 10s windows and three 10s windows respectively.

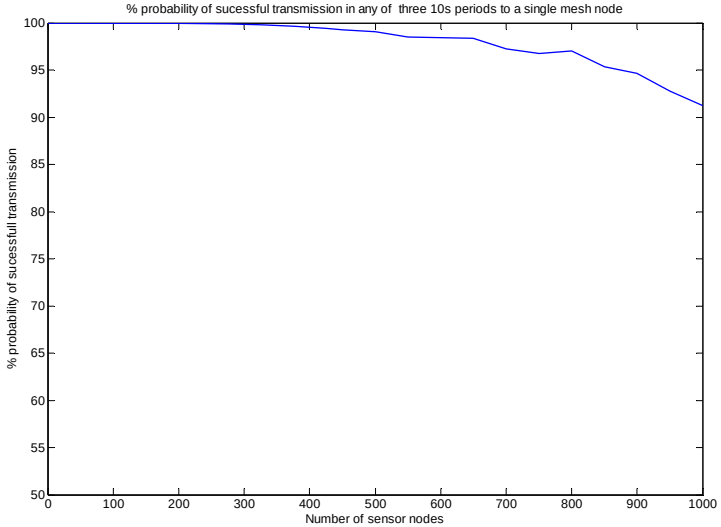
These results confirm that this MAC protocol would result in a highly probable successful transmission of data from the transmit-only sensor nodes to the mesh nodes. It has been shown that for 200 transmitting nodes in one zoned area the average probability of a successful single transmission is, $P_{success} > 0.92$ and for three consecutive transmissions this average probability increases to $P_{success} > 0.99$.



(a)



(b)



(c)

Figure 4.18: Probability of successful transmission in (a) one (b) two (c) three 10s window

4.2.3 Scalability

In order to establish the scalability of the system using the "Transmit and Hope" protocol described, the MAC protocol used to transfer data from the mesh node to the base station must also be taken in to account. This mesh node MAC protocol is described in chapter 6 and analysed on a deployed test network in chapter 7.

The analysis of the mesh node MAC protocol in chapter 7 shows that the mesh node requires 3ms in order to process, copy and transfer a data packet either to another mesh node or directly to the base station. Therefore the sensor node data packets must be separated by this 3ms to avoid collision. The scalability is calculated over a two minute period as it represents the three 10s transmission windows for the sensor nodes followed by the 1.5 minute sleep time.

Equation 4.1 can be used to calculate the potential data collision versus scalability if the additional 3ms required by the mesh node is included. The transmission slot for this equation is therefore extended by 3ms to approximately 5ms (3ms + 2050µs).

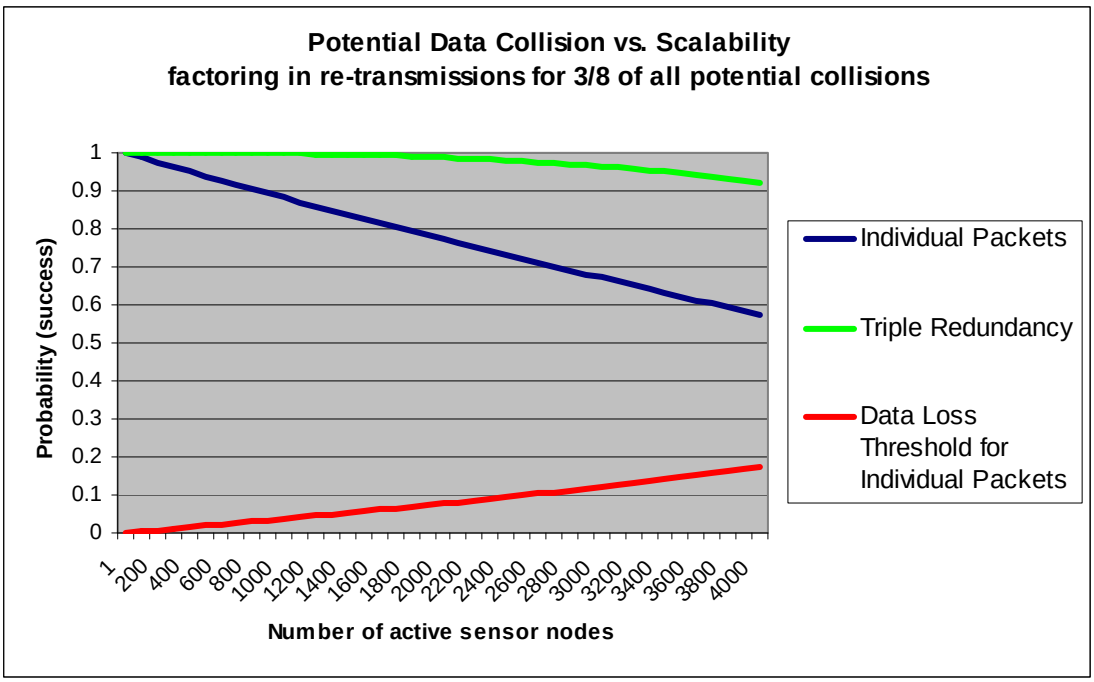


Figure 4.19: Potential data collision vs. scalability

Using equation 4.1 the potential for data collision can be estimated.

$$P_{collision} = 1 - P_{success} = 1 - \left(\frac{S-1}{S}\right)^{T-1}$$

Where:

S = Number of slots in a 2 minute period = 120,000,000 / 5 = 24,000

And:

T = Number of data packets = (Number of SNs) x 3

Figure 4.19 shows the result for this potential data collision versus scalability over a range of 1 to 4,000 sensor nodes. In figure 4.19 there are three plots. One is for the collision of every individual data packet. Another is for collisions taking in to account the three redundant data packets send by the sensor node. The third plot represents the data loss threshold for individual packets. The data loss threshold is the calculation of the point at which the required throughput exceeds the available data bandwidth over a two minute period. Details of how the data loss threshold is calculated can be found in chapter 7.

For the purposes of scalability only sensor node data is considered. The author is aware that other data such as mesh node housekeeping data is also reported by the system but this data amount is considered too small to have any noticeable effect on the results. The results displayed if figure 4.19, show that the scalability of the system could easily support the 1,320 sensor nodes of the typical housing estate described earlier in chapter 3.

5. WIRELESS SENSOR NODE DESIGN

This chapter presents both the hardware and software design of the wireless sensor node. The final design, detailed by its schematic in figure 5.1 and pictured in figure 5.2, contains four main components. These are the microcontroller unit (PIC12F675 MCU), the radio transmitter (rfPIC12F675), the sensor/sensor interface, and the power source.

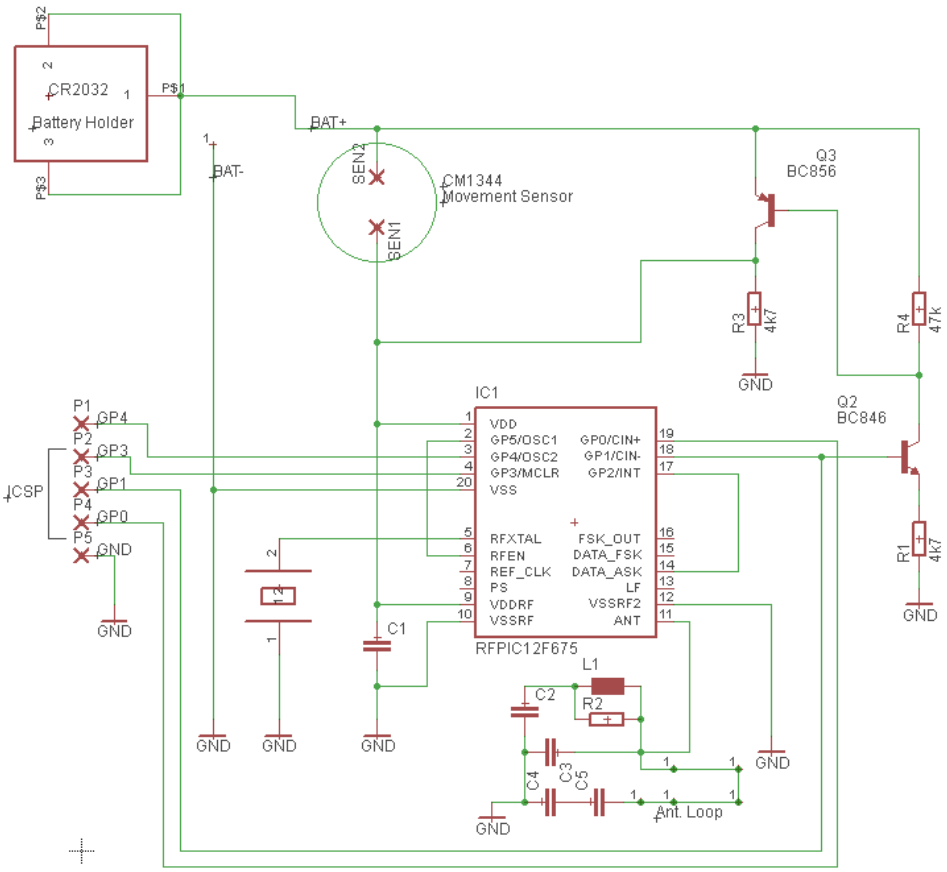


Figure 5.1: Wireless sensor node circuit diagram

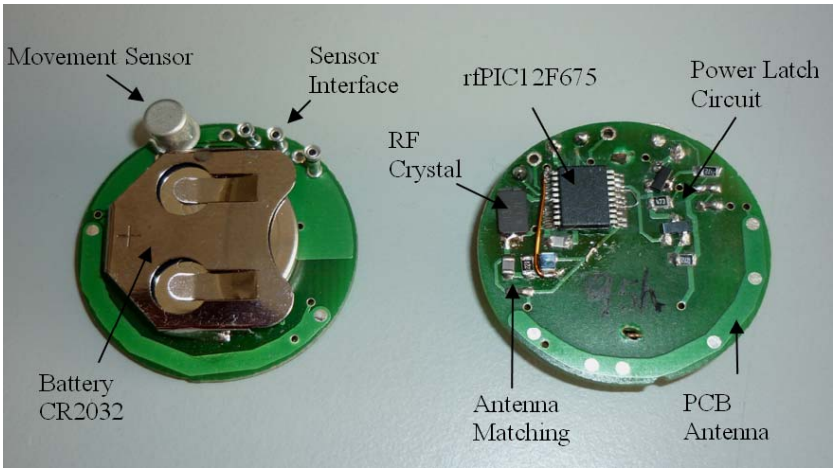
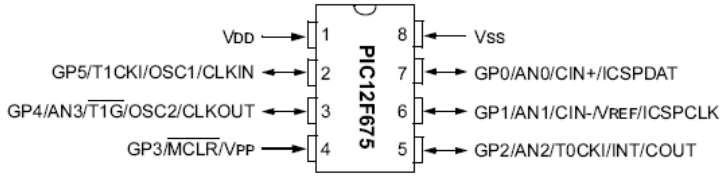


Figure 5.2: Photo of wireless sensor node

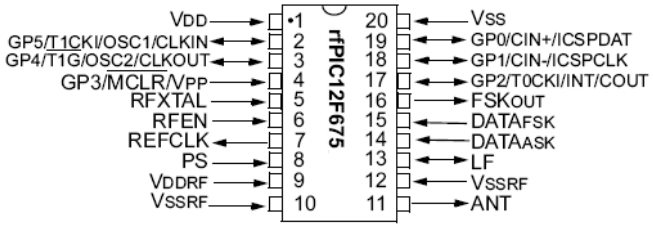
5.1 Microcontroller Unit (MCU)

The intelligence of the wireless sensor node is provided by a Microchip PIC microcontroller, the PIC12F675. This is an 8 bit MCU capable of operating at a clock speed up to 20 MHz from an external crystal oscillator. However, in order to keep cost and power low, this device has an internal 4 MHz oscillator option. It is this oscillator which is used to provide the system clock. The PIC12F675 also has 6 input/output (I/O) pins, a built in 10 bit analogue to digital converter (A/D), an 8 bit timer and a 16 bit timer. It has 1 Kbyte of flash program memory (14 bits wide) and can be serially programmed in circuit. The pin out for the PIC12F675 is shown in figure 5.3(a).

The reason for the 14 bit wide program memory on an 8 bit MCU is to enable the device to operate as a RISC (Reduced Instruction Set Computer) device. There are only 35 instructions for this MCU, therefore one program memory location can contain both the operational code (6 bits) and data (8 bits). This then provides the possibility to execute one instruction for every one instruction clock cycle. One instruction clock cycle is equal to four oscillator clock cycles. This means that this device can execute a program at 1 million instructions per second (MIPS) from a 4 MHz clock. This is more than sufficient for use in the proposed WMSN housing community application.



(a)



(b)

Figure 5.3: (a)PIC12F675 pin out (b) rfPIC12F675 pin out

Microchip produces a large range of microcontrollers that would be well suited for this task, some even better suited than the PIC12F675. The main reason for selecting this particular Microchip MCU is the availability of an integrated PIC12F675 and Radio transmitter in one package, the rfPIC12F765.

5.2 Radio Transmitter

The rfPIC12F675 was chosen mainly for its low power, small package outline (20 pin SSOP) and for the integrated PIC12F675 MCU. It also requires few external components. The rfPIC transmitter can use amplitude shift keying (ASK) and frequency shift keying (FSK) modulation at all the sub 1 GHz ISM radio bands. A pin out and package outline of this rfPIC is shown in figure 5.3(b).

The design of the wireless sensor node uses an rfPIC operating at 433 MHz and utilising ASK modulation. The transmission range of the rfPIC depends on its output power and antenna, but can be up to 50m indoors and 300m outdoors. The RF output power is selectable by use of a single external resistor.

The radio part of the rfPIC does not perform any unique encoding of bits other than to modulate the data. This makes it compatible with many low cost ASK receivers. Part of the design goal was to ensure modularity in the design. By using these generic

radio modules it is possible to use alternative radio modules in the sensor nodes without affecting the rest of the system. This would, of course, mean a redesign of the sensor node as the rfPIC is central to the sensor node design. In the case of the mobile sensor node the current design caters for both size and power requirements therefore a redesign would not be advantageous. In the case of the static node, where size isn't a strict constraint, the use of an alternative radio module can provide some advantages. For example, if the MCU and radio modules are separate devices then any MCU can be used. A MCU with more resources such as I/O could then be used to better effect.

While the rfPIC is a good initial device to work with, it is important that the system is not dependent on this device as the rfPIC has some restricting features. The main restriction of the rfPIC is the lack of general purpose I/O (GPIO). The device claims to have 6 GPIO pins. This is in theory true as the rfPIC uses the PIC12F675. In practice, however, this is not the case. The internal IC packaging of the rfPIC is shown in figure 5.4. It can be seen from this diagram that the PIC12F675 and the radio transmitter are two separate entities with no electric integration between the two.

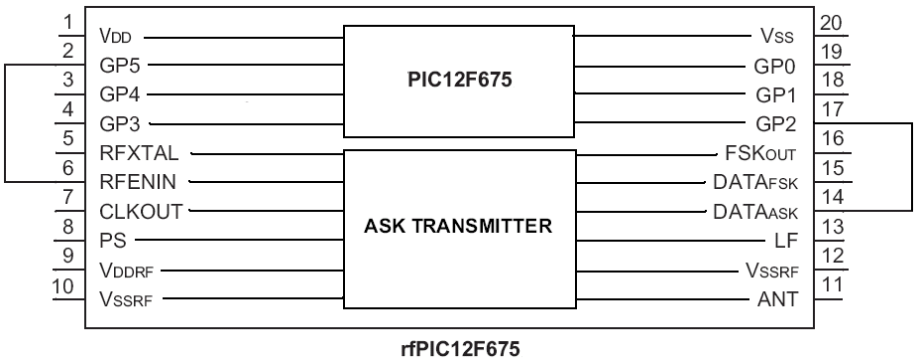


Figure 5.4: rfPIC12F675 requiring external connections

So in order to operate the rfPIC, it is necessary to make external connections. Figure 5.4 shows that two external connections are required. The RFENIN (transmitter RF enable pin) is required to be controlled by a GPIO pin (GP5 shown here). $DATA_{ASK}$ is the data input for ASK transmissions. Data into this pin is provided through another GPIO pin (GP2 shown here). Taking this into consideration the rfPIC, in practice, has

4 usable GPIO pins. This is a restriction in the design, especially for sensors and sensor interface.

5.2.1 Antenna

The antenna for the senor node can be implemented in one of three ways. The circuit layout design for the sensor node includes a PCB antenna. The area of the PCB is too small to implement a highly efficient PCB antenna so its performance range is limited as table 5.1 shows. Earlier, in section 3.9, it was discussed that short range sensor nodes could provide accurate radiolocation once detected by a mesh node, by inferring proximity to that node. The shorter range of this PCB antenna would be well suited to this. PCB antennas also have the added bonus that they are very low cost.

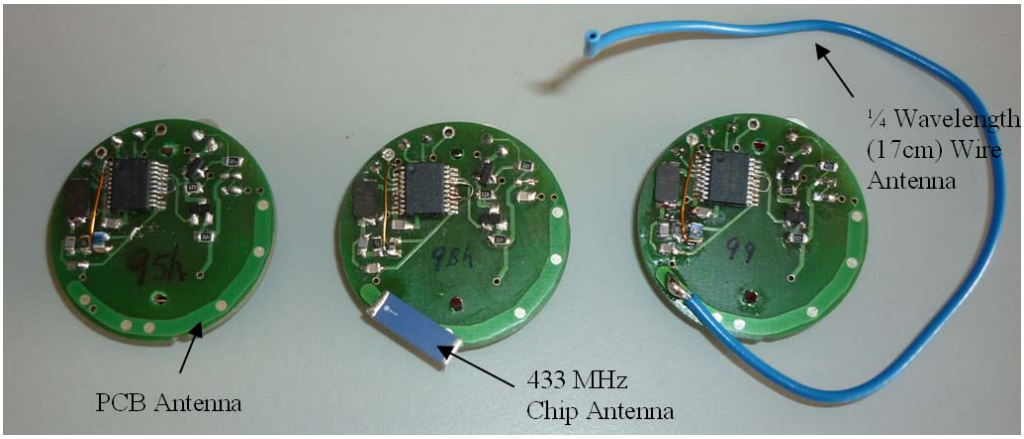


Figure 5.5: Alternative antennas for sensor node

The PCB antenna can be replaced by either a chip antenna or a simple length of wire cut to the appropriate fraction of the wavelength, for example a quarter of the wavelength. Figure 5.5 shows the implementation of each type of antenna. Tests were performed on each of these antennas. Table 5.1 gives a comparison of the measured results using these three antenna choices.

Antenna Type	Output Power Setting (dBm)[(1)]	Indoor Distance (m)	Outdoor Distance (m)
PCB	**9**	**5 to 10**	**30 to 35**
Chip	**9**	**15 to 20**	**60 to 70**
¼ Wavelength Wire	**9**	**30 to 35**	**90 to 100**
Note 1: The output power can be set from -70 to 9 dBm in five steps.			

Table 5.1: Measured range of different sensor node antennas

5.2.2 Transmission Format

Manchester encoding is used to encode each bit sent by the sensor node (except for the preamble). In Manchester encoding, logic 1 and 0 are represented by transitions rather than levels. There are two conventions for representing bits in Manchester encoding. The convention adopted for the sensor node is shown in figure 5.6. Logic 1 is represented by a transition from one to zero at the centre of the bit time. Logic 0 is represented by a transition from zero to one at the centre of the bit time. This bit time is 50μs, giving a maximum data rate of 20 kbps.

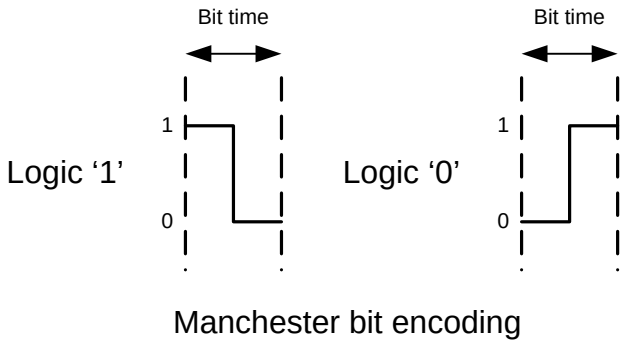


Figure 5.6: Manchester Encoding of Logic 0 and Logic 1

One advantage of using Manchester encoding of bits is that this method can be tolerant to a small amount of interfering signals (or noise). As the transition is expected at the centre of the bit the receiver can exclude signal transitions either side of the expected transition. So in the case of the 50μs bit time transmitted by the sensor node, the receiving mesh node can implement a detection window of +/- 10μs (either

side of the expected transition) to test for the transition. This means that transitions in the data outside this window caused by noise, will not affect the decoding of the bit. Another advantage of Manchester encoding is that from each bit transition the sampling time to the next transition can be reset, thus avoiding any drift in timing.

One disadvantage of Manchester encoding is that it uses two potential bit times to encode one bit. The rfPIC is capable of transmitting at a maximum bit rate 40kbps when using simple bit encoding i.e. logic high for '1' and logic low for '0'. When Manchester encoding is used, this maximum rate drops to 20kbps.

5.3 Sensors and Sensor Interface

In chapter 3 the system design outlined that there are two variants of the wireless sensor node, a mobile node and a static node. Both these nodes are based on the same hardware. The differences between the two include the sensor options, the power options, and some software differences to cater for these.

The mobile wireless sensor node basically acts as an active RFID tag and one of its primary uses is that of radiolocation of children in a housing estate. The device requires a sensor to detect when a child moves location. The child would also have to wear the device on their person. For test purposes a small wrist band enclosure was designed and rapid prototyped, as shown in figure 5.7. In order to detect the movement of a child, the motion sensor must be able to sense movement in all directions. This was one of the requirements from the system design. Other requirements included low power consumption, and the ability to wake the device from a low power condition such as sleep mode or powered off. For these reasons, the Assemtech CM1344 (Assemtech 2010) vibration/movement sensor was chosen. The CM1344 simply operates as a momentary switch when moved. This sensor is a passive mechanical sensor requiring no power. The CM1344 is somewhat unique compared to similar movement sensors in that, it is a non-position sensitive device and its contacts, at rest, are normally open no matter the orientation of the device. Due to these features, it was possible to incorporate the CM1344 as a *power on* switch as well as a motion detector.

Figure 5.7: Sensor node wrist band enclosure

The CM1344 sensor connects the battery to the power pin (Vdd) on the rfPIC. At rest no power is supplied to the circuit therefore the device is completely off. On movement the rfPIC is powered. It can then transmit data and on completion, it can switch itself off. This will be explained in more detail in the next section.

One advantage of this implementation is, by connecting the CM1344 sensor to the power rather than a GPIO pin, a GPIO pin is saved for other uses such as, for example, battery monitoring. This is not in the current version of the design.

A static wireless sensor node requires continuous power. To achieve this, the CM1344 is simply removed and its pads on the PCB shorted together. One of the design challenges for the static wireless sensor node is coping with the lack of I/O for sensor interfacing. The wireless sensor node has three GPIO pins available for sensor interfacing. These pins can be configured as inputs to an ADC peripheral on-board the rfPIC. These inputs can then be interfaced to analogue sensors such as temperature sensors. There are also simple hardware techniques to use a single ADC input to detect multiple switch inputs, see figure 5.8.

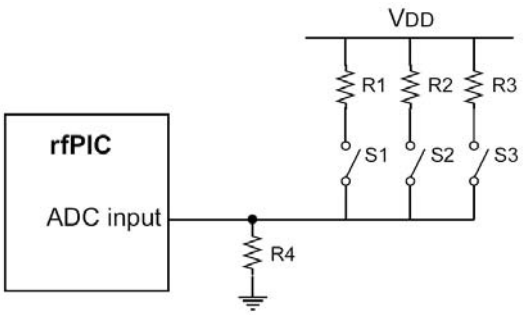


Figure 5.8: Multiple switch detection using an ADC input

With careful selection of values for R1, R2 and R3, the voltage at the ADC input will be unique for any combination of the three switches. This will enable the rfPIC to decode which switches are open and which are closed.

5.4 Power

In the previous section it was mentioned how the CM1344 movement sensor was used as a switch to power up the rfPIC. This is now explained in more detail.

On detection of movement the mobile wireless sensor node is designed to: power up, transmit data and power down. The CM1344 is directly connected between the 3 volt battery and Vdd to the rfPIC. This connection remains open while the device is stable. On movement this connection momentarily closes, supplying power to the rfPIC while closed. In order for the rfPIC to remain powered on it must be able to latch the power to the circuit. This is achieved using the power latching circuit in figure 5.9.

The latching circuit consists of two transistors, Q2 and Q3, and three resistors R1, R3 and R4. As soon as the rfPIC is powered its first tasks is to latch the power to the circuit. This is done by setting the GP1 pin high which switches Q2 on. When Q2 is switched on, the base of Q3 is driven low switching it on. Once Q3 is switched on power from the battery will flow through Q3 to Vdd on the rfPIC, bypassing the CM1344 sensor. The circuit will then remain on until GP1 is set low by software.

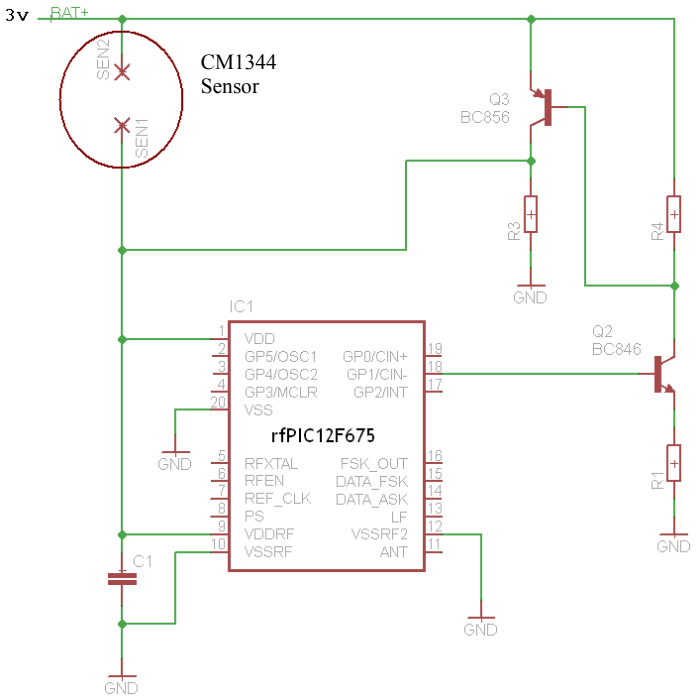


Figure 5.9: Power latching circuitry

Once the power is latched to the circuit the wireless sensor node can then start its transmission sequence. Once this is done, the wireless sensor node can switch itself off by setting GP1 low. The device will now remain off until the next movement is detected.

At the early stages of design there was some concern that a short pulse (spike) from the CM1344 would not be long enough for the rfPIC to start up and latch the power and that this could cause the PIC12F675 to latch-up. To test this possibility, a preliminary test circuit of the sensor node circuit, shown in figure 5.10(a), was constructed. Figure 5.10(b) shows the circuit mounted on a door. This circuit was tested over a period of two years and was activated approximately 20 times a day on average. When the door is opened or closed the device activates and flashes a LED. This test was visually observed during this testing period and operated correctly, verifying the design.

This circuit was then incorporated into the final design of the sensor node and a more formal test was performed over a six month period. Five sensor nodes were placed on

five doors which had combined activations of over 500 times per day on average. These activations were logged on a PC via a wireless link.

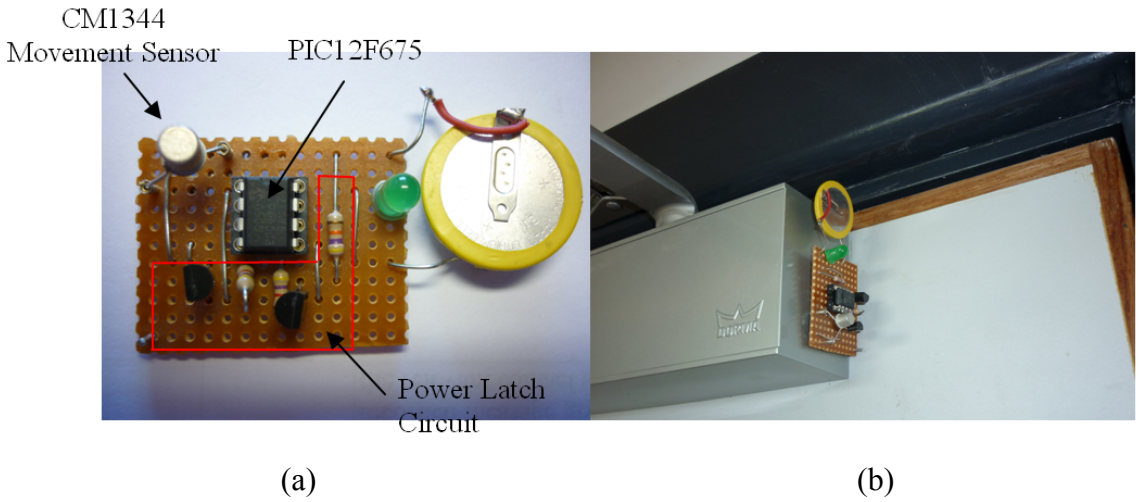


Figure 5.10: Testing of CM1344 as a power-on switch

5.4.1 Power Budget of mobile Sensor Node

On power up, the mobile wireless sensor node will remained powered for 2 minutes. During the first 30s the wireless sensor node will transmit one set of data three times. After this 30s period the wireless sensor node will remain in sleep mode for the remaining 1.5 minutes before switching itself off. This is to ensure that the maximum transmission rate of new data from the wireless sensor node is one transmission every two minutes (or thirty transmissions per hour).

A design goal for the wireless sensor node is for a battery lifetime in access of 5 years under normal use. In order to establish if current sensor node design meets this requirement, the following parameters have been established. A 3V battery with a capacity of 200mAh is used as the power source. The start-up power for the sensor node (with the transmitter disabled) is 1mA. The duration of this start-up period is typically 100ms. The power required while the sensor node is transmitting is 14mA. The sensor node transmits for 6ms every 2 minutes. At all other times, while the sensor node is powered, it will be in sleep mode, consuming 0.5µA. The actual duration of sleep time per transmission is 2 minutes less 106ms (start-up and transmission time). For calculation purposes 2 minutes will be used as the sleep time. This difference will have little effect on the overall result. The quiescent current draw

of the latch circuit is approximately 500pA. At continuous draw, this quiescent current would have negligible effect on the overall battery life calculation below. With this information, it is now possible to calculate how long the 3V battery will last for.

Assuming that the sensor node is transmitting continuously, i.e. 30 times per hour, the capacity of power consumed by the wireless sensor node for each hour can then be calculated as follows:

At start-up, 1mA will be consumed for 100ms and this will occur 30 times per hour, giving the following hourly power consumption:

$$30\frac{1mA}{1h/100ms} = 0.81\mu Ah \tag{5.1}$$

During sleep mode the sensor node will use 0.5μAh as the device is effectively in sleep mode continuously. While transmitting, 14mA will be consumed for 6ms, 30 times per hour. Hence:

$$30\frac{14mA}{1h/6ms} = 0.69\mu Ah \tag{5.2}$$

Therefore the capacity of the battery used per hour is simply the addition of the power used during start-up, the power while in sleep mode and the power consumed while transmitting. This gives a total hourly power consumption of 2μAh.

Therefore, a 200mAh battery will power the sensor node continuously for approximately 11 years. This far exceeds the design goal of 5 years.

5.5 Software Design

Microchip provides free development tools and compilers for their range of MCUs. The PIC12F675 can be programmed in assembly language or in higher level

languages such as C. The PIC12F675 does however lack the resources, especially RAM, for large complex C programs. In order to obtain the most efficient code and performance from this MCU the device is programmed in assembly language.

The software design of the wireless sensor node is outlined by the flowcharts in figure 5.11. It can be seen from these flowcharts that the software is mainly based around its 'Transmit and Hope' MAC protocol.

5.5.1 Random Number Generator

One of the tasks of the software is to be able to transmit data at random periods during the ten second windows. The MCU is therefore required to generate random numbers. To generate a truly random number requires the use of external events otherwise software can only generate a pseudo random number. The following method is used to generate the three random times for the three ten second transmission windows.

1. Each sensor node will have a unique 16 bit number stored in its non-volatile memory.
2. Timer0, an 8 bit timer which increments by 1 on every instruction cycle (1μs), will be preloaded with the lower byte of the 16 bit number.
3. The upper byte of the 16 bit number will be used as a counter for a 8μs delay loop.
4. On completion of the delay, which will have been in the range of 0 to 2ms, the value of Timer0 (between 0 and 255) is used as the random number.
5. To ensure that this pseudo random number is not repeated each time, the 16 bit number is updated. This is achieved by replacing the upper byte of the existing 16 bit number with its lower byte and replacing the lower byte with the new random number in Timer0.
6. This is repeated three times for the three different transmission windows.

In the case of the mobile sensor node an external event is provided by the CM1344 sensor. The activation of this sensor will be a random event and therefore the start of the transmission sequence will also be at a random time compared to all other sensor nodes.

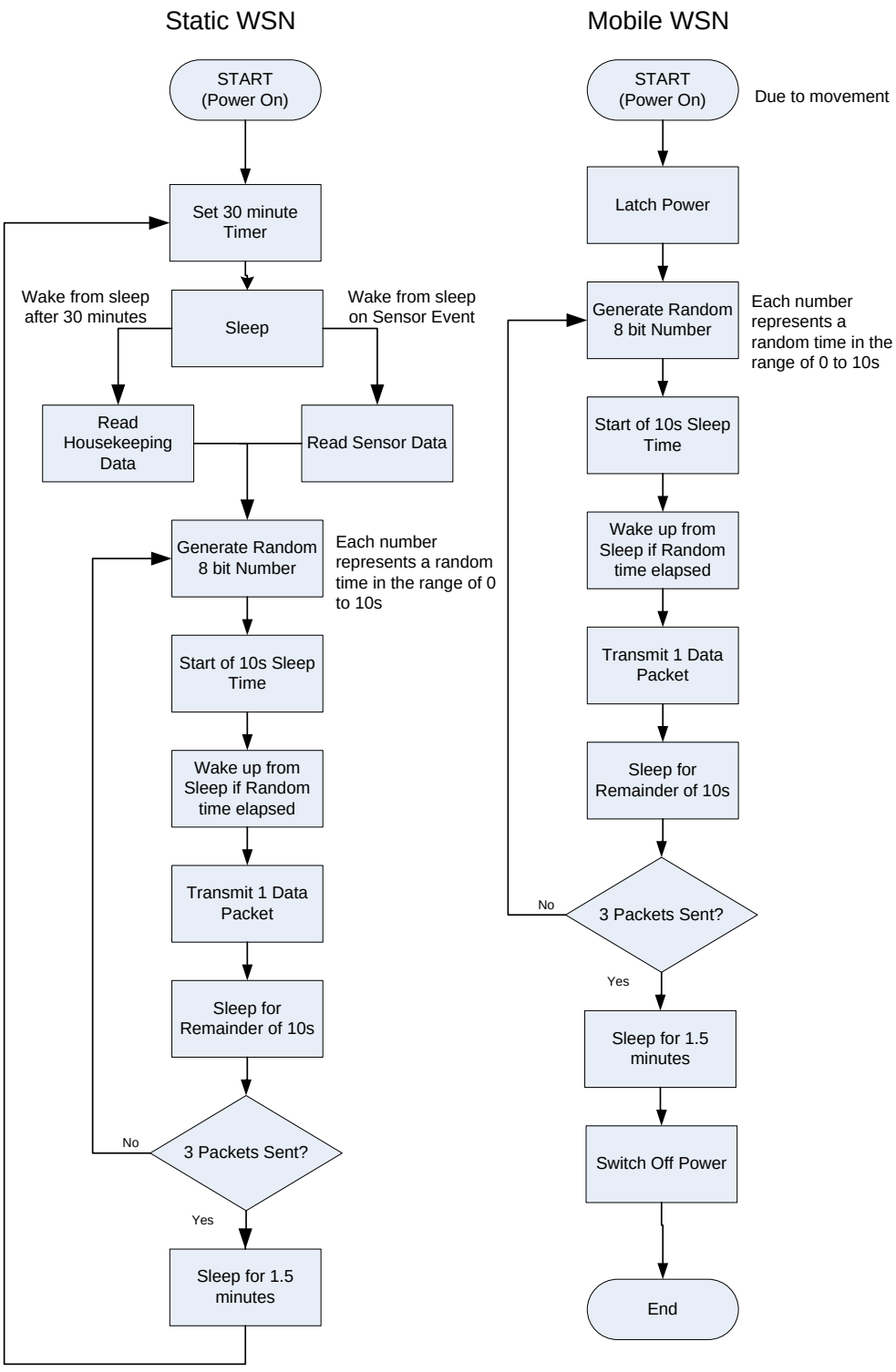
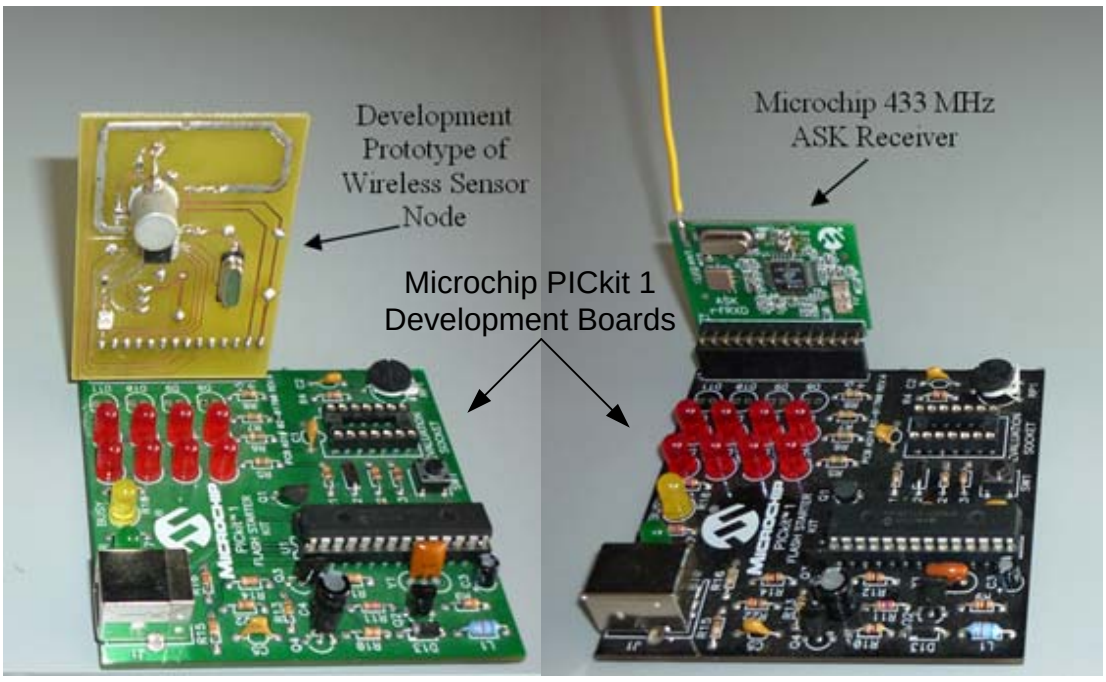


Figure 5.11: Top level flowcharts for static and mobile sensor nodes

5.6 Preliminary Test and Development

The sensor node software was developed using Microchips MPLAB Integrated Development Environment (IDE). This is a freely available development tool from Microchip. MPLAB IDE not only facilitates writing and compiling of source code but can also test code by means of its built in simulator. Much of the code was developed and tested using this simulator. However, for real world stimulus, hardware is required. In order to develop and test the software beyond the capabilities of the simulator, a prototype of the wireless sensor node was developed, figure 5.12(a). This prototype board was designed to interface with the Microchip PICkit 1 development board. This interface allows the rfPIC to be programmed from MPLAB via the PICkit 1 and left in place during testing. The PICkit 1 board also provides continuous power to the prototype board. In this prototype the motion sensor is connected to a GPIO pin as the power latch circuitry is not included.



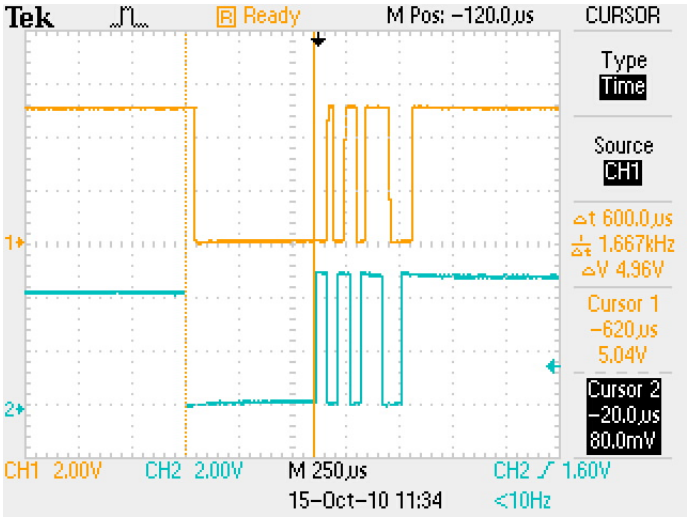
(a) (b)

Figure 5.12: Test and software development setup for sensor node

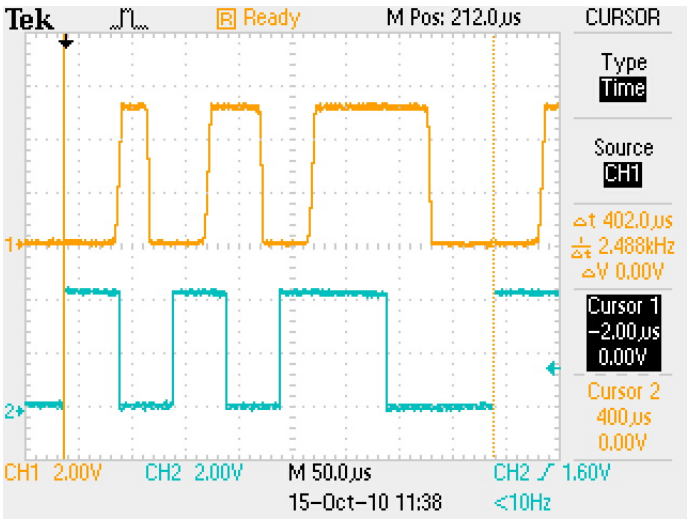
A Microchip 433 MHz ASK receiver, also interfaced to a PICkit 1, is used to receive data from the prototype sensor node as shown in figure 5.12(b). Data received by the

ASK receiver was monitored and captured on an oscilloscope for verification of data packet content and timing.

This setup for developing and testing the sensor node software proved very efficient in terms of modifying programs, reprogramming the sensor node and then retesting the modified code. The following tests results were obtained using this setup.



(a)



(b)

Figure 5.13: Sensor node (a) full preamble signal (b) last 400µs of preamble

Figure 5.13 show two oscilloscope images of captured sensor node preamble signals. The waveform on the bottom of both oscilloscope screens (channel 2) is the output from the sensor node microcontroller to the rfPIC transmitter. The signal on top (channel 1) is the output obtained from the ASK receiver. Figure 5.13(a) shows a

complete preamble sequence including the 600µs at the start were the rfPIC transmitter is enabled but no data is sent. Figure 5.13(b) zooms in on the 400µs period following the 600µs. This 400µs sample of the waveform contains the unique bit pattern which distinguishes this signal as the sensor node preamble/SOF.

This test verified that this short preamble was sufficient for the receiver to lock onto the signal transmitted by the sensor node. As can be seen from figure 5.13(b), top waveform, only part of the first 50µs high period was partially affected as the receiver locked on to the signal.

The slight shift of approximately 40µs between the two signals is due to propagation delays from the time the data is sent by the microcontroller to when it is demodulated by the receiver.

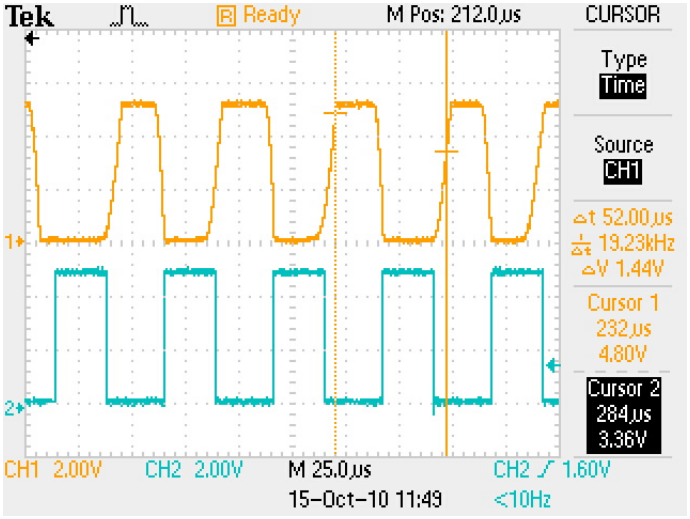


Figure 5.14: Manchester encoding at 20kbps

According to the rfPIC12F675 datasheet, its maximum ASK transmission speed is 20kbps when using Manchester encoding. In order to verify this, a series of bits were transmitted at this maximum rate. Figure 5.14 shows the transmitted bits in the lower waveform and the received bits above. The signals appear to be inverted but this is not the case. This is again due to the propagation delay between the original signal and the received signal. Overall, these tests show that the design works as required.

5.6 Sensor Node Cost Analysis

In order to develop a low cost system the sensor node should be as low cost as possible. Tables 5.2 provides the cost breakdown for the sensor node. These costing have been validated where possible by obtaining prices from the following online component distributors DigiKey, Microchip Direct, Radionics and Farnell. Prices for PCBs and have been obtained from PCB-Pool. The total cost of sensor nodes in quantities of one thousand is €3.50 per unit. To keep the costs low printed track antennas used on the sensor nodes. These antennas have no price impact on the overall cost. There is no significant cost associated with deployment of the sensor nodes as these nodes need only be registered with the base station and powered.

Part	**Description**	**Each € 1+**	**Each € 1000+**	**Qty**	**Price € 1+**	**Price € 1000+**
rfPIC12F675	Radio Transmitter/Microcontroller	1.70	1.00	1	1.70	1.00
*SW-180	MEC Vibration Switch	0.20	0.08	1	0.20	0.08
CR2032	Coin Cell Battery	0.30	0.20	1	0.30	0.20
Bat Clip	Battery Holder	0.20	0.12	1	0.20	0.12
PCB	Sensor Node PCB	3.00	1.00	1	3.00	1.00
ABS Box	Enclosure	1.00	0.50	1	1.00	0.50
Misc	All other components	1.00	0.60	1	1.00	0.60
	TOTAL				**6.40**	**3.50**

*The SW-180 is a low cost replacement part for the Assemtech CM1344 vibration sensor

Table 5.2 Breakdown cost of wireless sensor node

6. WIRELESS MESH NODE DESIGN

This chapter presents the design of the wireless mesh node. Key hardware and software design aspects of the mesh node are described. Although this thesis is primarily a design presentation, the main hardware components of the mesh node have been prototyped to an advanced stage. This has been done in order to facilitate the verification of both the hardware and software design.

The wireless mesh node consists of a mesh node main board containing a micro controller unit (MCU), a mesh node radio module using the Texas Instruments (TI) CC1101 radio chip, a PC (USB) interface module, a sensor node receiver module and a power source. Figure 6.1 shows all these main components in block diagram format.

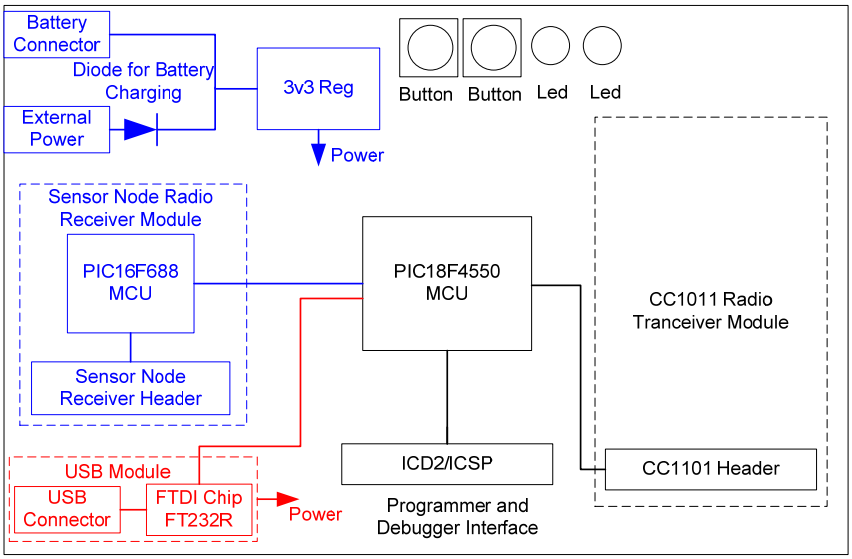


Figure 6.1: Wireless mesh node block diagram

The infrastructural mesh node, the house node and the base node are all variants of the wireless mesh node. All three utilise a common hardware platform (main board) based around the Microchip PIC18F4550 MCU (mesh node MCU). The mesh node *MCU* and *Radio Module* are common to all three variants. The *Sensor Node Receiver Module* and the *Battery/External Power* are used in both the infrastructural and house nodes but not required for the base node. The base node is the only node which requires the *USB Module*. This USB module also provides power for the base node.

Each of the main components and inter connecting interfaces will now be described in terms of hardware implementation and software control.

6.1 Mesh Node Main Board

The main board, pictured in figure 6.2 together with a battery pack and a mesh radio module, is the core component in the mesh node. This board is primarily designed around the mesh node MCU. This board also contains the interfacing hardware for the plug-in modules such as the mesh radio and the sensor node receiver modules. Two momentary push buttons and two LEDs are also included on the main board. These are used for testing, software development and functional deployment.

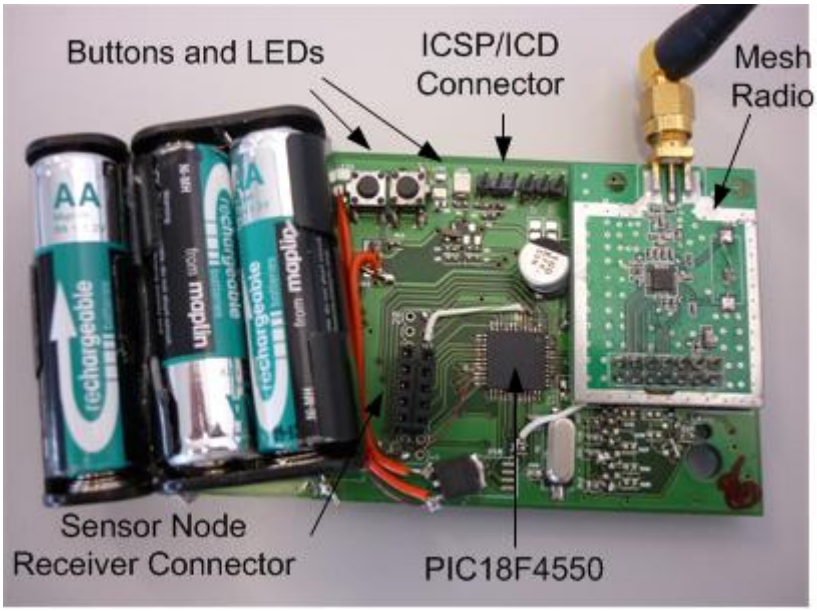


Figure 6.2: Wireless mesh node prototype

Figure 6.2 is an image of the final prototyped wireless mesh node. This single PCB design is used for all three mesh node variants.

6.1.1 Mesh Node Microcontroller Unit

The wireless mesh node utilises the Microchip PIC18F4550. This mesh node MCU was chosen for a number of reasons. This is a high performance 8 bit micro controller which can be programmed in C. It has 32 Kbytes of program memory and 2 Kbytes of RAM. It can operate at 48 MHz and perform at 12 MIPs. This MCU has 35 I/O pins and a UART interface which is use to communicate with a PC. It also has a SPI

(Serial Protocol Interface) used to interface to the mesh node radio module and a USB peripheral which supports full USB 2.0.

The design of the mesh node makes use of the ICSP/ICD (In Circuit Serial Programming/In Circuit Debugging) features of the PIC18F4550. An interface is included in the design of the mesh node to support these features. The mesh node MCU can be programmed on the board via the ICSP interface and debugged in real time via the ICD2 interface.

6.2 Mesh Radio

The mesh interface radio communications is based on the Texas Instruments sub 1 GHz transceiver chip, CC1101, operating at 868 MHz. This is a low power low cost device. In order to use this device, it requires a number of external components such as a crystal and antenna matching circuit. This radio chip together with these additional required components, and an external antenna, are designed as a plug-in module. The design of this module is based on a reference design from Texas Instruments, see Appendix II. The fabrication of this reference design module is shown in figure 6.3.

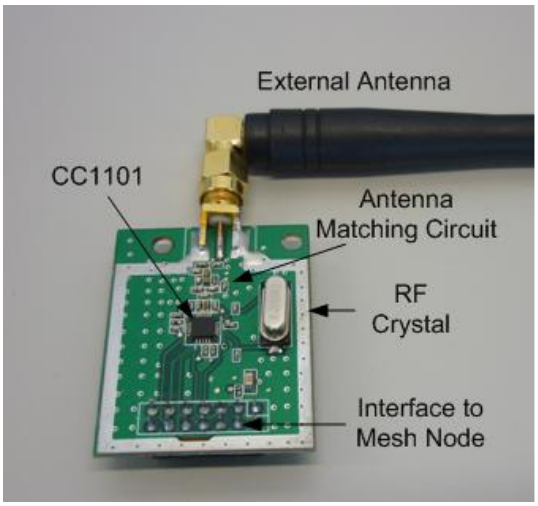


Figure 6.3: Photo of TI CC1101 868 MHz module base on a reference design

The mesh node MCU communicates with the mesh radio via SPI (Serial Peripheral Interface). This interface enables the mesh node MCU to send and receive data to and from other mesh nodes via this radio. It also allows for the programming of the radio's set of internal configuration registers. The mesh radio chip is a highly configurable device with over 40 configuration registers. Many of these need to be pre-programmed in order to operate the device in the desired manner.

Once the mesh nodes have been programmed and configured, they will have each received a unique identification and will then be ready for deployment. Once deployed as a fixed infrastructure, the mesh nodes must be initialised with a routing table. In order to accomplish this, the mesh nodes must enter a *discovery mode*. This mode will be automatically entered if the mesh node is not already initialised. An alternative method to enter discovery mode is to press and hold one of the push buttons on the mesh node. A led will flash once this mode is entered. The mesh node will then wait for a discovery broadcast and on receiving this will update its routing table and hop count. Once initialised, the mesh node will report back an acknowledgement to the base station. The flowchart in figure 6.4 describes the discovery mode in detail.

The mesh radio device has a number of built-in features which simplifies the handling of data. To send or receive data this radio transceiver has 64 byte transmit and receive FIFOs which are simply loaded or read via the SPI interface respectively. The mesh radio is configured to send a preamble automatically. On the receive side this preamble is decoded without any user intervention.

Another convenient feature is that the device can operate in broadcast mode or single destination mode. Broadcast mode is where transmissions are received and stored in the receive FIFO by all other devices in range. Single destination mode is when an id is used to specifically target another device. In this case if a mesh radio receives a data packet targeted for another device then it will ignore this data packet. This is very useful when routing data packets to particular mesh nodes.

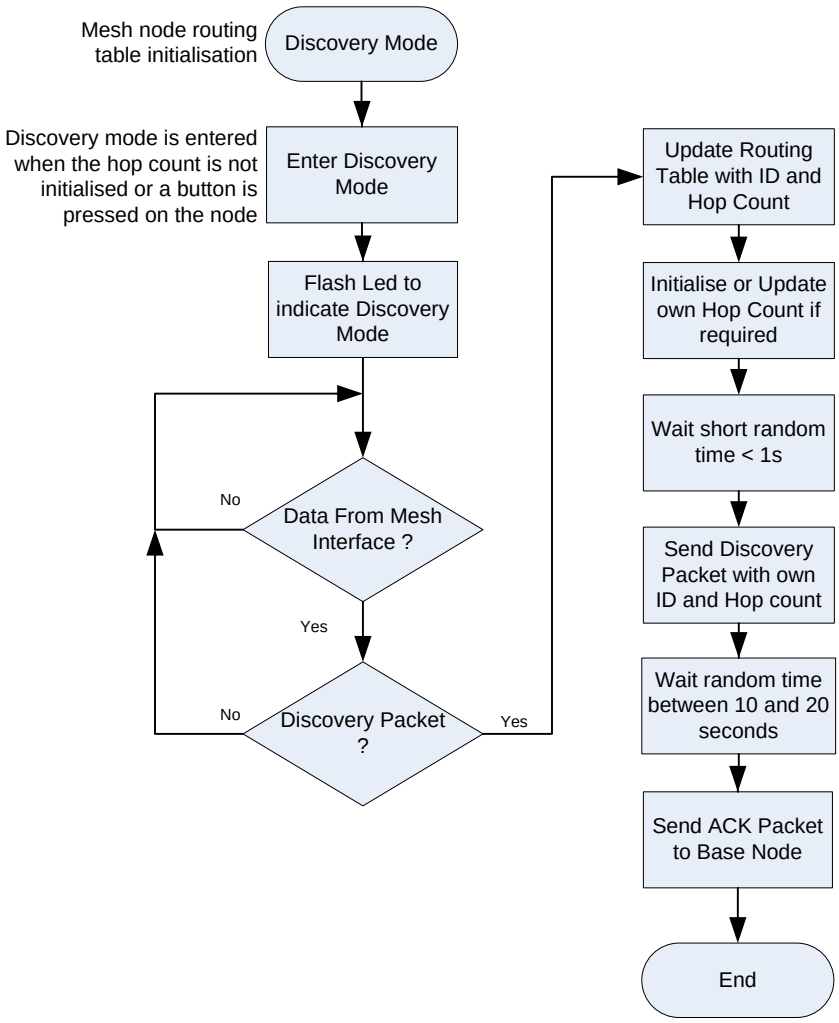


Figure 6.4: Mesh node discovery mode flowchart

Figure 6.5 gives an outline of the data packet handling for the mesh nodes. The design of this software aims to achieve a simple and reliable method for routing data to the base station. On receipt of a data packet the mesh node checks if there is any previous data packet pending transmission. If there is then the mesh node does not accept any more packets until the pending transmission is sent and the queue is empty. The transmitting node will try to transmit three times, and if it fails, then it will select an alternative route to send its data.

The mesh radio supports CCA (clear channel assessment). CCA uses the RSSI to determine if the RF channel is free. This feature supports the CSMA protocol for the transmission of data.

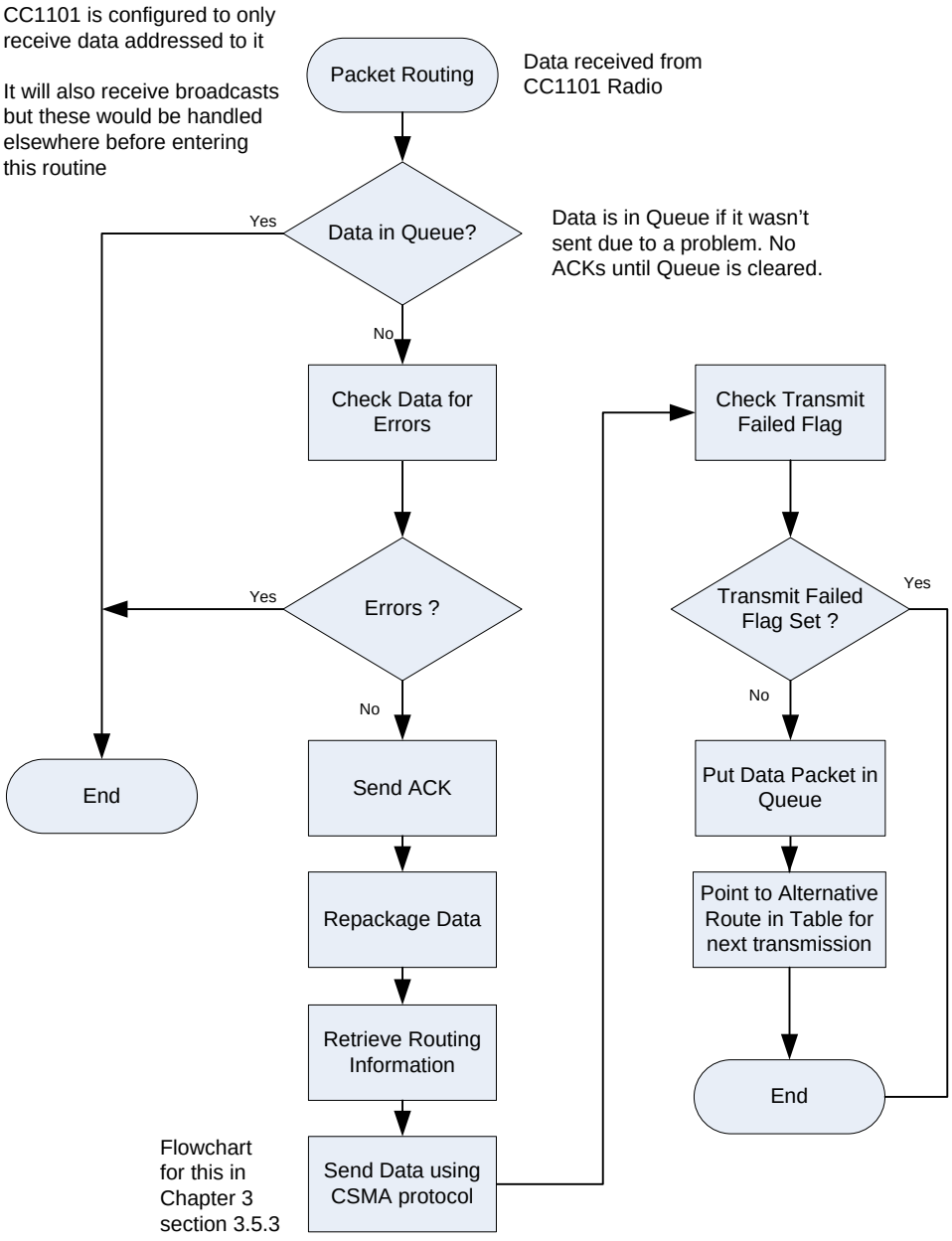


Figure 6.5: Mesh node data routing flowchart

6.3 PC Interface

The interface between the base node and the PC is accomplished by utilising an FTDI chip. This device, shown in figure 6.6, converts USB to a serial UART (Universal Asynchronous Receive Transmit) interface. The mesh node MCU has a UART peripheral on board. This interface is easy to implement and requires little programming. Even though this MCU has an on board peripheral to support a USB 2.0 interface, implementing full USB 2.0 is more complex than the FTDI option. The FTDI interface is set to a data rate of 38.4 kbits/s for testing purposes. The maximum baud rate for the mesh node MCU is 115.2 kbits/s.

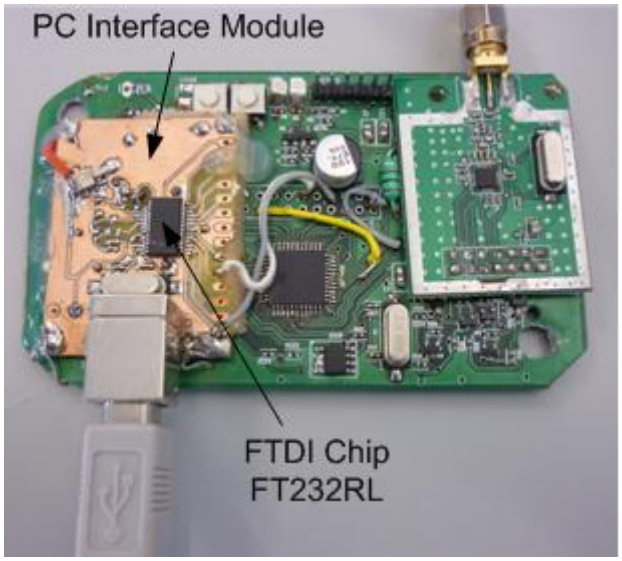


Figure 6.6: Base node module

The base node software is designed so that the device simply acts as a data interface between the PC and the mesh network. Data received from the PC is retransmitted by the mesh radio to the mesh network. Data received by the base node from the mesh network is simply checked for errors, acknowledged, and then sent to the PC.

It can be seen from figure 6.7 that the base node software is based around a simple state machine waiting for data from either the PC or the mesh radio. The state is determined by the use of two interrupts. A UART asynchronous receive interrupt is

used for receiving data from the PC. An external interrupt, driven by one of the mesh radio signals (GD0), is used to signal data from this radio device.

The verification of data to and from the PC and base node is achieved by using RealTerm, a serial terminal application program on the PC.

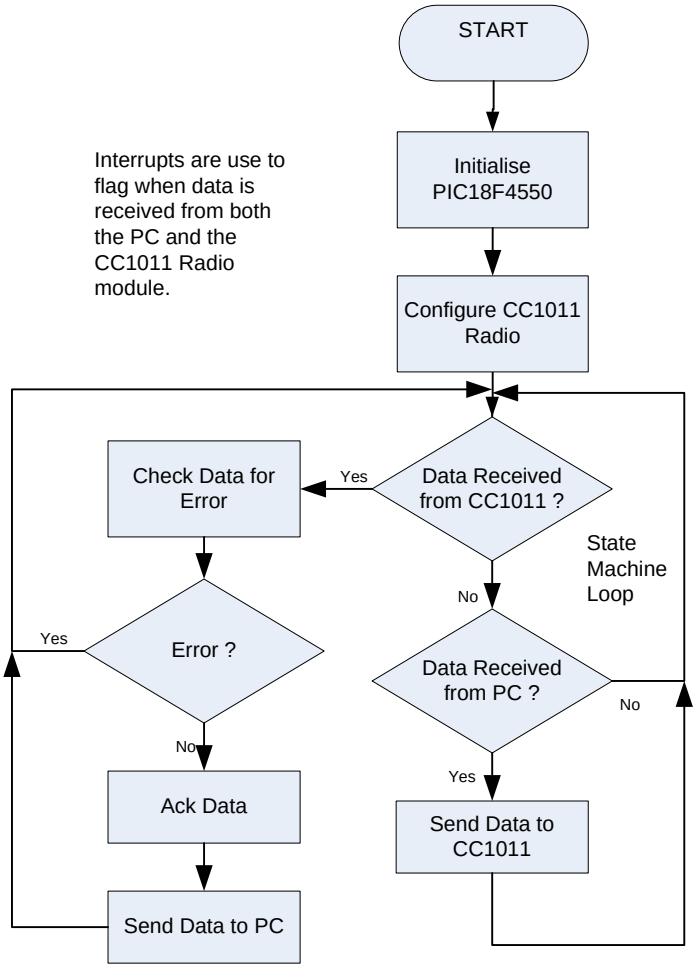


Figure 6.7: Flowchart of base node software structure

6.4 Sensor Node Interface

The sensor node interface is a wireless interface provided by an ASK radio receiver module. This receiver is a 433 MHz device compatible with the transmitter in the sensor node. A dedicated sensor interface MCU (PIC16F688) is used to decode the data received by this radio. This MCU also stores and forwards this data to the mesh

node MCU. A second MCU in the mesh node aids in distributing the processing tasks and simplifies the overall software development. The flowchart in figure 6.8 is a description of the software on board the PIC16F688.

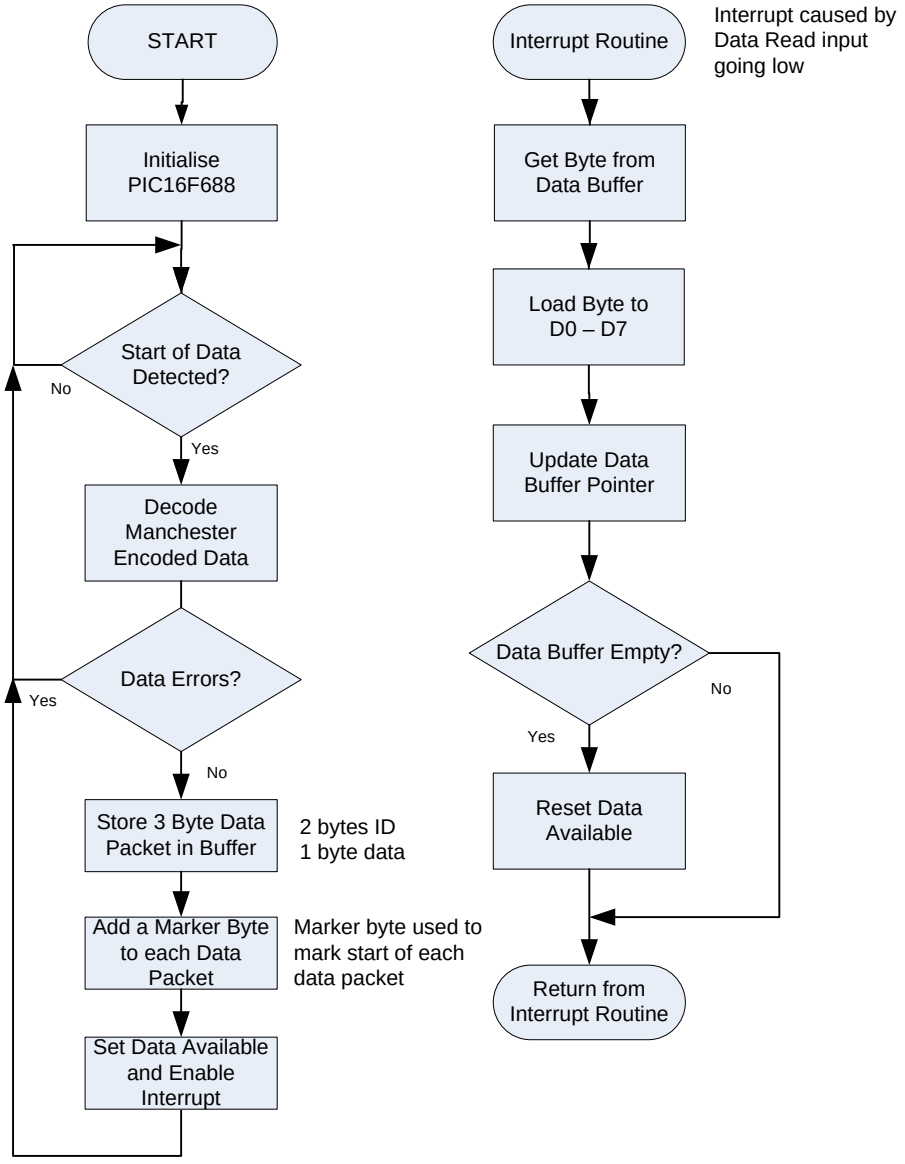


Figure 6.8: Software flowchart for PIC16F688

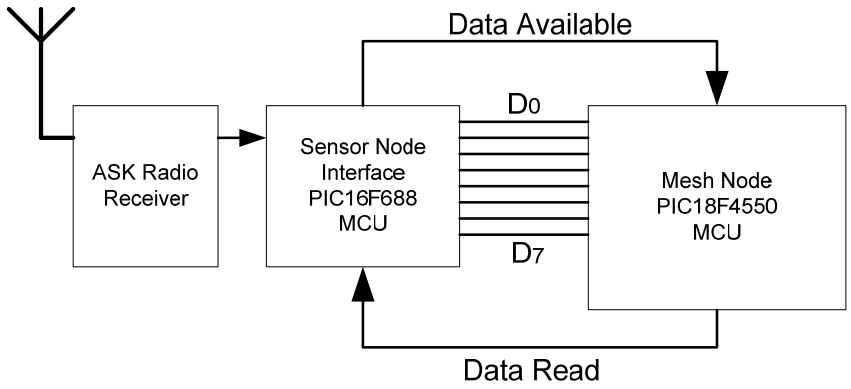


Figure 6.9: Sensor node receiver interface to mesh node

A simple interface is used between the two MCUs. Data is transferred from the sensor interface MCU to the mesh node MCU through an 8 bit parallel interface, indicated in figure 6.9 by D_0 to D_7. Two additional signals are used to control the flow of data. *Data Available* is signalled by the sensor interface MCU to indicate that data is present in a data buffer. Every time the *Data Read* line is pulled low by the mesh node MCU this causes an interrupt. An interrupt routine, on the sensor interface MCU, reads the first byte in the data buffer and writes it to the data port D_0 to D_7. The data buffer pointer is then updated to point to the next byte. If the data buffer is empty the *Data Available* signal is reset. When data is stored in the buffer an extra byte is added to each sensor node 3 byte data packet. This byte is used to identify the start of each 3 byte data packet. This extra byte is then discarded by the mesh node MCU once it has received the sensor node data.

This interface allows the mesh node MCU to control the rate at which data is received from the sensor node interface. This interface is integrated into the final design of the mesh node and can be seen in the mesh node circuit schematic diagram in Appendix I.

Finally, the software required to control this interface and read data from the sensor interface is described by the flowchart in figure 6.11.

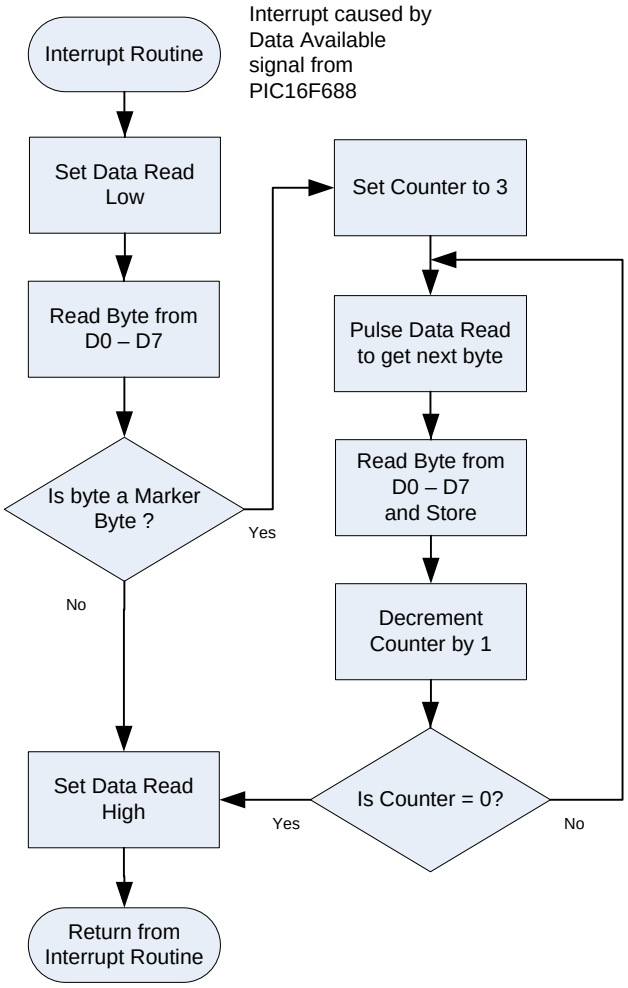


Figure 6.11: Reading data from sensor node receiver

6.5 Power Source

The proposed WMSN requires the infrastructural mesh nodes to be powered continuously. The power source for these wireless mesh nodes will depend on their deployment. In this system the radio devices account for most of the power consumption. A radio clearly uses power while it is transmitting or receiving. It also uses power while it is idle waiting to receive data (idle listening). In this mode it consumes approximately the same power as when it is receiving.

The base node must be connected to a PC to operate as designed. It is powered from by the PC through its USB (FTDI) interface and therefore batteries in the base node are not required.

The current consumption for the mesh node is 33mA when everything is switched on. This can be broken down into 5mA for the main board with the PIC18F4550 MCU, 8mA for the sensor node radio receiver module, and 20mA (average measurement) for the mesh radio module based around the CC1101. This value of 33mA could be reduced by implementing some power saving techniques. The mesh radio supports a *wake-on-radio* feature which could reduce the power significantly. This feature allows the mesh radio to remain in a low power state until it receives an RF signal. This helps reduce the power consumption by eliminating the need for idle listening.

The mesh node is normally powered by batteries where mains electricity supply is not available. The current prototype utilises a battery pack of three rechargeable nickel metal hydride (NiMH) AA type batteries. When fully charged this battery pack produces over 3.6 volts and has a capacity of 2.5Ah (can supply 2.5 amps for one hour). This battery pack could power the mesh node for a maximum of 75 hours. In order for the mesh node to be continuously powered, it requires a supplement power source. If the mesh node is conveniently deployed next to a mains electricity supply, then this could be used through an AC adapter. It is likely that a mesh node will be deployed outdoors with no possibility of connection to mains electricity. In this case the supplement power source is derived from renewable sources of either wind, solar, or a combination of both. This supplement power source can be used to charge the batteries and power the mesh node.

Trickle charging is a very simple method that allows batteries to be continuously charged without causing any damage to the battery pack. As a guideline, the maximum charging rate for trickle charging NiMH batteries is one tenth the capacitance (C/10) of the battery pack i.e. 250mA to allow for a large margin of safety. Here, a charging rate of C/20 has been selected (i.e. 125mA).

The following is the estimated requirements to power a mesh node continuously, using batteries and a solar panel as the supplement power source. These requirements are based on a mesh node located outdoors in Ireland during the months of December/January. This was chosen as a worst case scenario for solar power, as there are only approximately eight hours of daylight per day in these months.

The mesh node current is 33mA on average. During the eight hours of daylight it is necessary to charge the battery pack sufficiently so that it can supply 33mA for the remaining sixteen hours, a total requirement of 800mAh. Using a charging current of 125mA will charge the battery pack to 1000mAh in the eight hours. In order to reach this 1000mAh charge, the battery pack should not be discharging i.e. the mesh node should not be running off the battery pack. The solar panel requirement is to supply 125mA charging current for the battery pack and also to supply 33mA current to operate the mesh node. The solar panel should therefore be capable of producing 158mA on average during the eight hours of daylight. Details of tests and implementation of solar panels as an energy scavenging source will be presented in chapter 7.

The house node is powered from the house electricity supply via a suitable AC adapter. A battery supply is an option for the house node but it would not be recommended as the single source of power as the battery would only power the house node for 75 hours, assuming the same battery pack is used as in the mesh node. A more sensible use of batteries in the house node is to use them as a temporary power source when normal power supply is interrupted for relatively short periods of time.

6.6 Preliminary Test and Development

The final hardware design of the mesh node is complete. The final circuit schematic is shown in Appendix I. The mesh nodes and their associated modules pictured in this chapter are final prototypes which have been used during the testing of various aspects of the software design. With the prototype hardware available many of the mesh nodes functions and operating parameters have been tested at bench level first before deployment at a system level. This section addresses some of the preliminary bench level testing.

Eight mesh nodes, eleven sensor nodes and a base station have been prototyped. Much of the testing has been end-to-end testing with results and verification monitored on a PC using the terminal emulation program RealTerm.

The *Discovery Mode* and *Routing* routines have been tested using the test setup shown in figure 6.12, where the circles indicate which nodes are within RF range of each other.

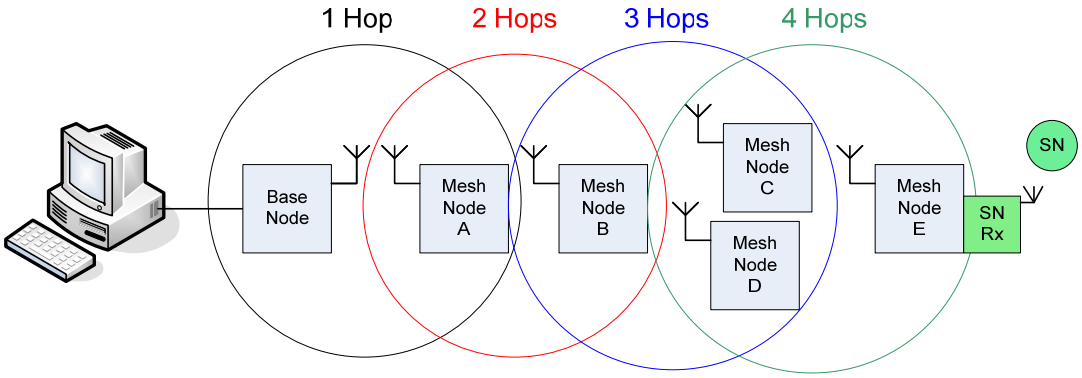


Figure 6.12: Mesh Node Test Setup

Discovery Mode Test

This test was to verify the basic operation to initialise the mesh nodes with a hop count and routing information. The following is an account on how this test was conducted.

All mesh nodes were placed in discovery mode. Nodes which did not already have a hop count automatically entered this mode. Those with an existing hop count were forced into discovery mode by pressing and holding the push button until a LED flashed.

A discovery command was sent by the PC from RealTerm. This command was then relayed as a broadcast by the base node. Mesh Node A was positioned to be the only node in RF range of the base node. Mesh Node A then relayed this discovery broadcast to Mesh Node B which in turn relayed it to Mesh Nodes C and D. The final node to receive this broadcast was Mesh Node E.

This test was configured so that all nodes would report their hop count and routing data to the base node after 2 seconds. This test was verified using RealTerm to monitor the data packets received by the PC. All nodes were correctly initialised.

Routing Test

The second test performed was to verify the acquisition of a sensor node data packet and to route this packet back to the base station (PC and base node). This test could only be performed once the mesh nodes had been initialised.

In this test a sensor node receiver module (SN Rx) was connected to Mesh Node E. A sensor node (SN) was then activated within RF range of this mesh node. The PC was then monitored to ensure the correct sensor node data was received. Sensor data was acquired and noted correctly.

These preliminary tests were performed to verify the functionality of the mesh nodes at bench level during the design phase. The chapter 7 deals extensively with the deployment, testing and verification at a system level.

6.7 Mesh Node Cost Analysis

One of the main goals of the design was to realise a low cost system. Tables 6.1 shows the cost breakdown for the mesh node. These costing have been validated where possible by obtaining prices from the following online component distributors DigiKey, Microchip Direct, Radionics and Farnell. Prices for PCBs and have been obtained from PCB-Pool. The total cost of mesh nodes in quantities of one thousand is €21.50per unit. To keep the costs low, quarter wave wire antennas are used on the mesh nodes. These antennas have no price impact on the overall cost. The cost of deployment is also relatively low. The deployment of the infrastructural mesh nodes incurs some costs with regard to positioning and powering. This does not require any specialised skills and could be undertaken by the housing community with little instruction.

Part	Description	Each € 1+	Each € 1000+	Qty	Price € 1+	Price € 1000+
CC1101	Radio Transceiver	1.70	1.00	1	1.70	1.00
PIC18F4550	Main Microcontroller	3.50	2.00	1	3.50	2.00
PIC16F688	Slave Microcontroller	1.00	0.80	1	1.00	0.80
HRR30	433MHz Radio Module	6.00	4.00	1	6.00	4.00
AA Battery	Rechargeable 2500mAh Battery	2.50	1.00	3	7.50	3.00
PCB	Mesh Node PCB	10.00	3.00	1	10.00	3.00
ABS Box	Enclosure	3.00	1.50	1	3.00	1.50
MC-SP0.8	Solar Panels	7.00	4.00	2	14.00	4.00
ElecMec	Switches, LEDs, Connectors	2.00	1.20	1	2.00	1.20
Misc	All other components	2.00	1.00	1	2.00	1.00
	TOTAL				**50.70**	**21.50**

Table 6.1 Breakdown cost of wireless mesh node

7. SYSTEM DEPLOYMENT AND VERIFICATION

One of the objectives of this research was to realise and fully test this application specific WMSN. To achieve this goal the system had to be deployed in a suitable location to facilitate testing. As mentioned in chapter 3, the deployment and testing of the system was mainly carried out at the Electronic Engineering building at NUI, Maynooth (NUIM). Some additional testing also took place in a housing estate in Maynooth. This chapter presents the testing and verification of this system which has been deployed, to date, for a period of six months from February to August 2011.

7.1 System Setup

This section details the system components and setup of the test network deployed at NUIM. The system consists of eight mesh nodes, eleven sensor nodes and a base station. The mesh nodes were deployed as a mesh network over three floors of the Electronic Engineering building allowing for ease of modification and testing purposes. Figure 7.1 depicts the location of each of these nodes.

One of the eight mesh nodes (MN8 in figure 7.1) has been located outdoors. This mesh node is powered by a combination of rechargeable batteries and solar panels and is used to test this energy scavenging method. Results of this testing will be discussed later in this chapter. Of the eleven sensor nodes, eight are deployed as static nodes and three are deployed as mobile nodes for radiolocation.

Three of the static nodes operated as temperature sensors, reporting their temperature every minute. The remaining five static sensor nodes were used as door activation monitors. These sensors were deployed over the most active doors in the building and activated by the vibration of the door opening/closing. These doors were in corridors and stairwells. These doors were chosen as they would generate a steady stream of data to the base station. Figure 7.2 shows one of the static nodes positioned over a door.

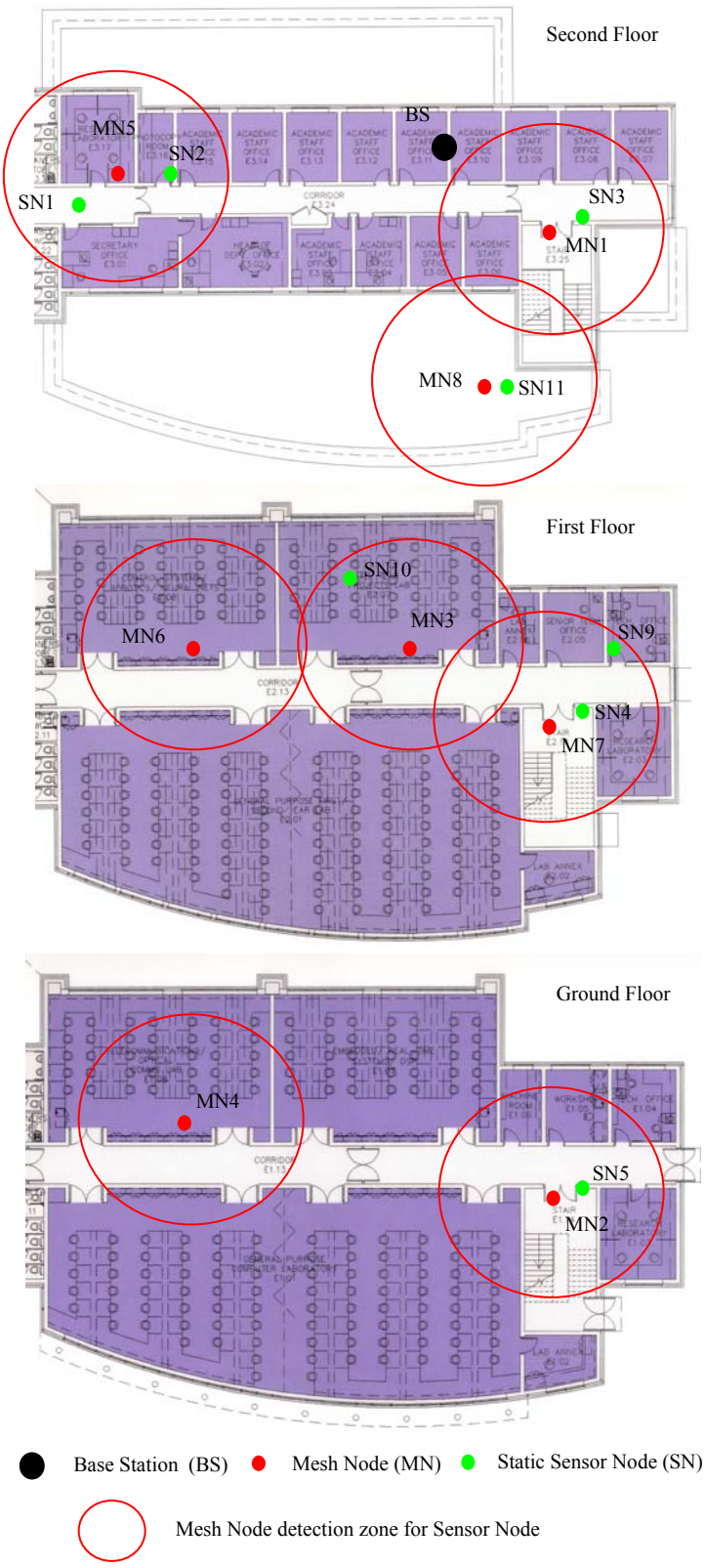


Figure 7.1: WSMN deployment at Engineering Building NUI, Maynooth

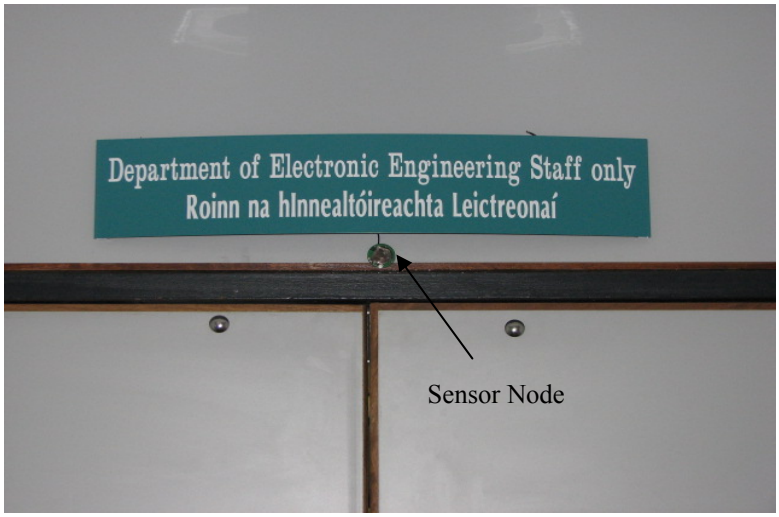


Figure 7.2: Static sensor node monitoring door activation

The three mobile sensor nodes were used for tracking. Two of these nodes were used for tracking people. One utilised a wrist band as shown previously in figure 5.7, while the other was carried in a pocket of the person. The third sensor node was used for tracking a key shown here in figure 7.3.

Figure 7.3: Mobile sensor node used for tracking a key

The final part of the system is the base station. The base station is a PC connected to a mesh network transceiver. This transceiver simply passes data between the mesh network and the PC, it does not process or analyse any data. The rate at which this data is transferred is 38.4 kbits/s. The PC is then effectively the base station. The physical location of the base station in the network is indicated in figure 7.1.

During bench level testing of nodes the base station utilised the terminal software RealTerm to monitor received raw data and to send some basic commands. In order to test and monitor the system more efficiently a PC application was written in Visual Basic to provide a graphical user interface (GUI) for the network. The PC was also permanently connected to the web to enable information and network status to be updated to a website. A GSM modem was also used to allow the system to send information by text messaging. These and other features will be presented in more detail in this chapter.

Part of the setup requires mesh nodes to be power continuously with or without the use of mains power. As the test system is deployed mainly indoors, all but one mesh node is powered from the mains. The mesh node located outside uses a solar panel and rechargeable batteries. Section 6.5 outlined the solar panel power requirement in order to maintain constant operation during the shortest days of the year. Figure 7.4 shows the outdoor mesh node together with the solar panels and a solar data logger.

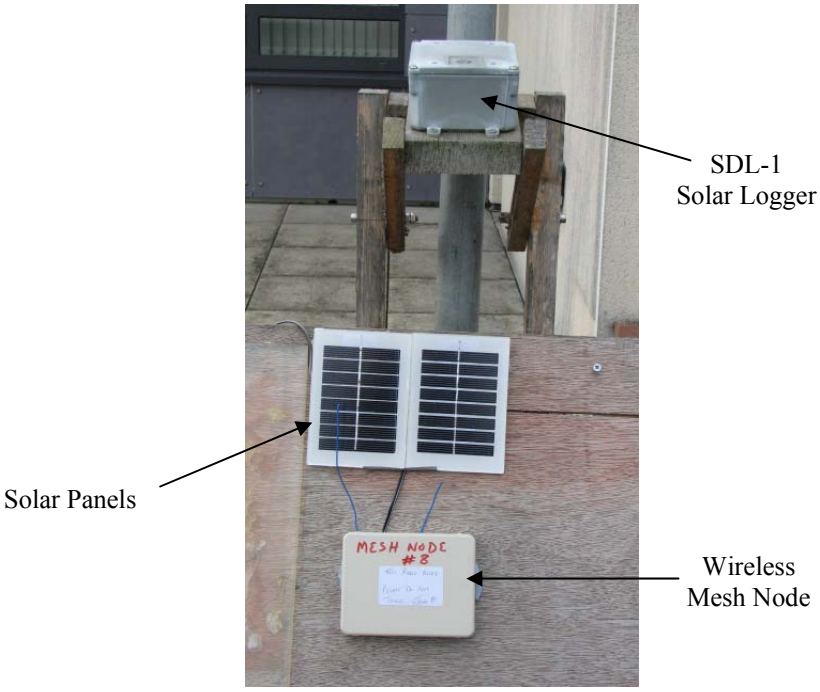


Figure 7.4: Mesh node with solar energy scavenging

Prior to the deployment of the system a number of tests were performed on the outdoor setup shown in figure 7.4. The solar data logger (SDL-1 from Micro Circuit Labs) has been obtaining daily solar irradiance levels at the site from October 2010 to

date. Both the solar panels and solar logger were set to be south facing to maximise their exposure to the sun. Figure 7.5 shows the results from the solar logger for the period October 2010 to April 2011.

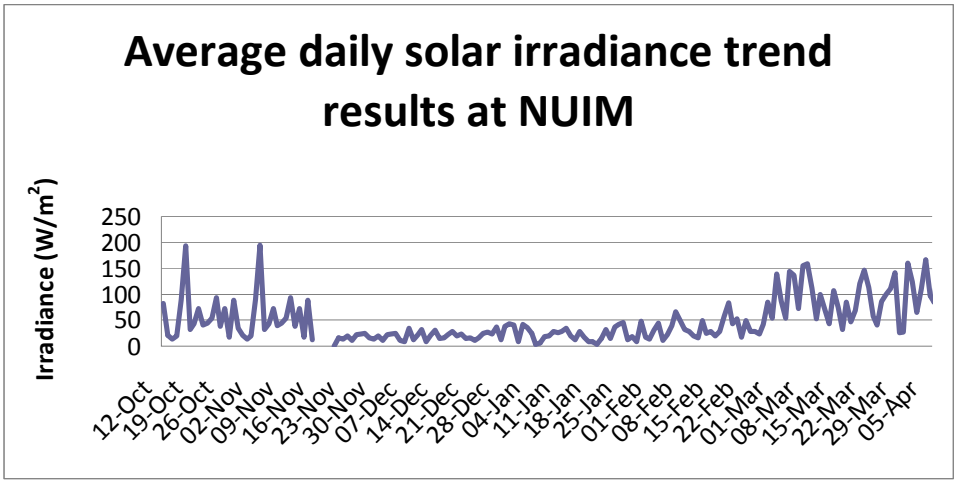


Figure 7.5: Solar data acquired at NUIM

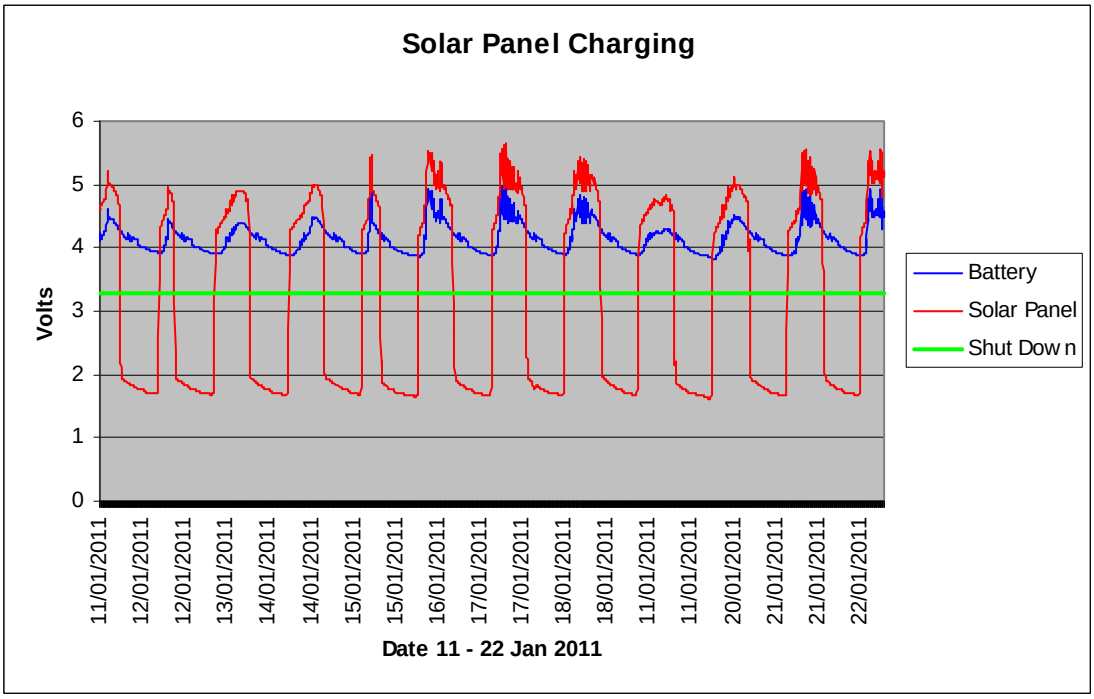


Figure 7.6: Solar charging of outdoor mesh node

As part of this initial testing the solar panel and battery voltages were logged every five minutes. Figure 7.6 shows results for the period 11-22 January 2011. During this period there was approximately 8 hours of daylight each day. These were among the

shortest days of the year and provided a good scenario for this solar energy scavenging test. The green line in figure 7.6 indicates the shut down voltage (3.3V) for the mesh node. While either the battery or solar panel voltage is above the shut down voltage, the mesh node remains powered.

On completion of these tests MN8 was deployed as part of the system. The solar panel voltage is monitored as part of the housekeeping information and reported back to the base station every minute.

7.2 System Operation

The system is monitored and controlled by customised PC software, as shown in figure 7.7. This GUI has been written specifically for the test network set up in the Engineering Building at NUIM.

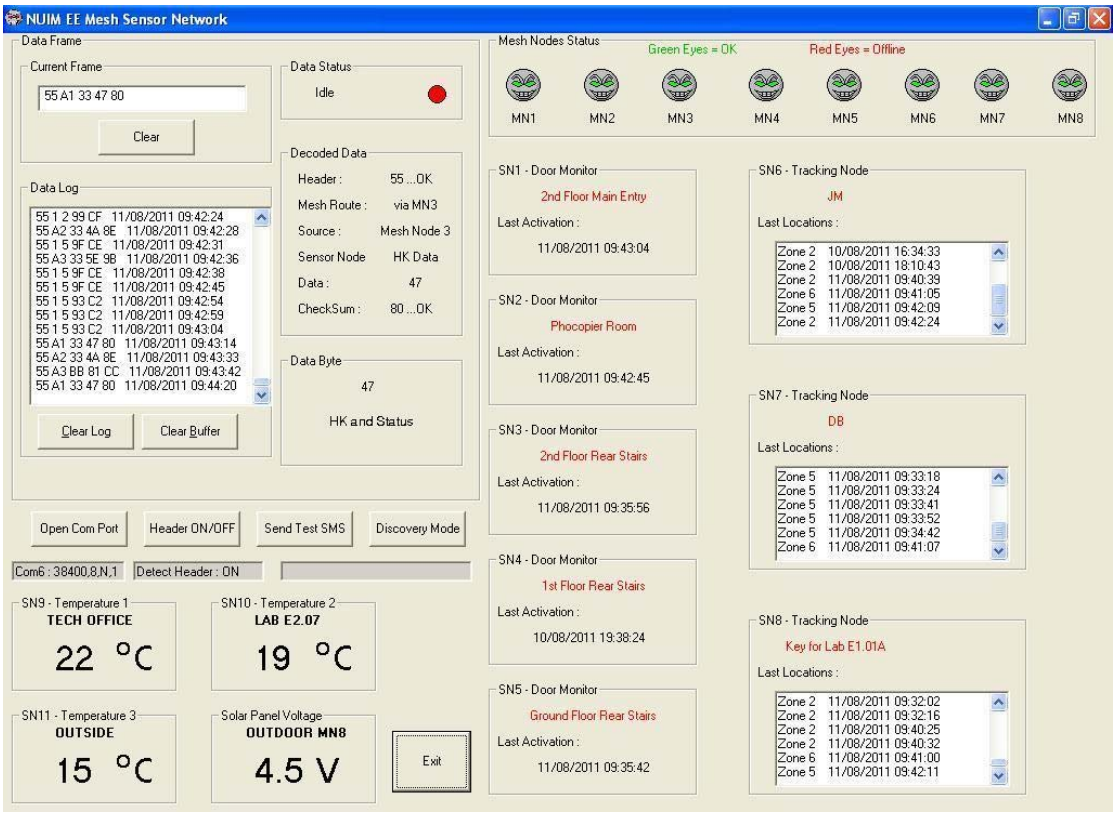


Figure 7.7: GUI for mesh sensor network

The top left of the GUI screen displays the current data packet. Below this a log is displayed of all data packets received, this log is also saved to file. The decoding of the current frame is also displayed. All data packets have a header byte of 0x55. The software searches for this byte before displaying the data packet. There is an option to switch off the header byte detect. This will allow all data to be displayed as it is received. This can be useful for debugging purposes. Other commands include initiating 'discovery mode' and the sending of a test SMS.

Latest readings from the three temperature sensors and the solar panel voltage are displayed at the bottom left of the screen. These are updated every minute. The eight icons at the top right of the screen indicate the status of the eight mesh nodes. If an icon has green eyes this means that the associated mesh node has sent data within the previous ten minutes. If a mesh node has no data to send a status data packet is sent within this ten minute period, ensuring the eye remain green. If communication is lost with a mesh node for more than this period the eyes of the associated icon turn red.

The last activation of the five monitored doors opening/closing is shown in the middle of the screen. Tracking data from the three mobile sensor nodes is time stamped and logged. A history of tracking location is important so that tracking direction can be inferred. The tracking ability of the system will be discussed in more detail later in this chapter.

7.3 Web and SMS features

Part of the system operation was to display system information on a webpage. As part of the validation process a webpage was updated once every minute with the current status of the system (http://www.eeng.nuim.ie/~jmaloco/wsmn.php). The system also supports the use of SMS text messages. The validation of the SMS feature was to verify that the base station could send and receive SMS messages. To test this, a Huawei E220 USB modem was used to send and receive text messages. The modem operated in serial AT command mode and was easily controlled by the base station GUI software.

7.4 Radiolocation

The method used for mobile sensor node tracking, or radiolocation, and the results obtained are discussed in this section. The majority of the testing of the network deployment took place at NUIM. In the case of radiolocation, a test network was also deployed in a housing estate to obtain results from the target environment.

7.4.1 Radiolocation Testing at NUIM

The radiolocation method adopted for the system is that of last known location/zone. Figure 7.1 shows the deployment of the network, the location of the mesh nodes and their associated detection zones for mobile sensor nodes, depicted by the red rings. The radius of these detection zones is governed by the transmission range of the sensor nodes. With the deployment area being relatively small (compared to a typical housing estate) the sensor node transmission range was reduced to approximately 5m. Any sensor node transmitting within 5m of a mesh node would be detected. This was achieved by a combination of reducing the output power of the sensor node transmitter and antenna selection.

Although the mesh node detection zone covered a small area, the layout of the target area in figure 7.1 was conducive to radiolocation. The mesh nodes were strategically positioned to cover corridors, stairways and main entrances/exits. This deployment ensured that no sensor node could enter or leave the building (by normal means) without passing through one or more detection zones. Detection was only guaranteed as long as the sensor node transmitted while in a detection zone.

In order to guarantee the detection of a mobile sensor node in a region of interest, the entire area is required to be covered by contiguous detection zones and the sensor node should transmit its first data packet immediately on activation. This would ensure that the initial movement of the sensor node would then be reported. The first packet would still be transmitted at a random time as the activation of a mobile sensor node is random.

The alternative to having contiguous detection zones is for the sensor nodes to transmit more often so that at least one transmission is guaranteed while passing through a detection zone. This can be achieved by reducing the 10s transmission windows and the 1.5 minute sleep time. The setup at NUIM does not have contiguous detection zones so this second option was adopted. As a result the transmission window was reduced to 5s and the sleep time removed. This compromise has proved to be reliable in detecting mobile sensor nodes.

7.4.2 Radiolocation Testing in Housing Estate

The network deployment in the housing estate is shown in figure 7.8. This was a temporary deployment and all tests were performed over a three hour period. The mesh nodes were positioned approximately 50m apart in a grid pattern and were powered by batteries only. The transmission range of the sensor nodes were set to around 40m. The ring around each mesh node in figure 7.8 is the sensor node approximate transmission range relative to each mesh node. Effectively this ring is the mesh node detection zone for a sensor node. All mesh nodes were in range of each other and of the base station. Data packets from all mesh nodes were directly sent to the base station. Unlike the set up at NUIM the detection zones for mobile sensor nodes overlapped, covering the entire region of interest. The software in the mobile sensor nodes was modified so that the node would transmit immediately on activation. With this set up a number of tests were performed.

The first test was to ensure that the reported location of a sensor node corresponded to the map in figure 7.8. This was achieved by placing a sensor node in the locations indicated in the map and recording data at the base station. The locations of SN2 and SN3, in figure 7.8, were chosen to ensure that their location would be reported by multiple mesh nodes. This first test was carried out while the sensor nodes were stationary. The result from this confirmed this operation of the system.

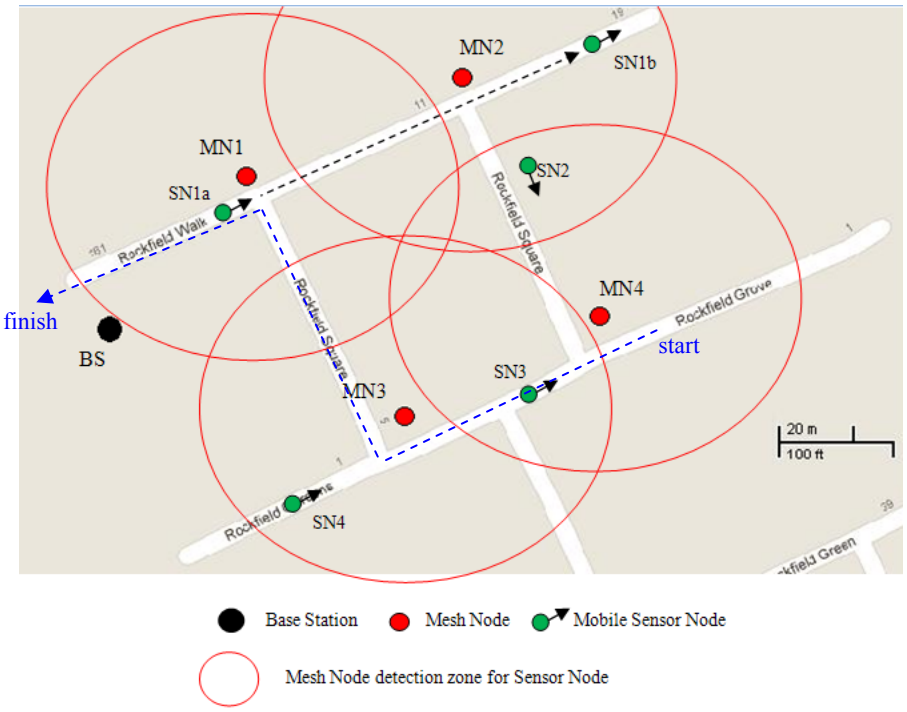


Figure 7.8: WSMN housing estate deployment

To verify the radiolocation of mobile sensor nodes a set of controlled tests were done. These tests consisted of walking, running and cycling predetermined route around the deployed network. One such route is indicated by the dashed line in figure 7.8, between SN1a and SN1b.

While the walking tests proved reliable some potential problems were revealed during the running and cycling tests. The main issue is with the sleep time of the sensor nodes which occurs after three transmissions on the detection of movement. This sleep time was set to 1.5 minutes as per the system design. During this sleep time it was possible to run or cycle the route on the map marked with the *start* and *finish* labels without being detected by MN3 or MN1. This was achieved by activating the sensor node at the *start* location and waiting 30s to ensure all three transmissions had been sent and the sensor node had entered sleep mode. A run or cycle to the *finish* location could then be done without detection. Although this may be perceived as a flaw, the system did report the last known location as zone MN4 which from the systems perspective was correct. This is a similar problem to that discussed in section 7.4.1 with regards to the sensor node tracking at NUIM.

7.5 Reliability

Over this six month testing period, the deployed network at NUIM has evolved to be very reliable. During the first three months, hardware and software tests were carried out on individual system components. The base station GUI was also developed during this period. This helped establish a reliable platform for the second three months when most of the system level testing and data monitoring was performed.

7.5.1 Sensor Node Reliability

The final design of sensor nodes had been extensively tested over a two year period prior to the system level testing. The sensor nodes were then deployed at a system level without any changes. The activation of the sensor nodes by the passive vibration sensor (CM1344) has been very reliable. Both static and mobile nodes have operated as expected. No software reset or battery replacement has been necessary for any sensor node during the test period.

The only issue with the sensor node was susceptibility to interference. The sensor nodes operate on a single radio frequency of 433MHz, utilising a simple carrier on/off modulation scheme. With the test network deployed in an electronic engineering department there were some occasions when some student projects utilising this same frequency would cause interference resulting in occasionally corrupted data packets from sensor nodes to mesh nodes. On one occasion this was a particular problem when a project was mistakenly left on transmitting continuously for a number of days. On discovering the data loss it was easy to track down the offending device due to it's proximity to a static sensor node with which it was interfering. There should be little or no interference when deploying the network in a housing estate.

7.5.2 Mesh Node Reliability

The hardware platform for the mesh node has proved reliable. The sensor node interface radio operating at 433MHz was susceptible to radio interference at NUIM as described in the previous section. The mesh radio interface operating at 868MHz was reliable throughout the testing period. No 868MHz radio interference was detected during the tests. One of the main reasons for using the 868MHz band is that this band

is less congested than alternatives such as the 2.4GHz band. The 2.4GHz band is utilised in many applications including Wi-Fi and a system based on this frequency would have to contend with many possible interfering devices, especially in a building full of technology such as the Engineering building at NUIM.

At a system level the mesh network reliability has been monitored by the GUI on the base station. During the second three months of testing this GUI performed as the main testing tool for monitoring the operation of the system and the status of the mesh nodes.

7.6 Scalability

The reliability tests have shown that the system deployed at NUIM is reliable. This system has operated for three months uninterrupted with few errors. This is partly due to the fact that the scale of the system is small and hence the data traffic is small. This section now addresses the issue of scalability.

Fully testing scalability through experiment was not practical as it would have required a large number of mesh nodes and an even greater number of sensor nodes. Some tests and calculations have been performed in order to estimate the likely scalability of the system. These results will be discussed here.

The physical scalability of the current system has an upper limit of approximately 250 mesh nodes and 65,000 sensor nodes. These limits are governed by the 8 bit addressing of the mesh nodes and the 16 bit addressing of the sensor nodes. These numbers of mesh and sensor nodes far exceed a typical deployment requirement for the targeted housing estate.

In chapter 3, figure 3.4 depicted a typical housing estate deployment which utilised 49 mesh nodes and ~1,320 sensor nodes. This typical housing estate deployment is used as a benchmark to establish if the current network design could satisfy this requirement. A number of factors influence the scalability of the mesh network. These include data rate, the number of hops required to reach the base station, packet copying of data received and then re-transmitted, and also data collision.

The system has been designed to have a sustainable asynchronous data rate of 38.4 kbits/s. This asynchronous data has the overhead of a start bit and stop bit for each byte. So the actual number of bits transmitted in a mesh node data packet of six bytes is 60. The time required to send the data packet is therefore ~1.6ms.

The following tests were performed to ascertain values which could be used in determining the scalability of the system. The first test was to determine the maximum sustainable sensor node data packet rate through a single hop to the base station.

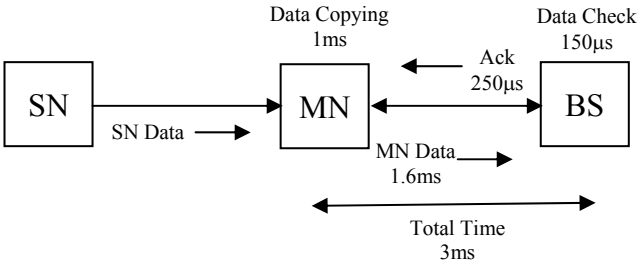


Figure 7.9: Single hop data transfer

Figure 7.9 shows the various timings required to transfer a single six byte data packet from a sensor node (SN) through one mesh node (MN) to the base station (BS). The 1ms for data copying is the time required to copy the data from the sensor node receiver interface to the mesh node microcontroller. The mesh node data transmission requires 1.6ms. Checking the received data packet by the base station takes a further 150µs. This is followed by a single byte acknowledgement from the base station which takes another 250µs. In total the transfer takes 3ms.

To verify this, a sensor node was programmed to continuously transmit 200 packets of data separated by 3ms when activated. These packets were received by one mesh node and relayed directly to the base station. All 200 packets were received by the base station. When this 3ms was reduced packet loss occurred.

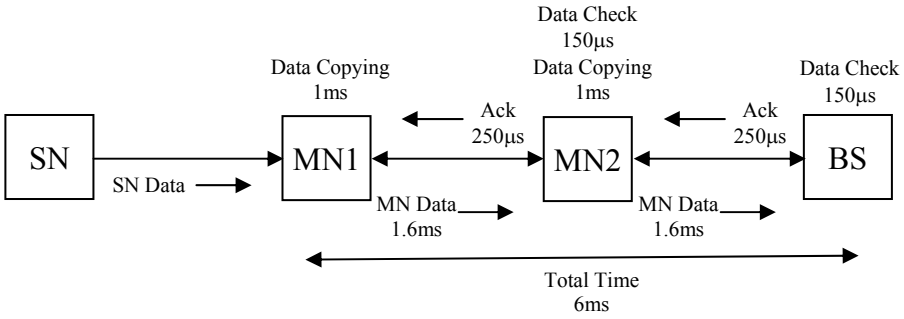


Figure 7.10: Multi hop data transfer

The same experiment was done for a two hop scenario, as shown in figure 7.10, and again for three hops. It was found that the gap between sensor node packets had to be increased to 6ms for two hops and then to 9ms for the three hops before all 200 data packets were received by the base station. It can then be assumed that a mesh node can only receive sequential sensor node data packets as long as they are separated by an additional 3ms. This effectively increases the sensor node data packet length from 2ms to 5ms. These tests were performance in a controlled setup were sensor node data was transmitted sequentially therefore eliminating the possibility of potential data collision. To estimate the reliable scalability of the system potential data collision must be taken into account.

The reliable scalability is determined by the likelihood of data sent by a transmitting node successfully reaching the base station as the number of nodes increase. This analysis determines the reliability over a two minute period. This time was chosen as it represents the three 10s transmission windows followed by the 1.5 minute sleep time for the sensor nodes.

The upper bound for sensor node data packet throughput between two mesh nodes is two minutes (120,000ms) divided by the total time to receive and transfer sensor node data (5ms). This results in the possibility to transmit 24,000 data packets between two mesh nodes within this two minute period. This is effectively the number of transmission slots.

The protocol used between mesh nodes is based on CSMA. With CSMA any detectable potential collision can be avoided. However, some collisions are unavoidable such as in the case of Hidden Terminal which was discussed in section 2.2.4.

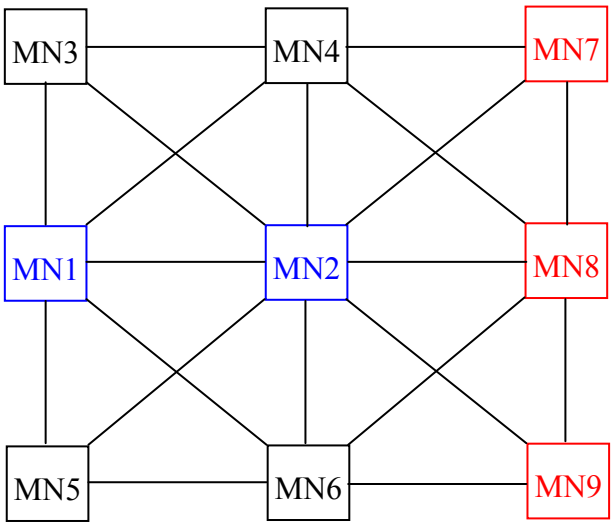


Figure 7.11: Unavoidable data collision in grid deployment

Figure 7.11 shows the grid deployment of nine mesh nodes. When MN1 wants to send data to MN2 it can detect a potential collision from five mesh nodes, MN2 to MN6. The remaining three mesh nodes, MN7 to MN9, are outside radio range of MN1 but in radio range of MN2 and therefore could cause a data collision at MN2. So in this grid deployment we can assume that three out of eight potential data collisions could be real collisions resulting in a loss of data. This would then require a re-transmission of the data packet. Tests have shown that this re-transmission takes 4ms in total, 1ms acknowledgement timeout and 3ms for the complete data transfer for the re-transmission.

The above information has been used to plot the scalability of the system in terms of the probability of a successful data transfer from a sensor node to the base station. See figure 4.19 in chapter 4.

Part of the scalability testing includes the use of a data loss threshold. This is the calculation of the point at which the required throughput exceeds the available data bandwidth over a two minute period and data loss is inevitable. The data bandwidth in this case is 24,000 data packets. Collided data above the data loss threshold may be recoverable through retransmission.

The data loss threshold (DLT) is given by the following formula:

$$DLT = \frac{DP_n P_{col} U_{col} RT_{col}}{T_{\max} - (DP_n T_{dp})} \qquad 7.1$$

where DP_n is the number of data packets, P_{col} is the probability of collision, U_{col} is the fraction of unavoidable collisions, RT_{col} is the time required to re-transmit a collided packet, T_{max} is the maximum time available and T_{dp} is the time required for sending a data packet.

The following is a worked example of equation 7.1 for 4,000 sensor nodes. Each sensor node transmits 3 data packets and each data packet requires 5ms this results in a total time of 60,000ms. The maximum time available is 24,000 by 5ms which is 120,000ms. The potential collision for 4,000 nodes is 0.57 (see figure 4.19) which results in 2,280 nodes of which 3 out of every 8 are potentially unavoidable collisions, as discussed previously. Re-transmitting each of the potentially unavoidable collisions requires 4ms. This can be formulated as follows:

$$DLT = \frac{12{,}000 \times 0.57 \times \frac{3}{8} \times 4}{120{,}000 - (12{,}000 \times 5)}$$

Therefore;

$$DLT = 0.171$$

In this chapter discussion on radiolocation included the possibility of removing the 1.5 minute sleep time from the mobile sensor nodes in order to improve aspects of radiolocation. Figure 7.12 shows the results of potential data loss when the sleep time is removed from the sensor node transmission protocol. Potential data loss of any individual sensor node packet, below the data loss threshold, is unavoidable.

The cross over point between recoverable data and possible data loss in figure 7.12 is ~1,330, which is just above the benchmark of our typical housing estate deployment of 1,320 nodes.

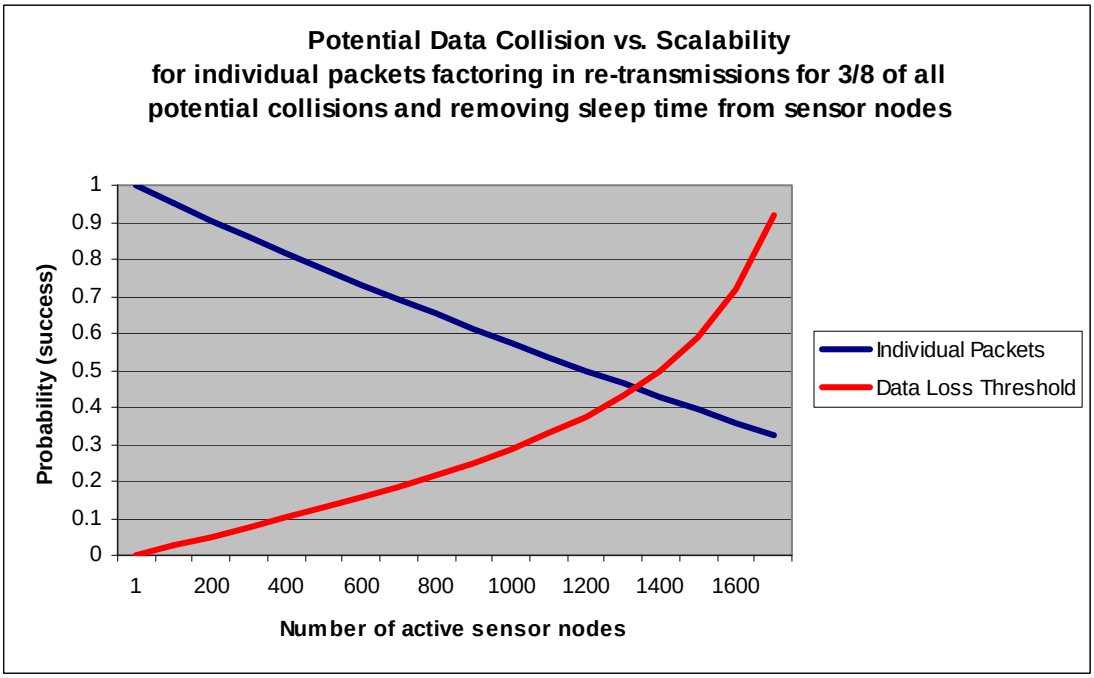


Figure 7.12: Potential data collision for each data packet when SN sleep time is removed

The results in figure 7.12 are for individual data packets. If the sensor node's triple data redundancy is factored in for these data packets, the results in figure 7.13 are obtained, supporting the possibility of removing the sleep time. Future work may look at reducing or removing this sleep time in more depth.

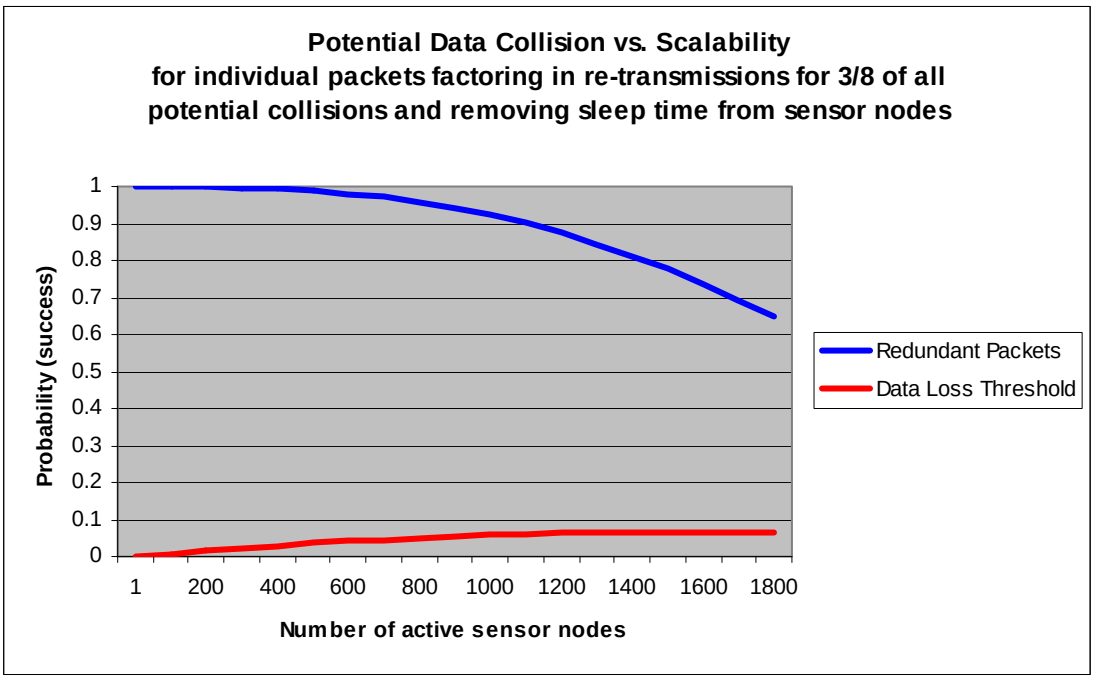


Figure 7.13: Potential data collision for redundant data packet when SN sleep time is removed

7.7 System Cost Analysis

The intention from the start of this research was to realise a low cost system. The cost break down for the sensor node was presented in chapter 5 and for the mesh node in chapter 6. The total cost of sensor nodes and mesh nodes in quantities of one thousand was shown to be €3.50 and €21.50 respectfully. In addition to the sensor and mesh nodes there is extra cost associated with the PC which acts as the base station and the USB modem. A low cost PC from Dell priced at €300 would satisfy the needs of the system. The USB modem is available from Vodafone for €20.

The cost of deploying the system in a typical housing estate, based on these prices is shown in table 7.1.

Description	Each €	Qty	Total €
Mesh Node	21.50	49	1,053.50
Sensor Node	3.50	1320	4,620.00
PC	300.00	1	300.00
USB Modem	20.00	1	20.00
TOTAL			**5,993.50**

Table 7.1 System cost for typical housing estate

Table 7.1 provides a total cost for the system of just under €6,000. The cost per household is for this system is less than €30 based on two hundred and twenty houses. This includes six sensor nodes per house.

8. CONCLUSIONS AND FUTURE WORK

8.1 Conclusions

The aim of this research was to design a wireless monitoring network for the benefit of a housing community or estate. This novel application is based on the technology of low power wireless mesh sensor networks. It was also the aim of this research to show how a simple and pragmatic approach would aid in the design and implementation of the system. In the authors view this has been achieved.

In chapter 2 an overview of existing related technology has been presented. It has focused on the key areas of wireless mesh networks and sensor networks. A number of benefits that such a network could provide a housing community have been discussed. One of the key aspects of the system is the ability to track individual sensor nodes. This provides the possibility of monitoring the location of children, pets or assets within the targeted area.

The network uses sensor nodes that are wirelessly connected to a fixed infrastructure of mesh nodes strategically place to cover the target area. This allows for greater flexibility in sensor deployment. It has been shown that the use of transmit-only sensor nodes can be beneficial in term of cost, power and complexity.

In order to ensure a successful transfer of data from these sensors nodes to the mesh nodes, two MAC protocols were proposed for this application. The first protocol is a novel technique based on TDMA. This collision avoidance protocol uses the MSF broadcast as a synchronisation signal for TDMA. Tests were carried out to ascertain the suitability of this method. It was illustrated that the MSF signal could be readily used for accurate synchronisations within a +/-3ms tolerance limit and could support up to 2000 nodes with acceptable data latency. The disadvantages of this protocol are scalability, and the requirement to incorporate a specialised receiver to receive the MSF signal.

The second protocol presented is a ‘transmit and hope’ scheme. In this protocol a number of techniques have been employed to reduce the possibility of data collision.

A scheme of three random transmissions in three consecutive ten second periods is proposed. An analysis on the probability of data collision in the system revealed that, for the application in question, the probability of data collision between sensor and mesh nodes is very low. In practical terms this figure is less than 0.1%. It is this MAC protocol which is adopted for the final design and implementation.

The sensor node hardware and software design have been presented. The sensor node has been prototyped to an advanced stage with tests and results presented. The battery powered mobile sensor nodes employs a mechanical motion sensor which powers the device when activated. The sensor node then powers off after transmitting data. This method extends the battery life of the sensor node far beyond its target life of 5 years.

The infrastructural mesh nodes collect data from sensor nodes and routes this data back to a base station. The static deployment of these nodes facilitates the implementation of a simple pro-active routing algorithm based on look-up tables.

The hardware and software design of the mesh node has been presented. Bench level testing has been performed on mesh and sensor nodes to verify their functionality. System testing has been carried out over a period of six months. This was facilitated by the deployment of a test network at NUI, Maynooth. Results of this testing have been presented.

It should be evident to the reader that this system design has adopted a simple application specific approach. The design of the system has avoided any major standards in terms of protocols or hardware implementation. This has been done to ensure the system design is void of any unnecessary or redundant features.

8.2 Future Work

Several ideas exist for extending the work in this thesis. These ideas are now outlined.

Currently, this proposed WMSN application is a monitor-only system. It would be worth investigating, as part of future work, the possibility of incorporating and

implementing control aspects. Possible applications include being able to remotely switch on/off lights, control temperature and even water garden plants. In part, this could be achieved without any hardware modifications and only minor software changes. The house node offers a solution, as it is equipped with a transceiver and is not part of the fixed infrastructure of mesh nodes. Therefore it can be deployed at any location in the system. To minimize the software changes required, control commands from the base station could be broadcast and relayed to all nodes. This would avoid the need to establish 'reverse' routes from the base node to a destination house node.

Another aspect of control is that pertaining to the sensor node. Being able to send data to the sensor node would allow for the possibility of "paging" children wearing these nodes. In the authors view, this would be of great benefit to a housing community. Currently the sensor nodes have transmit-only capabilities. In order to be able to control these nodes, they would require a radio receiver. A strong candidate for future work is the replacement of the transmit-only rfPIC in the sensor node with a transceiver, possibly the CC1101 as used in the mesh nodes. As mentioned in this thesis, this transceiver is low cost, low power and has a wake-on-radio feature which would help extend battery life. It is also possible to obtain this device with an integrated MCU (CC1110 Datasheet 2010).

One part of this WMSN application which could be investigated in future work, is to improve the ad-hoc deployment of mesh nodes. Currently the addition of ad-hoc mesh nodes requires that the deployment position is manually registered with the base station. An improvement to this would be the self registering of mesh nodes within the wireless mesh sensor network.

Many housing communities/estates are adjacent to each other. Currently this WMSN application is a standalone system targeting a single ROI. To extend the monitoring ability to adjacent housing estates, two key areas will need to be addressed, namely, preventing duplicity between systems and creating a central monitoring station for all housing WMSNs involved. A potential problem may occur when sensor nodes travel between networks as nodes with the same identification may exist in both networks. To avoid this duplicity, all sensor node identifications must be unique. The easiest way to achieve this is to extend the sensor node's identification by adding system identification data. This would associate sensor nodes to a particular housing WMSN

and provide unique identification for inter-estate mobility. In order to be able to monitor sensor nodes in other housing WMSNs, a central monitoring facility would have to be employed, which could be accessed by base stations from each network. This inter-estate mobility feature is worth investigating as part of future work.

This thesis has demonstrated the possibilities of implementing a simple networking concept which could provide substantial benefits to a housing community. It is hoped that the development of the work presented within this thesis will facilitate further development in the area of community based sensor networks which will be of primary benefit to the community, without being intrusive. The system design does not dictate what can or can not be monitored in this application. Some examples were presented but there are many opportunities to derive new sensing applications for a housing community. Hopefully future research will look to increase the number of sensing and monitoring applications and also to extend the capabilities of the system by addressing some/all of the future work possibilities outlined here.

9. REFERENCES

Adere, Ketema and Murthy, Garimella Rama (2010). "Solving the hidden and exposed terminal problems using directional-antenna based MAC protocol for wireless sensor networks," *Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On*, pp.1-5, 6-8 Sept. 2010.

Amber Alert (2010). *https://www.amberalertgps.com/,* 2010.

Assemtech (2010). Assemtech Europe Motion and Vibration Sensors, *website at, http://www.comus-intl.com/productpages/movement_vibration_switches_uk.asp* 2010.

Aziz, N.A.A., Aziz K.A. and Ismail, W.Z.W. (2009). "Coverage Strategies for Wireless Sensor Networks." *World Academy of Science, Engineering and Technology 50,* 2009.

Bai, X., Kumar, S., Xuan, D., Yun, Z. and Lai, T.H. (2006). "Deploying Wireless Sensors to Achieve Both Coverage and Connectivity," in *ACM MobiHoc*, 2006.

Balister, P. and Kumar, S. (2009). "Random vs. Deterministic Deployment of Sensors in the Presence of Failures and Placement Errors," *INFOCOM 2009, IEEE* , pp.2896-2900, 19-25 April 2009.

Bouhorma, M., Bentaouit, H. and Boudhir, A. (2009). "Performance comparison of ad-hoc routing protocols AODV and DSR," *Multimedia Computing and Systems, 2009. ICMCS '09. International Conference on*, pp.511-514, 2-4 April 2009

Broch, Josh, Maltz, David A., Johnson, David B., Hu, Yih-Chun and Jetcheva, Jorjeta (1998). "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols", *In Proceedings of the Fourth Annual International*

Conference on Mobile Computing and Networking (MobiCom'98), ACM, Dallas, TX, October 1998.

Business Week (1999). "21 ideas for the 21st century," *Business Week*, pp. 78–167, August 1999.

C. M. Roberts (2006). "Radio frequency identification (RFID)," *Computer Security*, vol. 25, pp. 18–26, 2006.

CC1101 Datasheet (2010). "Texas Instruments CC1101 radio transceiver datasheet" *http://focus.ti.com/lit/ds/swrs061f/swrs061f.pdf*, 2010.

CC1110 Datasheet (2010). "Texas Instruments CC1110fxx radio transceiver datasheet" *http://focus.ti.com/lit/ds/symlink/cc1110f16.pdf*, 2010.

Cerpa, A. and Estrin, D. (2002). "ASCENT: Adaptive Self-Configuring sEnsor Networks Topologies." *INFOCOM, IEEE,* Vol. 2. Issue 2002: 1278-1287.

Chen, J., S. Entong, S. and Youxian, S. (2009). "The deployment algorithms in wireless sensor net works: A survey." *Inform. Technol. J., 8: 293-301*, 2009.

Chenna Reddy, P. and ChandraSekhar Reddy, P. (2006), "Performance Analysis of Adhoc Network Routing Protocols," *Ad Hoc and Ubiquitous Computing, 2006. ISAUHC '06. International Symposium on*, pp.186-187, 20-23 Dec. 2006.

Chong, Chee-Yee and Kumar, Srikanta P. (2003). "Sensor networks: evolution, opportunities, and challenges", *Proceedings of the IEEE,* Vol. 91, No. 8, August 2003.

Contiki (2010). Official Website at *http://www.sics.se/contiki/* 2010.

C-Max (2010). C-Max Time Solutions Website, *http://www.c-max-time.com,* 2010.

Daintree Networks (2010). “Getting Started with ZigBee and IEEE 802.15.4” *ZigBee Primer at www.daintree.net/downloads/whitepapers/zigbee_primer.pdf*, Daintree Networks, 2010.

Davies, A.C. (2002). "An overview of Bluetooth Wireless Technology™ and some competing LAN standards," *Circuits and Systems for Communications, 2002. Proceedings. ICCSC '02. 1st IEEE International Conference on*, pp. 206- 211, 2002.

Esmaeili, M., Abbaspour, M., Alipour, H. and Mousavi, H. (2007). "Challenge in QoS Supporting via Integrating Differentiated Service and Multipath Routing on Mobile Ad Hoc Network," *Computer and Information Technology, 2007. CIT 2007. 7th IEEE International Conference on*, pp.359-368, 16-19 Oct. 2007.

Galleon (2010). Galleon Systems Website, *http://www.galleon.eu.com/contact.htm*, 2010.

Geetha, V., Aithal, S. and ChandraSekaran, K. (2006). "Effect of Mobility over Performance of the Ad hoc Networks," *Ad Hoc and Ubiquitous Computing, 2006. ISAUHC '06. International Symposium on*, pp.138-141, 20-23 Dec. 2006.

Gomez, C. and Paradells, J. (2010). "Wireless home automation networks: A survey of architectures and technologies," *Communications Magazine, IEEE* , vol.48, no.6, pp.92-101, June 2010.

HART (2007). “Why WirelessHART? The Right Standard at the Right Time”, *HART Communication Foundation White Paper*, October 2007.

Hiertz, G., Denteneer, D., Stibor, L., Zang, Y., Costa, X.P. and Walke, B. (2010). "The IEEE 802.11 universe," *Communications Magazine, IEEE* , vol.48, no.1, pp.62-70, January 2010.

Jianpo Li, Xuning Zhu, Ning Tang and Jisheng Sui (2010). "Study on ZigBee network architecture and routing algorithm," *Signal Processing Systems*

(ICSPS), 2010 2nd International Conference on , vol.2, pp.V2-389-V2-393, 5-7 July 2010

Koon, Hoo Teo, Zhifeng, Tao and Jinyun, Zhang (2007). "The Mobile Broadband WiMAX Standard (Standards in a Nutshell)," *Signal Processing Magazine, IEEE* , vol.24, no.5, pp.144-148, Sept. 2007.

Kumar, S., Lai, T.H. and Balogh, J. (2004). "On *k*-Coverage in a Mostly Sleeping Sensor Network," in *ACM MobiCom*, 2004.

Lang, Daniel (2003). "A comprehensive overview about selected Ad Hoc Networking Routing Protocols", *Master's thesis, Technische Universit at Munchen,* 2003.

Lombardi, Michael A. (2003). "Radio Controlled Clocks", *NCSL International Workshop and Symposium*, 2003.

Loy, Matthew, Karingattil, Raju and Williams, Louis (2005). "ISM-Band and Short Range Device Regulatory Compliance Overview," *Texas Instruments Application Report*, no. SWRA048, May 2005

Maloco, John and McLoone, Seamus (2007). "A Suitable MAC Protocol for Transmit-Only Sensor Nodes in a Housing Community Wireless Network," *The IET China-Ireland International Conference on Information and Communications Technologies (CIICT 2007),* August 28-29, 2007.

Maloco, John, McLoone, Seamus and Delaney, Declan T. (2006). "Using Rugby MSF Broadcast for Time Division Multiplexing Synchronisation in a Housing Community Sensor Network," *Irish Signals and Systems Conference, 2006. IET*, pp.289-294, 28-30 June 2006.

Mauve, M., Widmer, A. and Hartenstein, H. (2001). "A survey on position-based routing in mobile ad hoc networks," *Network, IEEE* , vol.15, no.6, pp.30-39, Nov/Dec 2001.

Microchip (2010). MiWi Wireless Network Protocol; *Microchip Application notes AN1024, AN1066 at http://www.microchip.com/* 2010.

Mittal, S. and Kaur, P. (2009) "Performance Comparison of AODV, DSR and ZRP Routing Protocols in MANET'S," *Advances in Computing, Control, & Telecommunication Technologies, 2009. ACT '09. International Conference on*, pp.165-168, 28-29 Dec. 2009.

NIST (2010). WWVB North American Atomic Time Signal, *The National Institute of Standards and Technology at www.nist.gov/pml/div688/grp40/wwvb.cfm*, 2010.

NPL (2005). "NPL Time and Frequency Services", *The National Physics Laboratory at http://www.npl.co.uk*, June 2005.

Nu.M8 (2010). *http://www.lok8u.com/us/*

Pirzada, A.A., McDonald, C. and Datta, A. (2005). "Reliable link reversal routing for mobile ad-hoc wireless networks," *Networks, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication., 2005 13th IEEE International Conference on* , vol.1, pp. 6 pp., 16-18 Nov. 2005.

Poor Robert and Hodges Brent (2002). "Reliable Wireless Networks for Industrial Systems" *Technical White Paper from Ember Corporation*, October 2002.

PTB (2007). DCF77 German Atomic Time Signal, *Physikalisch-Technische Bundesanstalt at http://www.ptb.de/en/org/4/44/442/dcf77_1_e.htm,* 2007.

Razavi, Roozbeh (2002). "How Routing Algorithms Work." *HowStuffWorks.com. http://computer.howstuffworks.com/routing-algorithm.htm*, 19 November 2002.

rfPIC Datasheet (2010). "Microchip Corporation, rfPIC12Fxx microcontroller datasheet" *http://ww1.microchip.com/downloads/en/DeviceDoc/70091a.pdf*, 2010.

Roberts, C.M., (2006). "Radio frequency identification (RFID)." In *Computers & Security*, 25(1), 18-26, 2006.

Stathopoulos, T., Kapur, R., Estrin, D., Heidemann, J. and Zhang, L. (2004). "Application-Based Collision Avoidance in Wireless Sensor Networks," *Proceedings of the 29th IEEE International Conference on Local Computer Networks (LCN'04)* 2004.

TI (2010). SimpliciTI OS by Texas Instruments, *http://www.ti.com/*, 2010.

TinyOS (2010). TinyOS Alliance official website at *http://www.tinyos.net/*, (2010).

Tiwari, Ankit, Balla, Prasanna and Lewis, Frank L. (2007). "Energy-efficient wireless sensor network design and implementation for condition-based maintenance", *ACM Transactions on Sensor Networks (TOSN),* Volume 3, Issue 1, 2007.

Wan, P. and Yi, C. (2006). "Coverage by Randomly Deployed Wireless Sensor Networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 14, pp. 2658–2669, 2006.

Want, R. (2006). "An introduction to RFID technology," *Pervasive Computing, IEEE* , vol.5, no.1, pp. 25- 33, Jan.-March 2006.

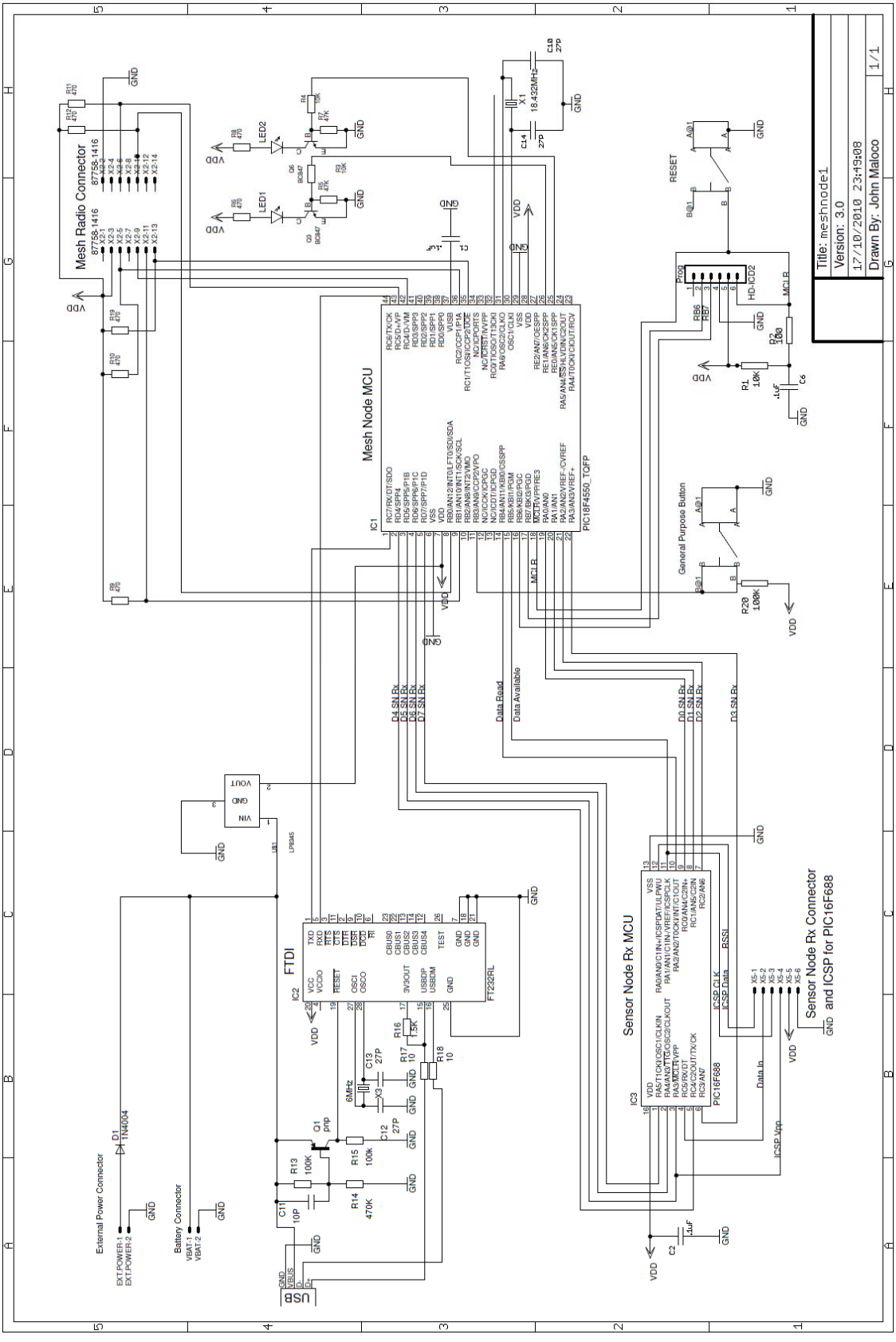
Ye W. and Heidemann J. (2003). "Medium Access Control in Wireless Sensor Networks," *USC/ISI Technical Report ISI-TR-580*, October 2003.

Zaidi, S. Ali Raza, Hafeez, Maryam, McLernon, D.C. and Ghogho, M. (2008). "A Probabilistic model of *k*-coverage in Minimum Cost Wireless Sensor Networks" *CoNEXT'08, Madrid, Spain,* December 9-12, 2008.

ZigBee (2010). ZigBee Alliance official website at *http://www.zigbee.org* 2010.

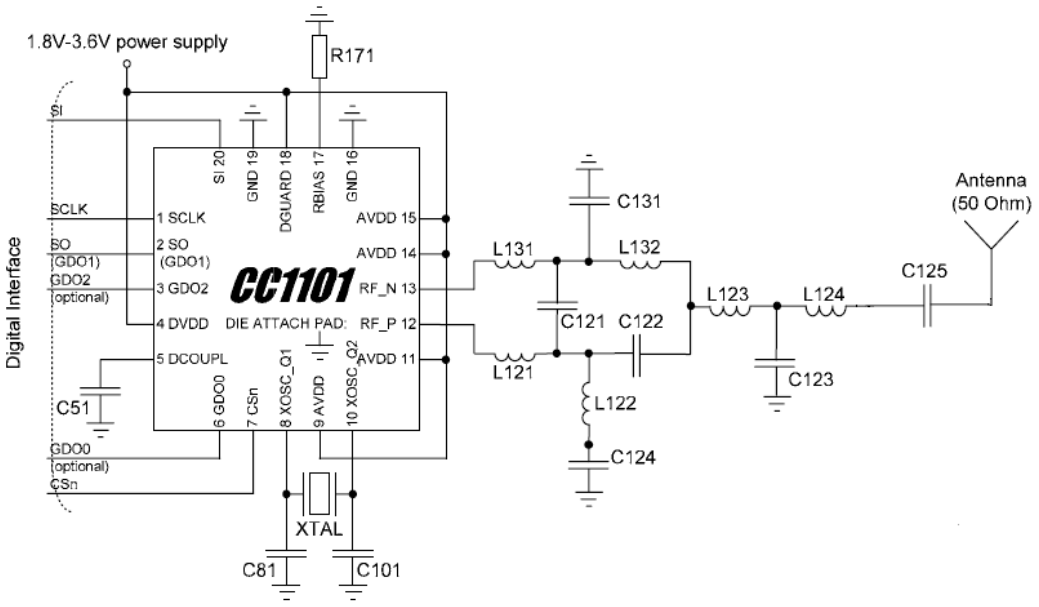
Zou, Y and Krishnendu, C. (2003). "Sensor deployment and target localization based on virtual forces", *Proceedings of Twenty-Second Annual Joint Conference of the IEEE Computer and Communications (INFOCOM 2003)*, March 2003.

APPENDIX I Mesh Node Circuit Design



APPENDIX II Mesh Radio Module Design

Texas Instruments CC1101 Reference Circuit Design



Reference circuit design for Texas Instruments CC1101 radio transceiver chip operating at 868 MHz taken from the CC1101 datasheet

Component	Value at 868 MHz		Component	Value at 868 MHz
C51	100 nF ± 10%, 0402 5R		R171	56 kΩ ± 1%, 0402
C81	27 pF ± 5%, 0402 NP0		L121	12 nH ± 5%, 0402
C101	27 pF ± 5%, 0402 NP0		L122	18 nH ± 5%, 0402
C121	1.0 pF ± 0.25 pF, 0402 NP0		L123	12 nH ± 5%, 0402
C122	1.5 pF ± 0.25 pF, 0402 NP0		L124	12 nH ± 5%, 0402
C123	3.3 pF ± 0.25 pF, 0402 NP0		L131	12 nH ± 5%, 0402
C124	100 pF ± 5%, 0402 NP0		L132	18 nH ± 5%, 0402
C125	12 pF ± 5%, 0402 NP0		XTAL	26.0 MHz
C131	1.5 pF ± 0.25 pF, 0402 NP0			

Bill of materials for reference design

APPENDIX III Matlab Simulation Code

Matlab Simulation 1
Probability of data collision for a single transmission window

```
%Name: Matlab Simulation 1

%By: John Maloco
%Date: September 2010

%Description

%This model is used to test the probability of a transmit-only Sensor
%Node successfully transferring its data to a Mesh Node

%Model Parameters

%This model simulates 200 sensor nodes transmitting in one 10s period
%to a single mesh node. The model takes a single transmission and
%tests the probability of this transmission colliding with another.

%The transmission time for one data packet is 2050 us
%Any transmission starting 2050us before this will collide. Likewise
%any transmission starting within 2050us after the packet will also
%collide. This effectively means that there is a transmission window
%of +/-2050us.

%A data transmission occurs randomly is a 10s (or 10,000,000us)
%period.

%Method

%This test generates 200 random starting points in the 10s period
%with a resolution of 1us.
%One transmission start time is then compared to the other 199 with a
%tolerance of +/-2050us. If the chosen start time is within this
%period a collision is said to have occurred.

%This is repeated 1000 times to establish an average and this data is
%logged. This simulation is then repeated a further 100 times and an
%overall average is established.

Nt = 0;

for loop = 1:100        %Overall 100 time loop

nodes = 200;            %Number of node to simulate
out = [nodes,1];        %Create an array of 200

z = 0;

for t = 1:1000          % number of transmissions
```

```
    for y=1:nodes
    out(y,1) = randint(1,1,[1,10000000]);   %Generate 200 random
start
    end                                     %times with in the 10s
period

a=1;
b=2;

%Here the first value in the array is compared to the other 199
values +/-2050

for x = 1:nodes-1
    if ((out(a,1) > out(b,1)-2050)) && ((out(a,1) < out(b,1)+2050));
        beep;
        z = z+1;
    end
    b=b+1;
end
%
end

z = z/10;   %z is the % likelihood of collision.
%
% %beep
z
Nt = Nt + z;        %this is done 100 times so as to be able to look
at the
                    %deviation in individual simulations
end

Nt = Nt/100
```

Matlab Simulation 2
Probability of data collision for multiple transmission windows

```
%Name: Matlab Simulation 2

%By: John Maloco
%Date: September 2010

%Description

%Plot the number of nodes (X) against the
%percentage probability of no collision.

%Array Y is the %percentage probability of collision produced by
%using Matlab simulation 1 using the corresponding values in Array X
%as the number of nodes for the simulation.

%Array X is the number of nodes used in the simulation for the
%corresponding probability of collision in array Y.
```

```
%The graphs produced are plots of Number of Node (X) against the
%percentage probability of no collision (100-Y)%


% For 1000 Nodes%
%Probability of successful transmission to a single Mesh Node in one
%10s period
y = [0 2.5000 2.7000 6.4000 7.6000 8.9000 11.8000 13.5000 16.7000
19.2000 21.1000 24.6000 25.2000 25.3000 30.3000 32 30.9000 36 37.6000
41.7000 44.4000]
x = [0 50 100 150 200 250 300 350 400 450 500 550 600 650 700 750 800
850 900 950 1000]

%Plot the result as a percentage
plot(x,100-y)

%Probability of successful transmission to a single Mesh Node in two
%10s period.
%This is given by (Probability of Collision)^2

y = [0 (2.5000/100)^2 (2.7000/100)^2 (6.4000/100)^2 (7.6000/100)^2
(8.9000/100)^2 (11.8000/100)^2 (13.5000/100)^2 (16.7000/100)^2
(19.2000/100)^2 (21.1000/100)^2 (24.6000/100)^2 (25.2000/100)^2
(25.3000/100)^2 (30.3000/100)^2 (32/100)^2 (30.9000/100)^2 (36/100)^2
(37.6000/100)^2 (41.7000/100)^2 (44.4000/100)^2]
x = [0 50 100 150 200 250 300 350 400 450 500 550 600 650 700 750 800
850 900 950 1000]

figure(2);

%Plot the result as a percentage
plot(x,(1-y)*100)

%Probability of successful transmission to a single Mesh Node in
three %10s period
%%This is given by (Probability of Collision)^3

y = [0 (2.5000/100)^3 (2.7000/100)^3 (6.4000/100)^3 (7.6000/100)^3
(8.9000/100)^3 (11.8000/100)^3 (13.5000/100)^3 (16.7000/100)^3
(19.2000/100)^3 (21.1000/100)^3 (24.6000/100)^3 (25.2000/100)^3
(25.3000/100)^3 (30.3000/100)^3 (32/100)^3 (30.9000/100)^3 (36/100)^3
(37.6000/100)^3 (41.7000/100)^3 (44.4000/100)^3]
x = [0 50 100 150 200 250 300 350 400 450 500 550 600 650 700 750 800
850 900 950 1000]

figure(3);

%Plot the result as a percentage
plot(x,(1-y)*100)
```