Design of an ad hoc wireless network for wildlife telemetry tracking in the Cederberg

by

Johan George Brits

Thesis presented in partial fulfilment of the requirements for the degree of Master of Science in Electronic Engineering at Stellenbosch University

Department of Electrical and Electronic Engineering,
University of Stellenbosch,
Matieland, 7601, South Africa.

Supervisor: Dr. H.A. Engelbrecht

March 2011

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the owner of the copyright thereof (unless to the extent explicitly otherwise stated) and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Signature: ....
J.G Brits

Date: 2011/03

Abstract

Design of an ad hoc wireless network for wildlife telemetry tracking in the Cederberg

J.G Brits

Department of Electrical and Electronic Engineering,
University of Stellenbosch,
Matieland, 7601, South Africa.

Thesis: MScEng (Electronic)

March 2011

This thesis involves research on wildlife telemetry tracking for the Cape Leopard Trust (CLT). The CLT needed a network to transfer GPS data and single frame photos from remote locations in the Cederberg to a researcher's base station. The proposed solution is an ad hoc wireless network, where nodes perform polling of leopard collars and send information via the multi-hop network to the researcher's base once it is downloaded from a collar. The literature study involved medium access control - and routing protocols for effectively transferring information. The solution was implemented in hardware and range tests were done in the Cederberg to determine feasible locations for nodes in this network for covering most of the CLT study area. Link budgets for this area was determined with Radio Mobile to compare with actual ranges as measured. The simulation of protocols was done in OMNET++ which could be compared with actual results from the physical network.

Uittreksel

Ontwerp van 'n ad hoc draadlose netwerk vir opsporing van luipaarde in die Cederberge

("Design of an ad hoc wireless network for wildlife telemetry tracking in the Cederberg")

J.G Brits

Departement Elektriese en Elektoniese Ingenieurswese,
Universiteit van Stellenbosch,
Matieland 7601, Suid Afrika.

Tesis: MScIng (Elektronies)

Maart 2011

Hierdie tesis handel oor navorsing wat gedoen is vir die Kaapse Luipaard Trust (CLT) vir die opsporing van luipaarde. Die CLT het 'n netwerk nodig gehad wat GPS data en enkel raam fotos van afgeleë gebiede in die Cederberge na 'n navorser se basis stuur. Die voorgestelde oplossing is 'n ad hoc draadlose netwerk, waar nodisse luipaard nekbande oproep om data af te laai en dan te stuur deur die multi-hop netwerk na die navorser se basis. Die literatuurstudie handel oor medium toegangs beheer - en roete verkryging protokolle vir die effektiewe oordrag van informasie. Die oplossing is in hardeware geïmplimenteer en radio-afstand-toetse is gedoen in die Cederberge om goedgeleë posisies vir nodisse te bepaal om die grootste gedeelte van die CLT studie area te dek. Radio Mobile is gebruik om voorspellings te maak rakende die afstande verkrygbaar tussen radios om te vergelyk met die fisiese metings in die veld. Die simulasie van protokolle is gedoen in OMNET++ en vergelyk met prestasie metings op die fisiese netwerk.

Acknowledgements

I would like to express my sincere gratitude to the following people and organizations:

- My supervisor Dr. H.A. Engelbrecht for his guidance
- Mr. Quinton Martins of the Cape Leopard Trust for answering project related questions
- Mr. J. Arendse for soldering the five test units
- Mr. W. Croucamp for hardware related services
- Mr. A. Barnard for radio frequency related knowledge
- Mr. D. Kotze for help with Omnet++
- Mr. R. Wiid for his help with the range tests in the Cederberg
- Mr. D. Warnich for various project related insights
- Jean Mearns, Managing Director of W.H. Circuits for sponsoring the printed circuit boards of the tests units
- My family for their support
- My Saviour Jesus

Dedications

Hierdie tesis word opgedra aan my ouers wat my elke oomblik ondersteun het deur my ingenieurswese studies

Contents

List of Figures

List of Tables

Nomenclature

Acronyms

AC Alternating Current
ACK Acknowledge message
ASK Amplitude Shift Keying modulation
CSMA Carrier Sense Multiple Access
CTS Clear To Send message
DATA Data message
DC Direct Current
DS Data Sending message
FAMA Floor Acquisition Multiple Access protocol
FIFO First In First Out queue
FSK Frequency Shift Keying modulation
FU Functional Unit
GPS Global Positioning System
GSM Global System for Mobile Communications
IC Integrated Circuit
ICASA Independent Communications Authority of South Africa
LED Light Emitting Diode
MAC Medium Access Control
MACA Media Access Collision Avoidance protocol
MACAW Media Access Collision Avoidance for Wireless protocol
OSI Open Systems Interconnection model
PCB Printed Circuit Board
PER Packet Error Rate
POLL Poll message
PSK Phase Shift Keying modulation
RF Radio Frequency
RREP Route Reply message
RREQ Route Request message
RRP Round Robin Polling
RTS Request To Send message
SIM Subscriber Identity Module card
SLA Sealed Lead Acid battery

TCP/IP Transmission Control Protocol/Internet Protocol

TTL Transistor Transistor Logic

USART Universal Serial Asynchronous Receiver Transmitter serial bus

USB Universal Serial Bus

VHF Very High Frequency

Definitions

Broadcast Sending a message to more than one recipient

Unicast Sending a message to only one recipient

Milking station Synonymous with Relay station, this is the station that polls leopard collars and leopard trap cages for data, thus milking them

Base station The station residing at the researcher's house where all data will be forwarded to

Leopard collar A collar fitted with a GPS and radio for sending location information of the leopard to a milking station while passing by

Leopard trap cage A cage fitted with a camera and radio to take an image of a captured animal to send it to a milking station

Nomadic A node that moves infrequently

Node A wireless station, could be a base station, leopard collar or milking station

List of symbols

ΔI_{ripple} Ripple current [A]

ΔV Ripple voltage [V]

C_{in} Input capacitor value [uF]

h_r Height of receiving antenna [m]

h_t Height of transmitting antenna [m]

$I_{chg(max)}$ Maximum charging current [A]

$I_{diode(max)}$ Maximum current through diode [A]

$I_{saturation}$ Inductor saturation current [A]

$E_{3.3V}$ 3.3V regulator's energy consumption per day [Wh]

$P_{3.3V-regulator}$ 3.3V regulator's power consumption [W]

E_{5V} 5V regulator's energy consumption per day [Wh]

$P_{5V-regulator}$ 5V regulator's power consumption [W]

E_{gps} GPS's energy consumption per day [Wh]

P_{GPS} GPS's power consumption [W]

P_{max} Total power consumption of all on-board components [W]

E_{radio} Radio's total energy consumption per day [Wh]

$P_{radio-t}$ Radio transmitter's power consumption [W]

$E_{receiver}$ Radio receiver's energy consumption per day [Wh]

E_{sd} SD-card's energy consumption per day [Wh]

$E_{subtotal}$ Total energy consumption of all on-board components per day [Wh]

E_{total} $P_{subtotal}$ including the solar charger IC's energy dissipation per day [Wh]

$E_{transmitter}$ Radio transmitter's energy consumption per day [Wh]

E_{uC} Microcontroller's energy consumption per day [Wh]

$P_{uController}$ Microcontroller's power consumption [W]

R_1 Float voltage programming resistor 1 value [Ω]

R_2 Float voltage programming resistor 2 value [Ω]

R_{in1} Input supply voltage programming resistor 1 value [Ω]

R_{in2} Input supply voltage programming resistor 2 value [Ω]

R_{sense} Current sense resistor value [Ω]

V_{bat} Battery charging voltage [V]

$V_{forward}$ Diode forward voltage drop [V]

$V_{in(max)}$ Solar input voltage maximum [V]

V_{in} Solar input voltage [V]

B Bandwidth [Hz]

d Distance [km]

L Inductor value

N Noise power [W]

S/N Signal to Noise ratio

S Signal power [W]

V Number of discrete levels

Chapter 1

Introduction

1.1 Motivation for this study

The need exists with the Cape Leopard Trust to more effectively determine the home range and behavior of the Cape leopard. This will help with leopard ecology in this area by monitoring their activity and movements to better manage predator-land owner conflicts.

1.2 Background

Key aims of the Cape Leopard Trust is to estimate gene flow, genetic variability and genetic relatedness among South African leopard populations by capturing the leopards and taking samples [20]. The leopards' home ranges are determined by equipping them with GPS (Global Positioning System) fitted collars. The Global Positioning System provides location information to earth-bound receivers by determining latitude and longitude from satellite signals.

Previous solutions for the Cederberg area included handheld radio tracking devices to collect GPS data and manually operated trap cages to catch leopards. An automatic system is required that delivers the GPS coordinates and photos from trap cages directly to the researchers base. This will help to reduce man-hours considerably by eliminating the need to monitor trap cages twice a day and following leopards in the field to download GPS data with handheld devices. The aim of designing this network is thus to create a limited coverage area, so that GPS collars and camera trap cages can send data over a shared network to a base station and thereby automating the data retrieval process.

1.3 Existing solutions to obtaining wildlife tracking data

1.3.1 Aerial telemetry

Wildlife Air Aerial telemetry is a means of obtaining GPS-data via an aircraft with an on-board receiver and antenna. This is an effective tool if the type of animal tracked has a very large home range, or the terrain cannot be accessed by motor-vehicle. The transmitters on the animals use UHF or VHF frequencies which means that line-of-sight is crucial. Using an aircraft will increase the line-of-sight range over which radio signals can be acquired as opposed to the receiver being on the ground. Safety is a concern, as there have been accidents in the past few years in which aircraft has been operated in environments for which the pilot or aircraft type was not suited for. [9]

1.3.2 Satellite telemetry

Argos Argos is a satellite tracking solution covering the globe. Argos has existed for the past 32 years. It uses six satellites at 850km above the earth's surface. It makes use of the doppler effect, needing only one satellite to be in range at any given time. As the satellite passes a transmitter, the frequency of the continuous signal drifts, allowing it in combination with the satellite's speed, position and the original frequency to calculate the transmitter's position. Argos satellites receives the data from transmitters on animals, sends it to a station on land to process and makes it available to the researcher via the Internet. One organization using Argos is Seaturtle.org and claims that a transmitter including communication time, costs between 3000 and 5000 USD. [8]

1.3.3 Terrestrial telemetry

Homing Homing involves a researcher following an animal transmitter by walking in the direction of the greatest signal strength detected by the hand-held receiver. When the animal is viewed, the location is determined by a GPS unit or visually estimated.

Triangulation This involves the simultaneous recording of two signal bearings by two researchers from different locations. The bearings is plotted onto a map to give the animal's location where they cross.

1.3.3.1 Automatic systems

Zebranet Zebranet is a wireless sensor network which takes advantage of Zebras coming into contact with each other to share data. In order for the researcher to gain information about the whole herd (or part thereof) by a single download, each collar coming into contact with others store the data about all the others, thus creating a redundant system. Researchers have to find Zebras on a weekly basis to download data. The motivation for using a sensor network is to save on energy, because collars will only transmit when they are close to each other, thus reducing the energy need for transmitting to a far-off base station or satellite. [1]

EcoLocate Ecolocate is a wireless ad-hoc network which uses the diversity of the animal kingdom to create a network through animal contact with each other and with a base station [19]. This architecture allows for data about all animals to be automatically gathered at the researcher's base, rather than going into the field and finding animals as with Zebranet.

GSM (Global System for Mobile Communications) Many pet tracking solutions like "The Pet Detective" from Telepet, "GPS Pet Tracker" from Micro Tech etc. takes advantage of mobile phone infrastructure and GSM transceivers to send location information to the pet owner [6]. The project "Push to Talk on Cellular" uses the same technology to protect wildlife in Kenya from poachers [25]. When location information on an animal is required, an sms (short message service) is send to the collars' SIM (Subscriber Identity

Module) card, which then responds by determining its location and sending it back to the owner via the local GSM network.

1.4 Advantages and disadvantages of wildlife telemetry tracking arising from literature

From the existing solutions mentioned, it is clear that aerial telemetry and satellite telemetry are expensive. With aerial telemetry the researcher has to carry the cost of hiring a pilot and airplane every time data is downloaded from animals. This will be a recurring cost as there will always be new data and one runs the risk of not finding the animal. With Argos there is also the airtime cost for data transmitted via the satellite and the equipment is expensive. The advantage of aerial telemetry is the large area that can be covered by an airplane, if the animal being studied has a large home range. This is even more true of satellite telemetry, as it covers the globe, which means migratory animals can be studied as well. These two will be feasible solutions if no other system can download the tracking data due to the home range of the animals being too large or animals visiting a fixed location too irregularly. Homing and triangulation involves a lot of man-hours as one has to physically find the animals using hand held devices. These will be feasible solutions if cost is of great concern and if many researchers can partake in the tracking. Zebranet has the advantage that only one animal has to be found to gain information about the whole herd, but again this could be time consuming as newer data will always be available to download and one animal might not have come into contact with all the others, so that more animals will have to be found. Ecolocate is fully automated which means no extra time will be spent on finding animals. All data is delivered to a base station. It does however also depend upon animals coming into contact with others to form a network through which data can be sent. Larger animals like elephants also has to form part of the system as they are the moving relay stations due to their large batteries. GSM tracking could be a great solution if the animals dwelt under cell phone coverage. The cost of using the network must still be considered.

It is thus desirable to create one's own data retrieval system so that recurring costs do not apply and the cost of setting up the system still justifies not using an existing network. An automatic system is also desirable.

1.5 Objectives of this study

The scope of this project entails the system level design and implementation of a wireless ad-hoc network which could be used in practice for animal tracking and general environmental data acquisition, in the Cederberg area. The aim of the project is to design the network of the system so that it is economical and more efficient than the current system employed by researchers in this area. The main areas of focus will be:

1. Determining the design specifications of the wireless ad-hoc network. This includes the following aspects:
   a) Selection of an ICASA approved frequency of operation.
   b) The necessary radio coverage required in the Cederberg.
   c) Suitable locations for the nodes in the ad-hoc network.

   d) The type of data to be transferred between nodes.
   e) The necessary bandwidth requirements and associated data rate.
   f) Selecting and developing appropriate communication protocols.

2. Simulation of the particular communication protocols

3. Selection of suitable hardware components (including radios, weatherproof casing, efficient power source, etc) to meet the design specifications.

4. Software and hardware development including assembly of a number of test units.

5. Field testing and verifying that the deployed ad hoc network meets the design specifications by measuring parameters such as the power consumption, data throughput and route acquisition delay.

The goal is to demonstrate a fully functional ad-hoc network , created by deploying a number of the nodes designed as part of this project.

1.6 Contributions

- Five test units were designed and built that will form part of the eventual network employed in the Cederberg
- A link budget was calculated specifically for the study area in the Cederberg and range tests were done as verification which yielded a maximum line-of-sight link of 10.43km
- Range tests confirmed that no non-line-of-sight links are possible at 151.3 MHz
- The MAC and network protocols MACAW and AODVjr were simulated and implemented in firmware to characterize their performance in this application where both the simulation and measured results showed that a network with 3 hops has a maximum sustainable throughput at 0.1 packet per second message arrival rate.

1.7 Overview

The multi-hop characteristic of ad hoc networks makes it a viable solution to wildlife telemetry tracking for extending the area of coverage in a wireless network. It also provides the ability for nodes to be nomadic and thus accommodates wildlife researchers in being able to move network nodes, as wildlife walking patterns or research objectives change. Wireless networks however have several design constraints resulting from the nature of a wireless channel that should be considered. One of these constraints is interference in the wireless transmission channel such as topography and vegetation of the specific area that should be covered by the network. Another consideration is in the limited range of a wireless link. In this thesis the considerations are taken into account when deciding on hardware, algorithms and protocols that govern the flow of information. This work is done for the application of leopard tracking in the Cederberg mountain area.

In chapter 2 we discuss existing ad hoc protocols that govern the information flow in ad hoc networks and decide on suitable protocols for this application. In chapter

3 we consider the physical constraints pertaining to the wireless medium in use and calculate link budgets for the study area in the Cederberg. Chapter 4 describes the detail implementation of the protocols as chosen in chapter 2. Chapter 5 discusses the hardware design of a wireless node together with a system verification. In chapter 6 all measurements related to the network and hardware are discussed. This chapter also compares the predicted link budget with actual measurements in the field and protocol simulation results with those measured on the real network. Chapter 7 concludes the thesis and gives recommendations for future work on the project.

Chapter 2

Literature study

2.1 Introduction

Data communication is defined as the means of getting information from one point to another reliably. To implement a communications system, two popular models is widely used: the Internet Reference Model and the OSI (Open systems interconnection) model. Both models use a layered approach to divide communication tasks into logically defined subsystems. Each layer provides a known interface and a set of services to the above layer. A layer is concerned with its own tasks and uses the advertised services of a lower layer for completing its tasks. Each layer incorporates a subset of the functions needed for communication between nodes. The entities performing the tasks on each layer are called protocols, which are defined rules for transferring information between communicating parties[17]. The advantage of this approach is that it simplifies the programming of a communications system, as the tasks of each layer and the interfaces between layers are well defined. It is also advantageous when different protocols need to be tested, since a layer can be exchanged for one implementing a different protocol by just adhering to the specified interface. In this way different applications will also be able to communicate by only using the network services in the same way. The Internet Reference Model is a model used for internet communication and not appropriate for applications other than the TCP/IP protocols developed for computer applications. The OSI model was developed from a telecommunications perspective and more suited to the ad hoc network developed as part of this thesis.

Figure 2.1 shows the seven layers of the OSI model grouped into media layers and host layers. The two bottom layers has the task of physical communication of messages between two adjacent nodes. The network layer has the task of routing messages if intermediate nodes exist between two communicating nodes. The top four layers has to format the data such that it will make sense to the user [17]. This communication system will concern itself with the media layers.

1. **Physical:** This layer deals with the mechanical and electrical aspects of the communication link such as connector type, wire or wireless, voltage levels, frequency, modulation scheme etc. Data is transferred in the form of bits.

2. **Data link:** The bits from the physical layer is formatted into frames on this layer. It deals with the reliable communication over the physical layer by means of error detection and correction and flow control. Data is transferred in the form of packets.

3. **Network:** The network layer interconnects adjacent nodes to form a network. It provides a path for communication from a source node to a destination node via intermediate nodes. The user messages are formatted into addressable packets.

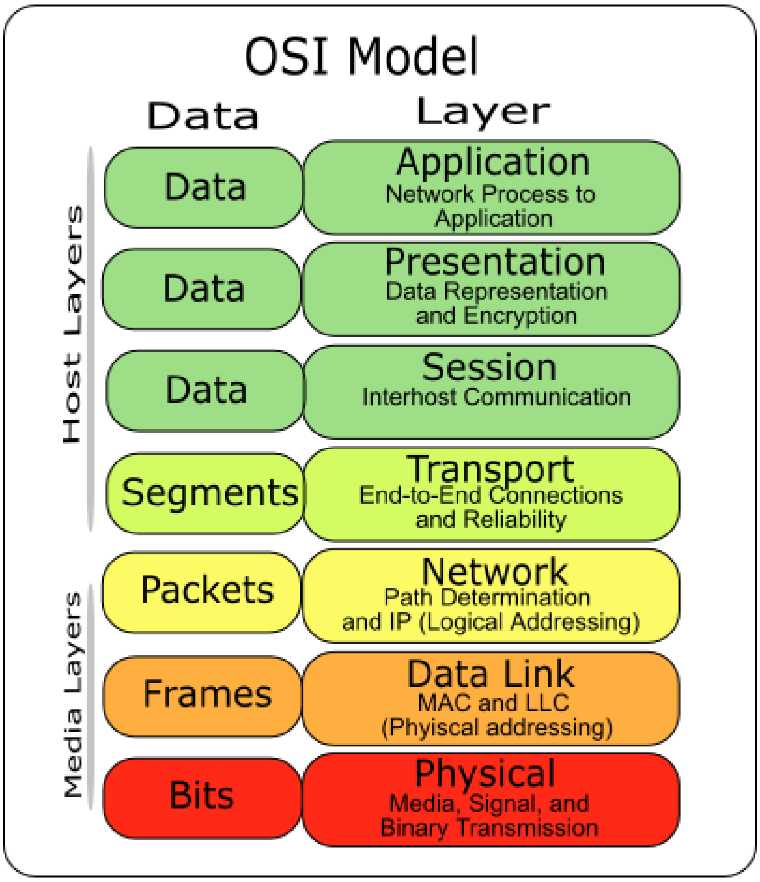

Figure 2.1: OSI model

Figure 2.1 is taken from [14].

2.2 Physical layer

The physical layer uses the Bim1H-151.3-10 narrow band transceiver as chosen in chapter 5 in half-duplex mode. This means that communication is possible in both directions, but it can only happen in one direction at a time, because the transmit and receive circuitry shares the same frequency and antenna. In this way if one radio is in transmit mode, the other has to be in receive mode and vice versa. This module uses FSK (frequency shift keying) modulation with a carrier frequency of 151.3MHz. FSK modulation is one of the basic digital modulation techniques. The other two are ASK(amplitude shift keying) and PSK(phase shift keying). Figure 2.2 from [18] shows the carrier frequency being modulated according to the digital input signal with respect to the three parameters: amplitude, phase and frequency. With ASK the carrier signal is present or not present according to a 0 or a 1 (amplitude maximum or minimum). With Phase shift keying the signal shifts its phase 180^o apart resulting in two different phased signals representing the 1 or 0. In frequency shift keying the signal is alternated between two different frequencies around the carrier frequency to represent the 1 or 0. Many other variations and combinations on this techniques exist.

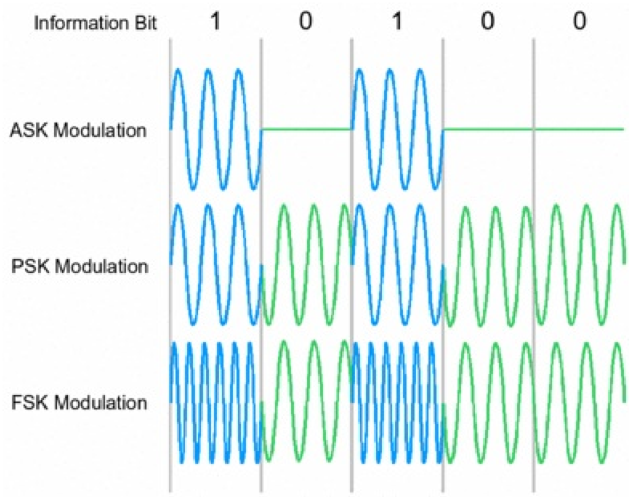

Figure 2.2: Digital modulation techniques

As explained by [24] the physical bit stream may contain long strings of zeros or ones. These strings can behave like a DC voltage, since the bits are AC coupled when transmitted over the radio. The data slicer of the radio which are responsible for producing a 1 or a 0 from the AC signal can become biased by this DC voltage to later attenuate the incoming stream. The transition in the start/stop bit may now be missed by the comparator of the radio and synchronization errors will occur when feeding incoming data to the microcontroller's USART. To overcome this problem, Manchester encoding is used, because it enforces symmetry in the data stream. Figure 2.3 from [29] shows that for each clock signal, there is both a high and low transition in differential Manchester encoding, yielding a bit stream with no long stings of ones or zeros, which will produce unbiased data at the receiver.

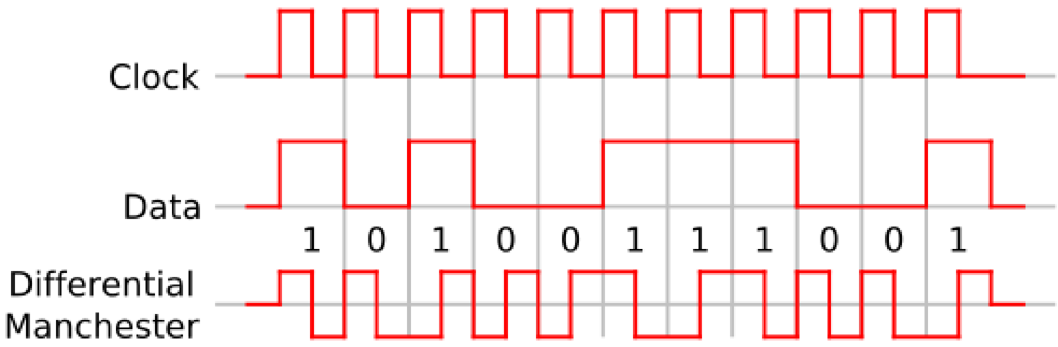

Figure 2.3: Manchester encoding

The flow of information through the physical layer is shown by figure 2.4. It shows the bit stream being line coded into a Manchester code and then modulated onto a radio frequency by the transmitter. The receiver demodulates the analog radio frequency into a digital signal, which is Manchester decoded to deliver the original base band signal.

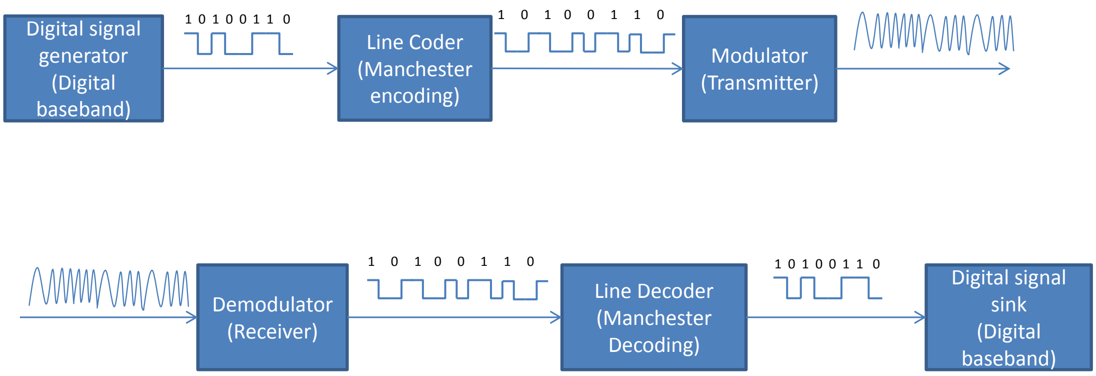

Figure 2.4: Physical layer

2.3 Medium Access Control (MAC) and routing Protocol selection

The MAC protocol's main goal is to control each node's access to the shared wireless medium. The routing protocol has the task of routing data packets through the network to a destination. Both of these protocols has to be chosen out of the abundance of existing protocols to best fit the application at hand. When considering these protocols we keep in mind the assumption that leopards will visit milking stations infrequently because of their huge dwelling area. We also consider the fact that nodes will have to reside in secluded areas for having the most success of downloading leopard data, thus power awareness is of concern. Another consideration is the low bandwidth used by long range VHF telemetry equipment.

The following section will discuss the most popular MAC protocols used for ad hoc networks.

2.3.1 Data link layer - MAC Protocols

MAC protocols for wireless media differ from its wired counterpart in that it suffers from issues such as error-prone shared broadcast channel, hidden and exposed terminal problems, limited bandwidth availability, node mobility and power constraints. Protocols designed for wireless media try to overcome these issues. To make effective use of the shared broadcast channel, collisions should be minimized by the MAC protocol and fair access should be granted to all nodes. The throughput of the network is influenced by the hidden and exposed terminal problems. Figure 2.5 demonstrates these problems. The hidden terminal problem occurs when two nodes who do not know of each other, in this case N1 and N2, transmit at the same time and cause a collision at the receiver R1. The exposed terminal problem occurs when one node is in transmission range of another transmitting node, and can therefore not transmit to its receiver for fear of interference of the ongoing transmission. In this case N2 is transmitting to R1 and N3 cannot send to R2. The scarce bandwidth of the channel should be used efficiently by reducing control overhead, that is increasing the ratio of data transmitted to the the control packets transmitted. The degree of mobility of nodes should be taken into account when designing a protocol to not drastically influence the performance of the network. The power of a wireless node is limited as it makes use of a battery, thus a protocol should again minimize the overhead so as to spare battery power [21]. Networks in wireless communication are broadcast networks as opposed to point-to-point connections. The key problem with such networks is to determine which nodes transmit when so that collisions do not occur when a few nodes start to transmit simultaneously.

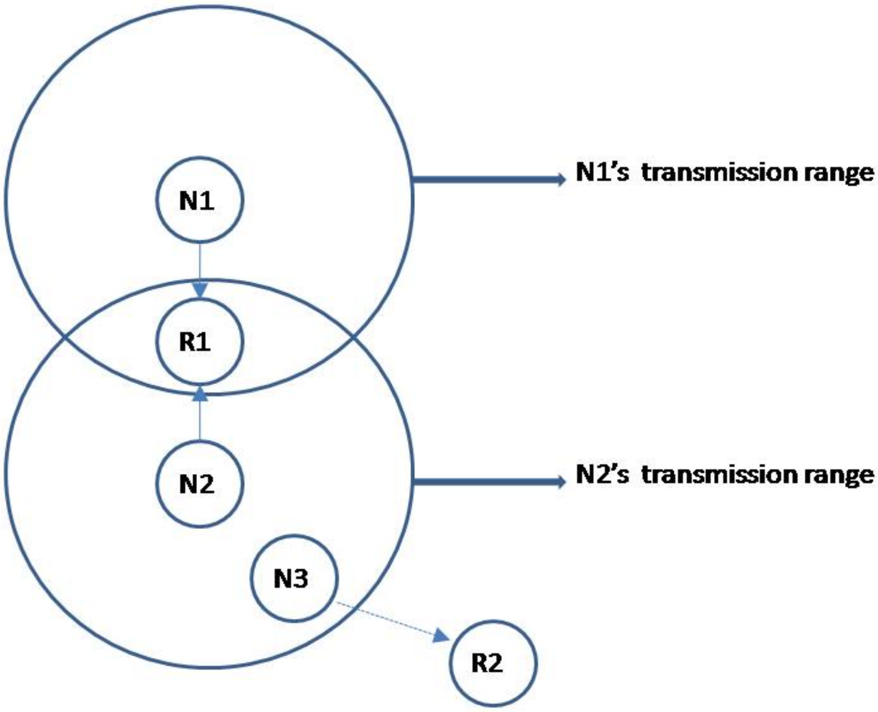

Figure 2.5: Hidden and exposed terminal problems

2.3.1.1 Reservation-based protocols

In this class of protocols collisions do not occur, thus efficient use of the medium is made possible. A central entity controls the access to the channel and gives every node a fair chance.

Round Robin Polling A host polls each node individually granting that node access to the channel for a certain period of time, to give fair access. An advantage of this system is that the host has a global view of the network as opposed to the rather limited one a node would have. The host could thus implement a variety of algorithms to optimize the whole queuing system to a specific metric. For example if it is important that no data is lost due to full queues at nodes, the host could give access to those nodes first to prevent customers from being shown away. The drawback of this scheme is that it generates significant overhead if nodes transmit data infrequently, thus leading to unnecessary polling. Hybrid schemes attempt to overcome this by keeping a list of nodes that transmit frequently and by only polling them. If a dormant node has something to send, it uses contention to connect with the central controller and is then added to the list for frequent polling. [17]

Token Ring A central controller generates a token that is passed from node to node. When a node has possession of the token it has permission to transmit its messages to other nodes. The central controller will check from time to time if the token is still in circulation and generate a new one if the token got lost. A node may only transmit when it has possession of the token and only for a predefined time slot. The token is passed onto the next node if the current has nothing to send anymore or the time slot has passed. When a node has data to send to another node, it adds the destination and source addresses along with the data onto the token. Upon receiving the data, the destination node will remove the data from the token and replace it with an acknowledgment that will be returned to the sender. If there is long periods of time that the network is not busy, the token will be passed from one node to another indefinitely and waste the battery power of a node. Priority levels can be added to a token, so that only nodes with high priorities will receive the token at certain times.

2.3.1.2 Contention Protocols

Contention protocols, as opposed to centrally scheduled protocols, do not make any reservations for any node. The nodes are in competition with each other for access to the channel. Since no reservation is made for any node to transmit at a given time, no quality of service guarantees can be made. Figure 2.6 as adapted from [21] shows the classification of contention protocols that exist as pure contention-based, contention-based with reservation mechanisms, contention-based with scheduling mechanisms and power controlled MAC protocols. We will only discuss the most popular of these protocols.

[21]

Media Access with Collision Avoidance for Wireless (MACAW) As an alternative to CSMA (carrier sense multiple access), MACAW is designed to overcome the shortcomings of CSMA when working with wireless networks, since CSMA was originally designed for wired networks. The problem with CSMA on wireless networks is that the contention occurs at the receiver rather than at the transmitter (as with wired networks). Thus it does not overcome the hidden terminal problem. In wireless networks the receiver should be contending for bandwidth so as to eliminate the possibility of another transmitter sending whilst a transmission is ongoing. Thus the carrier sensing done by the transmitter is of no use in wireless networks. MACAW is an extension of MACA (Media Access Collision Avoidance). MACA overcomes the hidden and exposed terminal problems by making use of packet signaling instead of carrier sensing. The two signaling packets is the RTS (request to send) and the CTS (clear to send) packets. Refer to figure 2.7 for the MACA message exchange. The transmitter starts with a RTS packet which is received by both the receiver and the neighbor of the transmitter. The neighbor node knows not to transmit until the transmitter has received a CTS. This CTS is also heard by the neighboring nodes of the receiver and they know not to transmit while data packets will be sent. The duration of this transmission is contained in both the RTS and CTS packets. Effectively the hidden and exposed terminal problems is now overcome.

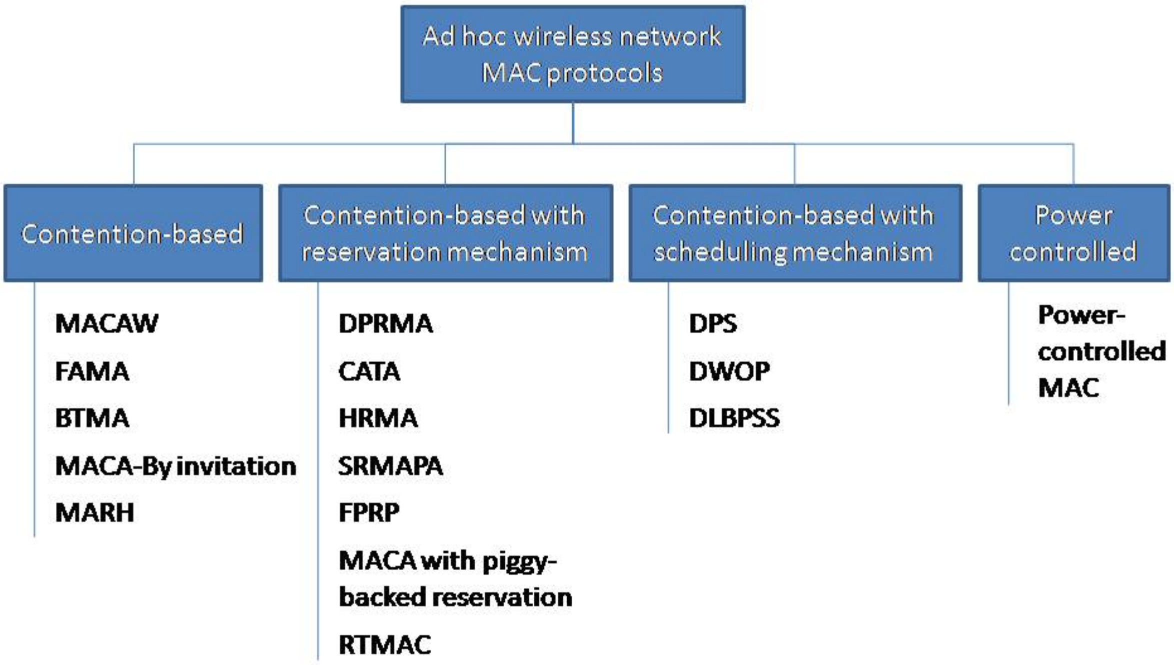

Figure 2.6: Contention MAC protocol classification

MACAW now improves on the design by changing the BEB (binary exponential backoff) algorithm used by MACA. The BEB algorithm used by MACA can cause some nodes to become blocked, because of an increasing back-off period when the transmission channel is already captured. The MACAW protocol allocates bandwidth in a fair manner by including the back-off counter into the header of the packet sent by the transmitting node. The back-off counter value is also adjusted less rapidly. The back-off algorithm is run independently for each queue at a node, rather than for each flow. This creates more fairness among nodes. [21]

Floor Acquisition Multiple Access (FAMA) FAMA makes use of both carrier-sensing and the RTS-CTS control exchange to gain control of the channel. This protocol guarantees that no data packet will ever collide with any other packet, be it control packets or other data packets. Control packets may collide with other control packets. An exchange of control packets is required to acquire the channel, whilst carrier-sensing is used to determine if a station should back-off or go forth with the exchange. [21]

[16] discusses two variants of this protocol: FAMA-NPR and FAMA-NBR. The authors claim that both these variants gets up to 39% better throughput than MACAW and also provide a solution to the exposed-receiver problem not addressed by MACAW. One advantage of FAMA is that a train of data messages can be sent by a station providing a performance inprovement of 25 % over single-packet transmission and 55 % over MACAW with single-packet transmission.

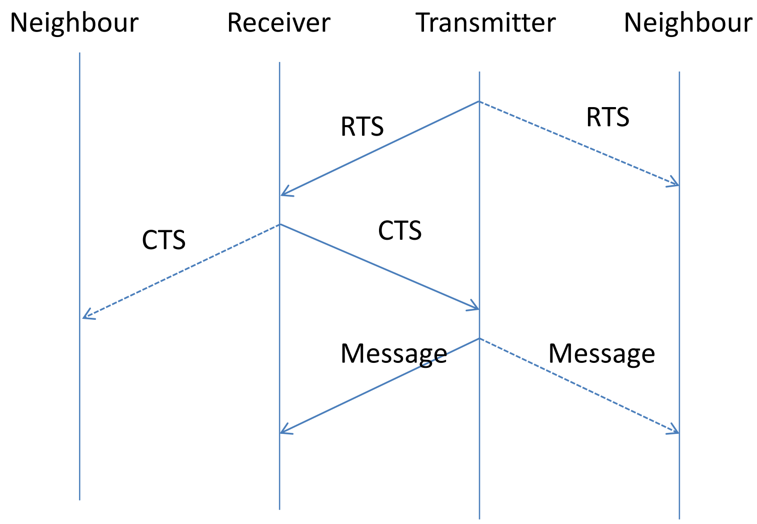

Figure 2.7: MACA illustrated

Power control MAC protocol With this protocol nodes can manage the power with which each packet is sent, thus conserving power when communicating short-distance. The two control packets RTS and CTS are transmitted with maximum power, whilst the data and ACK packets with the adapted power level. The RTS packet is received at the receiver at a certain power level. Knowing what the original power level was, the receiver can now calculate the attenuation and thus the minimum power level at which a packet can be sent. This power level is added to the CTS packet, so that the transmitter can send the data at that power level. The ACK packet is returned at the same power level. This can cause hidden terminal problems, due to the fact that the transmission range of the DATA packet is smaller than that of the RTS and CTS packets. The solution is that the power level of the DATA packet is increased periodically during the same transmission, causing neighbor nodes to sense that the transmission is still ongoing and thus to back-off. [21]

Summary Of the reservation-based schemes round robin polling (RRP) performs best, because the central controller knows the state of the system and can thus act upon that knowledge, whilst token-based schemes have limited knowledge of the state of the system. Contention based-schemes are generally simpler than reservation-based schemes and offer better performance at light traffic loading as no permission is required to transmit [17]. When considering that leopards will visit milking stations infrequently and thus generate data packets infrequently, a contention protocol seems to be an attractive choice, since such a protocol only seeks access to the medium once it has data to send to another node.

With reservation-based protocols nodes are continuously probed for data. This kind of protocols can waste bandwidth and energy if the network is used infrequently. Of the three MAC protocols discussed, FAMA and Power control MAC need extra circuitry for performing their tasks which can make the physical layer more complex than necessary. FAMA depends on carrier sensing for gaining access to the channel, which can be highly unreliable [26]. Power control circuitry (as required with the Power control MAC) adds complexity to the radio which is also not found on common VHF radio transmitters. MACAW is a simple contention protocol which uses packets to sense the channel (virtual carrier sensing) and guarantees collision-free transmission because of its use of control packets preceding a data packet to clear the channel. Therefore we have chosen to use the MACAW protocol.

2.3.2 Network layer - routing protocols

A routing algorithm deals with ways to establish end-to-end communication through a network. Two possible ways exist to arrange this communication, namely connection-oriented and connectionless. For a connection-oriented switching technique such as circuit switching, a dedicated communications path is set up between two communicating parties. This path usually includes intermediate nodes. The connection is then reserved or guaranteed for the entire duration of time that the two parties want to communicate. For a connectionless switching technique such as packet switching, the information to be sent between two parties are divided into chunks called units or packets. Each unit is provided with address information to find its way through the network to its destination. Circuit switching has the advantage that the connection is guaranteed for the entire duration that information wants to be transferred, and the transfer is unaffected by network traffic. The disadvantage lies in the bandwidth that is wasted during times of no information transfer. In wireless mobile networks this would also be inefficient, as the connection has to be reestablished every time a node moves or link quality becomes unacceptable. Packet switching has the advantage that it uses the network only when information is to be transferred, thus saving on bandwidth. The disadvantage is that some overhead and thus additional information is introduced to indicate the source and destination addresses of each packet. However, we will use a packet switched technique because of the wireless medium being unreliable. In the case of circuit switching this could lead to many connection breaks, leading to much wasted bandwidth. We will now discuss a number of routing protocols in order to select an appropriate protocol for our system.

2.3.2.1 Table driven routing protocols

The two major categories in this class of protocols are Link State Routing(LSR) and Distance Vector Routing(DVR). The major difference between the two resides in the way in which each node constructs its routing table and the amount of information that is included in a routing table.

Link state routing (LSR) Link state routing is used in packet switched networks. Each node in the network that is prepared to forward a packet performs this protocol on the packet. The concept lies in that each node independently forms a map of how it is connected to every other node in the network. It then can find the next logical hop from it to every other destination in the network. The combination of all these logical hops forms the routing table of a certain node. In this protocol the information shared between nodes is only connectivity related, which means that nodes don't share their routing tables with other nodes. Each node is responsible for constructing its own routing table. It is required that a router running this protocol informs all the nodes in the network of topology changes and thus not only its neighbors. [21]

Optimized link state routing (OLSR) OLSR is a proactive or table-driven routing protocol. It operates by electing MPR (multi-point relay) nodes to efficiently broadcast hello-messages for updating of routing tables. These MPR nodes are elected by neighboring nodes due to the fact that they have the most links connected to them, and therefore will reach the most nodes with their broadcast messages. Broadcast messages are sent out from time to time by these MPR's to update the tables of its neighbors with new topology information. Two kinds of messages exist within this protocol: Hello-messages and Topology control messages to discover and then disseminate topology information throughout the network. [21]

Distance Vector Routing (DVR) The Bellman-Ford Algorithm is used to calculate paths in this protocol. DVR calculates routes based only on link costs. The cost of reaching a destination is calculated using a specific routing metric. Metrics that can be used includes hop count, node delay, bandwidth and, for mobile nodes, battery power. It is required that a router using this protocol informs only its neighbors of changes in topology and not the whole network as with link state routing(LSR). As is indicated by the name, the DVR protocol calculates the distance and direction of the next hop to any link in a network. Two disadvantages of using the Bellman-Ford Algorithm are the count-to-infinity-problem and routing loops. The count-to-infinity-problem occurs when a node goes down. The other nodes then still propagate route information containing this unusable node. This false information is slowly propagated through the network until it reaches all the nodes(infinity). The routing loop problem describes the phenomenon when a route to a destination points back to the starting node, because of nodes in the path not having information about the overall topology of the network. [21]

Destination-Sequenced Distance Vector (DSDV) The DSDV routing protocol depends on global and periodic dissemination of connectivity information for its correct operation. It is only effective for small networks because the control message overhead grows as $O(n^2)$ where n is the number of nodes in the network. This protocol also requires each node to keep a table with all routes to all destinations. This requires increasing amounts of memory as the network grows. Each table contains the shortest distance and the first node on this path to every other node in the network. Loop prevention is done by increasing sequence tags for table updates. If a node senses a significant change in local topology, tables are forwarded to other nodes reflecting this change. On receiving a table, a node checks the sequence number and based on the received information, a node may reject, or update its own table and forward this information. This protocol however reduces route acquisition latency before the transmission of a first message to a destination. [21]

Wireless routing protocol (WRP) WRP is an enhanced version of the distance vector protocol and introduces mechanisms to reduce route loops and ensure reliable message exchanges. This protocol keeps four tables to maintain more accurate information namely: distance table (DT), routing table (RT), link cost table (LCT), and a message retransmission list (MRL). While DSDV is similar to WRP, it only maintains a topology table. The advantages in keeping these tables over DSDV includes that less table updates are required and faster convergence of routes is possible. However, similar to DSDV, it also suffers from limited scalability. More tables requires more memory and more processing power to keep them updated. This protocol counters the count-to-infinity- and routing loop problems by storing the successive and previous hops. [21]

2.3.2.2 On-demand routing protocols

An on-demand routing protocol only finds a route when there is demand for one, and is not pro-active like its table-driven counterpart.

Dynamic source routing (DSR) DSR attempts to minimize bandwidth wasted by routing overhead such as periodic routing update messages (as is used in table-driven approaches). Instead it broadcasts Route Request packets throughout the network in order to receive a Route Reply from the destination node containing the route it traversed. A sequence number is built into the route request to avoid loop formation and duplicate route requests. Nodes keep a route cache to store routing information it overheard and can thus reduce the route setup time when it already knows a route to the destination. Multiple Route Replies may be received by the source node via different routes, therefore the source node selects the latest and best route according to some metric. A data packet will carry the complete set of intermediate nodes to its destination. [21]

Ad-hoc On-Demand Distance Vector Routing (AODV) AODV differs from DSR in that it does not send the addresses of each intermediate node on the path to the destination along with the data packets. Each node stores the next hop in its cache and thus makes path information unnecessary in a data packet. This decreases the overhead of a data packet. AODV always determines up-to-date path information because of its use of a destination sequence number(DestSeqNum). A node will only update its path information if the current DestSeqNum is greater than the previous one. [21]

AODVjr AODVjr is a simplified version from the full featured AODV protocol described above. [12] compared the two in simulation and found that AODVjr performed just as well as AODV. The benefit of implementing AODVjr is that it eliminates many sections of the specification which is prone to erroneous programming. AODVjr differs from AODV in the following aspects:

- No intermediate nodes may respond to a RREQ
- Route lifetimes are only updated by the reception of messages
- Route error message, hello messages and sequence numbers are eliminated

Temporally ordered routing algorithm(TORA) TORA, similar to DSR, is a source-initiated on-demand routing protocol. It is unique in that it is able to detect partitions and keep control packets to a limited region when a path breaks. The routing metric used in TORA is the distance to the destination. Similar to most routing protocols it performs the basic tasks of establishing, maintaining and erasing routes. Similar to AODV, when demand exists for a route by a data packet, a route finding or Query packet is broadcast throughout the network. When it reaches the destination node it responds with an Update packet. Each node that reverses this Update packet to the source node, sets a field in the packet indicating its distance from the destination node, so that the source node can choose the route with the shortest path. When any node detects a link break in the forward path, it sends an Update packet back on the path to the source with a distance value higher than the neighboring nodes. A Clear message is issued when a partition is detected which only erases routing information in that partition. The reconfiguration of routes can lead to non-optimal routes. [21]

2.3.2.3 Summary

Pro-active routing protocols uses bandwidth and energy to continuously update their routing tables by sharing topology information, while reactive routing protocols will only use the channel once a route to a destination is required. Keeping in mind that the network nodes will remain mostly stationary (nomadic) and that changes in routes will not occur that often, it is realized that a reactive protocol will be more suited to the application. It is also important that nodes poll leopard collars more frequent (so that leopards don't slip by) than sending out messages for updating tables the whole time. AODV is selected as the routing protocol because it uses less resources (memory and bandwidth) than pro-active schemes. In comparison to source routing schemes, AODV introduces less routing overhead because it only points to the next node on the route (distance vector), instead of containing all the addresses of all the nodes on the route in a packet header. For implementation purposes the simpler AODVjr will be used.

2.4 Addressing

For an ad hoc implementation we consider four ways of assigning addresses to a node:

- Hard-coding in software
- Hard-coding in hardware
- Distributed address assignment
- Central address assignment

Advantages and disadvantages of each technique: Hard-coding each node's address in software before deployment ensures that each node always has a unique address. The disadvantage is that the user will need the designer to code nodes with new addresses every time new nodes need to be added to the network. Hard-coding each node's address in hardware enables the user to set addresses manually at will, however there is always the possibility that the user mistakingly duplicates addresses. Designers tend to rather make most designs as transparent as possible to the end-user.

Distributed addressing refers to the scheme where each node randomly chooses an address, then sends out address verification messages to determine if the same address already exists. If not, the address is assumed, otherwise another random address is chosen and the process repeated until a unique address is found. The advantage of this scheme would be that nodes can be added to the network at will and every node will automatically find itself an address. The disadvantage is that the possibility for duplicates still exists when the network tends to get segmented.

Central addressing refers to the scheme where a central node or base station handles all addressing, therefore duplicates cannot arise. The disadvantage is that considerable network usage is required to establish and reestablish addresses of all nodes when new nodes arrive or once dead nodes come alive again.

Too avoid any problems with addressing and keeping the network simple and robust, we choose the reliable hard-coding of each address in software.

2.5 Summary

The OSI reference model is used to divide the communication tasks into layers. The physical layer implements a radio with FSK modulation and Manchester encoding as channel coding technique. The MACAW protocol will be implemented as a MAC strategy on the data link layer, because of its simplicity and contention basis. We expect this will save on energy and bandwidth in the infrequently used network. The AODVjr protocol will be implemented as a routing protocol on the network layer, because of its reactive nature which we expect will also save on energy and leave more time for milking stations to perform polling of leopard collars. The software hard-coding addressing technique will be used.

Chapter 3

Theoretical work

3.1 Design constraints

The wireless medium used to propagate information poses some restrictions. The following are the restrictions concerned with the channel capacity, throughput, regulatory constraints and link distance.

3.1.1 Regulatory constraint

ICASA (Independent Communications Authority of South Africa) specifies the 148 to 152 MHz frequency band as license less for wildlife telemetry tracking, but with the constraint of a maximum radiated power of 25mW [2]. The Cederberg is a very secluded area, so we decided not to adhere to the maximum radiated power of 25mW, but to use radio modules with larger transmit power. Modules with a center frequency of 151.3MHz are available on the market and used by the other students working on the leopard tracking project.

3.1.2 Channel capacity

"The bandwidth of a medium is the range of frequencies that pass through it with minimum attenuation" [27]. We will now examine the theory of bandwidth and data rate using the chosen radio's specifications as selected in chapter 5. The modulation bandwidth of the radio at -3dB is given as 5kHz. In figure 3.1 the center or carrier frequency is 151.3MHz [5]. Only a range of frequencies around this center frequency is passed through a bandpass filter i.e. the bandwidth. Because filters are not perfect, the cut-off is sloped and do not end immediately at the cut-off frequencies. Thus the -3dB frequencies are given on each end, which are the same as most manufacturers give on their data sheets as the points where the amplification factor has been approximately halved. The bandwidth of the single channel given by the manufacturer for the radio module being used is 5kHz [5]. This gives the cut-off frequencies as 151.2975 MHz and 151.3025 MHz.

Claude Shannon(1948) introduced the ultimate limit on channel capacity in the presence of noise on a channel. Shannon's theorem states that:

$$\text{maximum number of bits/second} = B \log_2(1 + S/N) \text{ bits/sec} \tag{3.1.1}$$

[27]

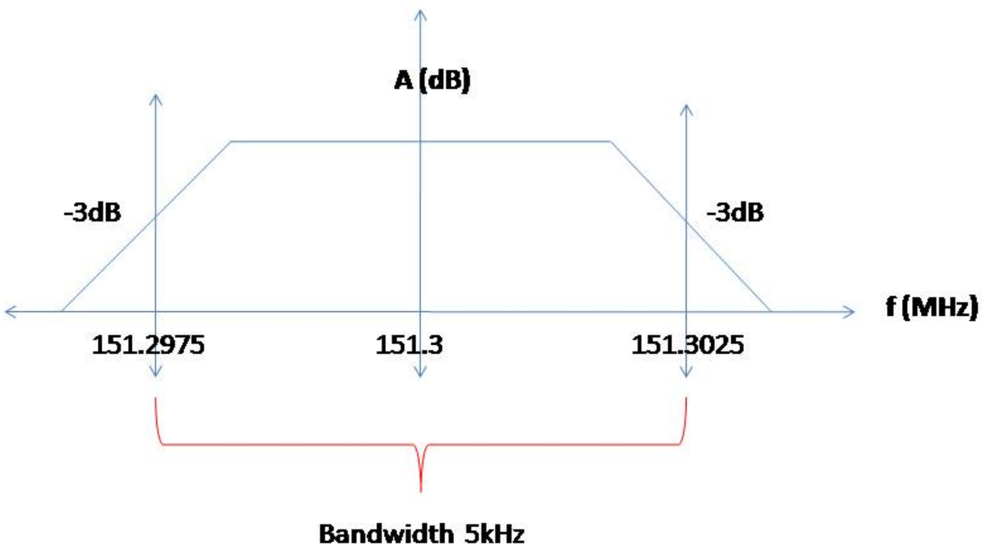

Figure 3.1: Modulation bandwidth

$$B = \text{Bandwidth in Hz}$$
$$S/N = \text{Signal to noise ratio}$$

The radio outputs 500mW of RF power, ie. signal strength S. We know that the modulation bandwidth is 5kHz, but the noise power N is still unknown. Channel noise is closely related to bandwidth. The noise is due to the motion of molecules in the system. The amount of noise is given in the datasheet in terms of SINAD = 12dB. SINAD = Signal to noise and distortion ratio. The S/N ratio from this gives 14.8

Thus,

$$\text{maximum number of bits/second} = 5\log_2(1 + 14.8) \text{ bits/sec} = 19.9 \text{ k bits/sec} \quad (3.1.2)$$

This is the theoretical maximum data-rate for a noisy channel, which is hardly ever reached. The Shannon-Hartley theorem however gives the maximum data-rate in terms of the number of discrete levels used by a modulation scheme.

The theorem states:

$$\text{maximum data rate} = 2B\log_2 V \text{ symbols/sec} \quad (3.1.3)$$

$$B = \text{Bandwidth in Hz}$$
$$V = \text{number of discrete levels}$$

We assume two discrete levels to represent the two binary digits 1 and 0, so in this case a symbol will represent a bit.

$$\text{maximum data rate} = 2 \times 5\log_2 2 \text{ symbols/sec} = 10 \text{ k symbols/sec} \quad (3.1.4)$$

The data rate of 10kb/sec is the same as the maximum data rate specified by the radio's data sheet. Note that coding schemes that make use of more than two voltage levels exist that achieve higher data rates, however the given radio module makes use of only two.

3.1.3 Throughput

A network designer always wants optimal throughput. Throughput is affected by:

1. Bit error rate at the physical layer
2. Queuing delay at the network layer

which can both can be minimized or improved. The bit error rate is caused by inevitable noise. Forward error detection and correction can be implemented in software resulting in less errors. The network routing protocol can be chosen and modified to work optimally for the specific network thus reducing routing delay as compared to the performance of other schemes.

3.2 Link Budget

The link budget takes into account all the gains and losses between two radios to predict the signal strength arriving at the receiver. These include antenna gains, cable and connector losses and attenuation due to distance between antennas.

A simple link budget calculation is as follows:

Received Power(dBm) = Transmitted Power(dBm) + Gains(dB) - Losses(dB)

$$P_r = P_t + (G_t + G_r) - (L_{fs} + L_m + L_t + L_r) \tag{3.2.1}$$

$$L_{fs} = 32.44 + 20logd + 20logf \tag{3.2.2}$$

L_{fs}=free-space loss in dB
P_r=received power in dBm
P_t=transmitted power in dBm
G_t=transmitting antenna gain in dBi
G_r=receiving antenna gain in dBi
L_m=miscellaneous losses (fade margin etc.)
L_t=transmittor losses (cable,connectors)
L_r=receiver losses (cable,connectors)
d=distance between transmitter and receiver,in km
f=frequency,in MHz

The link budget will be based on the transceiver module from Radiometrix with the following specifications:

1. Operating frequency : 151.3 MHz

2. Max transmit power : 500mW = 27dBm
3. Receiver sensitivity : -115dBm (for 1ppm BER)

And the antennae from Web Industries with a nominal gain of 2dB.

A rough first estimate will be made to determine the maximum propagation distance using free space propagation. Cable loss for RG58 at 151MHz is 14dB/100m. RG58 is a type of coaxial cable used for connecting radio frequency devices such as between the rf pin of a radio module and the antenna. Attenuation in the cable depends upon frequency. For 2m of cable the loss is thus 0.28dB. Assuming the connector between the radio module and antenna introduces a loss of 0.22dB and the total cable loss is 0.5dB.

We now have all parameter values and can calculate the maximum distance between two nodes using the maximum transmitter power rating of 500mW. From equation 3.2.2, d can be solved for:

$$d = 10^{\frac{(-P_r+P_t+G_t+G_r-L_{fs}-L_m-L_t-L_r)}{20}}$$

$$d = 10^{\frac{(115+27+2+2-32.44-20log151.3-0-1-1)}{20}}$$

$$d = 2500km$$

There are many effects other than distance that also influences the received signal not accounted for in the above equations. The more influential ones are:

- **multi-path reception:** Radio signals reaches the receiver by two or more paths due to signals being reflected and refracted by obstacles in the path.
- **shadowing:** Signal properties change due to obstacles affecting the wave propagation.
- **fading:** Difference in the S/N ratio at the receiver over time which is caused by multi-path reception or shadowing. Multi-path reception causes the signals to add or subtract according to the phase of the received signals, thus causing communication to fail with subtracting signals.
- **diffraction:** Loss of transmitted power due to obstructions in the line-of-sight path such as hills and trees.
- **scattering:** Radio waves are forced to deviate from a straight path due to non-uniformities in the medium through which they travel.

[31] suggests a fade margin of 20dB to 30dB. Recalculating using this extra loss gives a reach of 79km.

The RF link budget calculator from [10] will serve as validation software for this calculation. The link budget calculator in figure 3.2 predicts nearly the same reach as the mathematical formula.

According to [11], the practical communication distance for line-of-sight propagation is limited by the curvature of the earth. The approximate value for the maximum distance between transmitter and receiver is given by the equation:

$$d = \sqrt{17h_t} + \sqrt{17h_r} \tag{3.2.3}$$

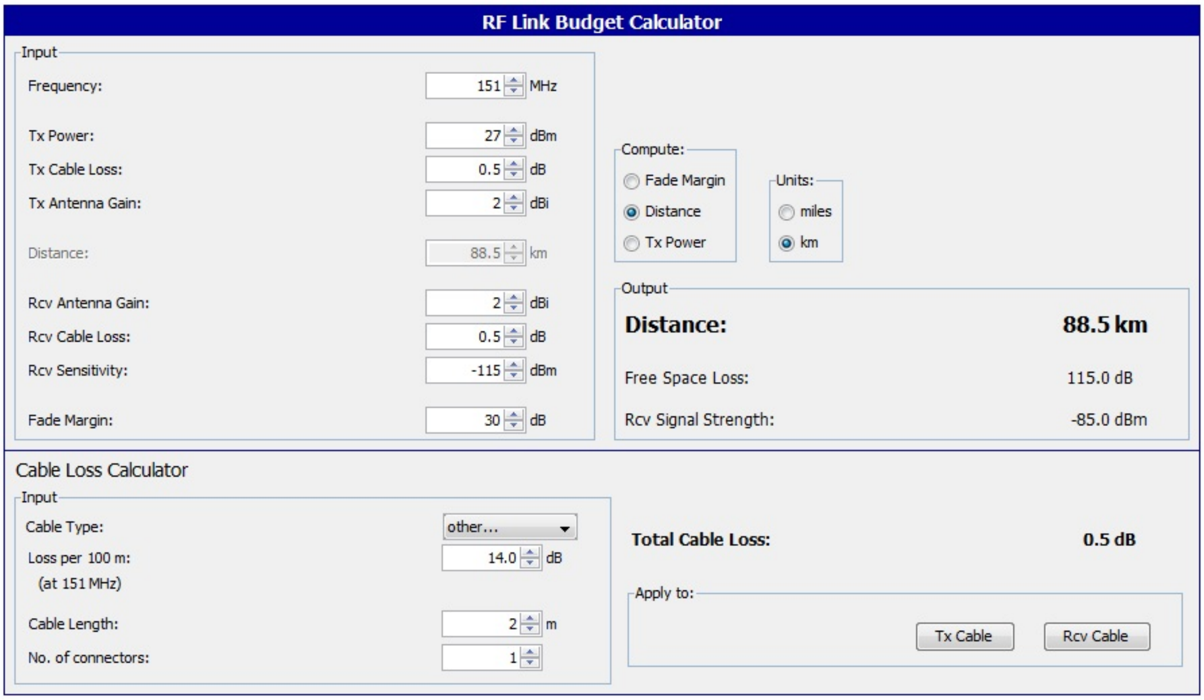

Figure 3.2: Link budget validation software

$$h_t = \text{height of transmitting antenna}$$
$$h_r = \text{height of receiving antenna}$$

$$d = \sqrt{17 \times 2} + \sqrt{17 \times 2} = 11.66km \tag{3.2.4}$$

Which limits the maximum communication distance to 11.66 km if the antennas has a height of 2 meters above the ground.

In the above calculations the effects of topographical terrain and vegetation was not accounted for. A great tool for taking into account the topography and vegetation of the area, is Radio Mobile (designed by Roger Coude). This software uses Digital Elevation Model (DEM) files, which is a digital representation of ground surface topography or terrain. In this case it uses SRTM data from the Space Shuttle Radar Terrain Mapping Mission. The propagation prediction model used by this software is the Irregular Terrain Model(ITM) developed by the US Institute for Telecommunications Science (ITS) [13]. We expect the range of the radio to drop, but need to determine the exact range. The area of study in figure 3.3 shows the coordinates of the vertices of this area. This is very useful as Radio Mobile uses these coordinates to get a digital elevation map from the Internet corresponding to the actual location on earth. The study area is projected onto the digital elevation map of the Cederberg where it is drawn in Radio Mobile as shown in figure 3.4. Wireless nodes should be placed near leopard trap cages in order to transmit single frame pictures generated from a camera at each cage. Figure 3.5 shows the study area plotted onto the digital elevation map with the wireless nodes placed in position as

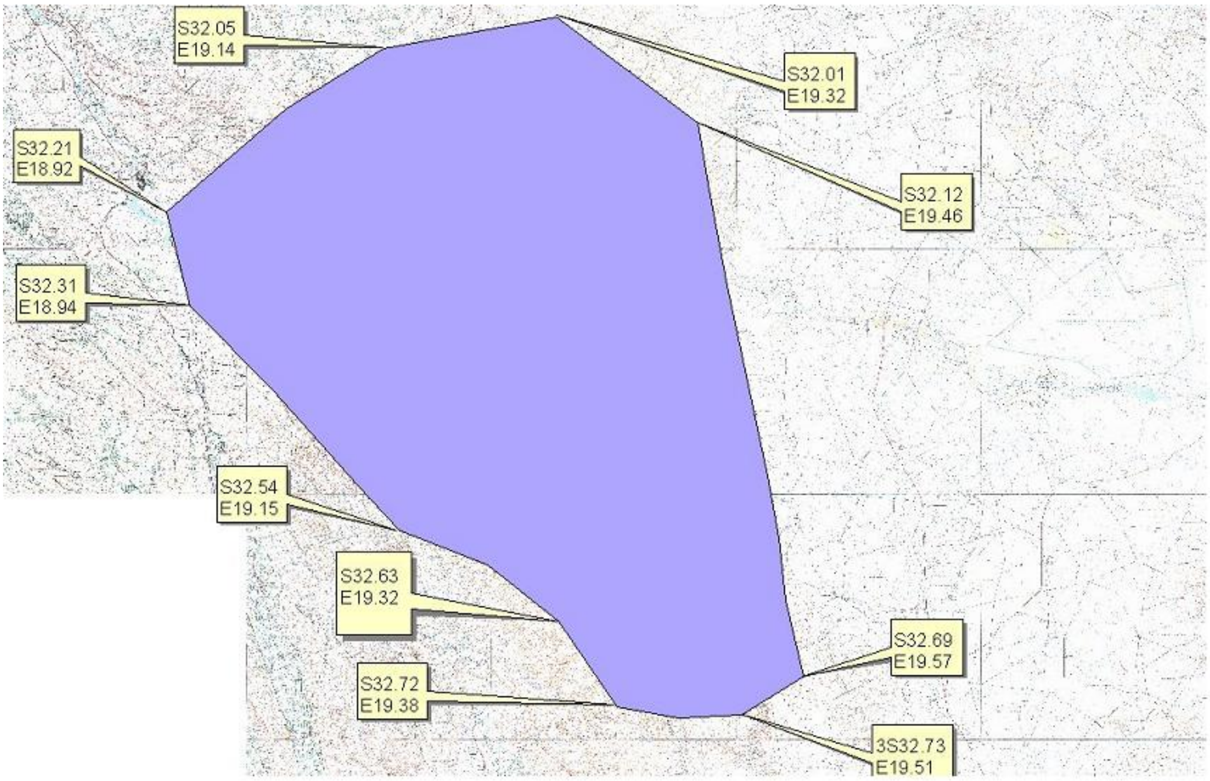

Figure 3.3: Study area

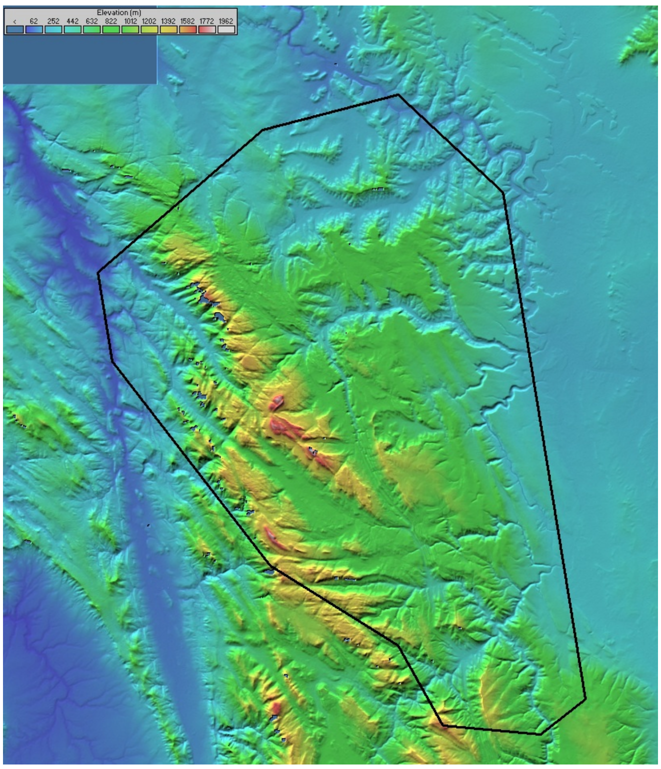

Figure 3.4: Study area as drawn in Radio Mobile

determined by the current position of leopard trap cages in the Cederberg area. Figure 3.6 shows all the cage names and coordinates.

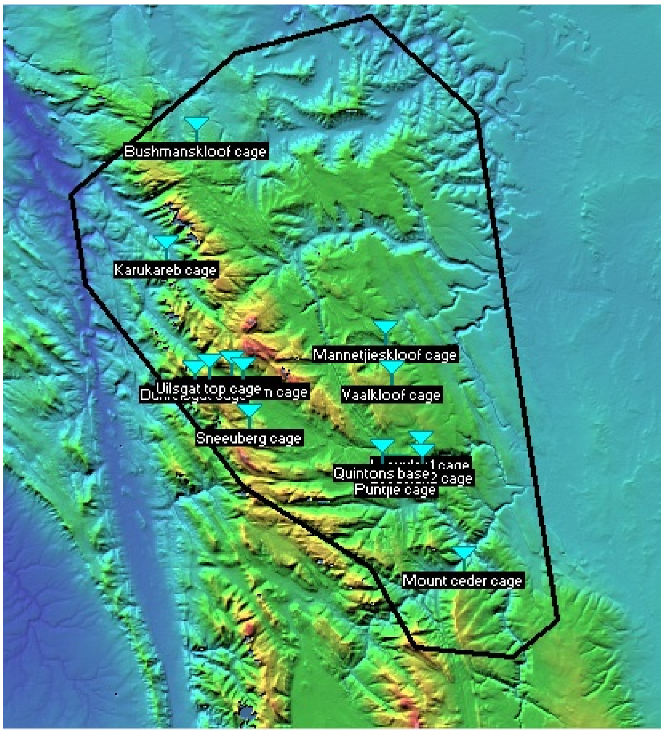

Figure 3.5: Study area showing position of nodes

When all the parameters are kept as described in the two examples above, but topography and vegetation information is included as well, only cage pairs Leeuvlak1 and Leeuvlak2, Unnamed cage and Uilsgat bottom cage, and Quintons base and Puntjie cage are connected.

The parameters used are:

- Transmit power of 27 dBm
- Receive signal strength of -115dBm
- Antenna gain of 2 dBi, which implies an omni-directional antenna
- Antenna height of 2 m
- Total cable loss of 0.5dB

To increase the number of connections, the antenna gain is boosted to 10dBi. The value of the antenna's gain is only varied to show the effect thereof, whilst a practical omni-directional antenna will never have a gain of 10dBi. Figure 3.7 shows that now only Bushmanskloof cage, Karukareb cage and Mount Ceder cage are not connected to the network. Mannetjiekloof cage and Vaalkloof cage forms a cluster. Note that the green lines between nodes show connections.

Increasing the transmit power to 37dBm with the same 10dBi antennae, delivers a network with only Bushmanskloof cage and Mount Ceder cage not connected to the network as seen in Figure 3.8. Increasing the transmit power further to 45.4 dBm (35 Watt) still does not deliver a network with all units connected. This is not desirable as the batteries should be as small as possible and last as long as possible. Also one would want to design as close to an omni-directional antenna as possible and therefore the antenna gain should approach 0dBi.

Cage name	Coordinates
Unnamed cage	32.40139S, 19.13667E
Uilsgat bottom cage	32.40806S, 19.15E
Karukareb cage	32.27083S, 19.04778E
Mannetjieskloof cage	32.36611S, 19.34111E
Vaalkloof cage	32.41084S, 19.35028E
Puntjie cage	32.51805S, 19.35389E
Leeuvlak1 cage	32.49139S, 19.38722E
Leeuvlak2 cage	32.50444S, 19.38972E
Sneeuberg cage	32.46083S, 19.16028E
Duiwelsgat cage	32.41139S, 19.08722E
Uilsgat top cage	32.40472S, 19.10611E
Mount Ceder cage	32.62083S, 19.44667E
Bushmanskloof cage	32.13639S, 19.08945E
Quintons base	32.49997S, 19.33583E

Figure 3.6: Cage names and coordinates

An alternative solution would be to add repeater units to the network and place them on strategic points in order to have all units connected to the network with as little power transmitted and as little antenna gain as possible.

It was found by inspection that by transmitting 27dBm, lowering the antenna gain to 2dBi and the antenna height to 2m and by introducing six repeater units a network will form with all units connected. This is shown in Figure 3.9.

Figure 3.10 shows the land covered in vegetation which is used by Radio Mobile to calculate a more accurate link budget for each two units. Referring to the legend on this figure, the greatest part of the area is covered in open- and closed shrub-land and grassland which does not account for too much of the signal loss. However, to the West of this area lies a strip of woodland which would cause much signal loss should a leopard dwell there.

Figure 3.11 shows a combined Cartesian coverage plot, generated by Radio Mobile for the study area. The signal strength is greatest in the red areas, whereas the white spots shows areas of little coverage. The other colors indicates signal strength in between. It is thus predicted that the network with 13 monitoring nodes, 6 relay nodes and the base station, will be able to provide coverage to leopard collars dwelling in more than 85 percent of the study area.

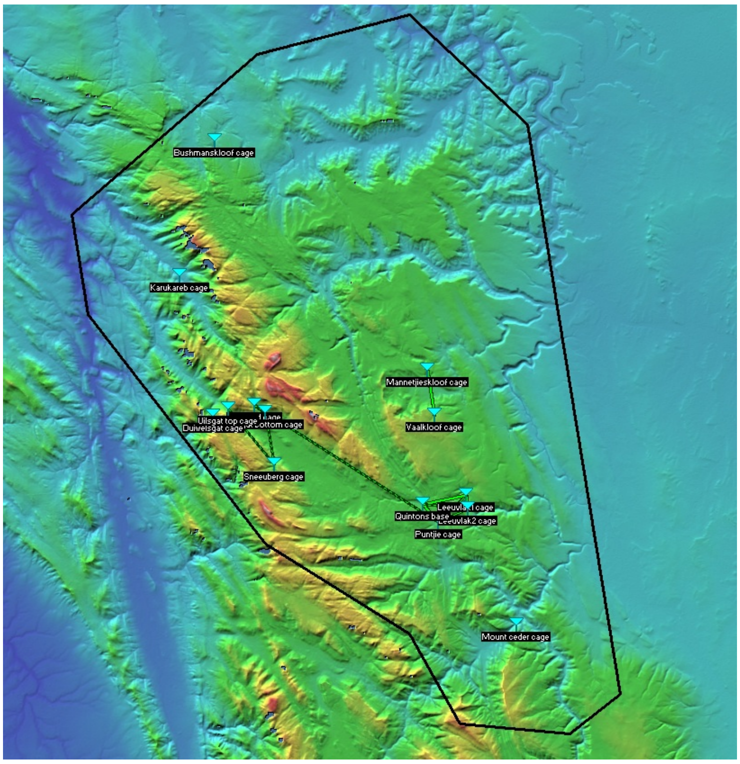

Figure 3.7: Network with units fitted 10dBi antennae and still transmitting 27dBm

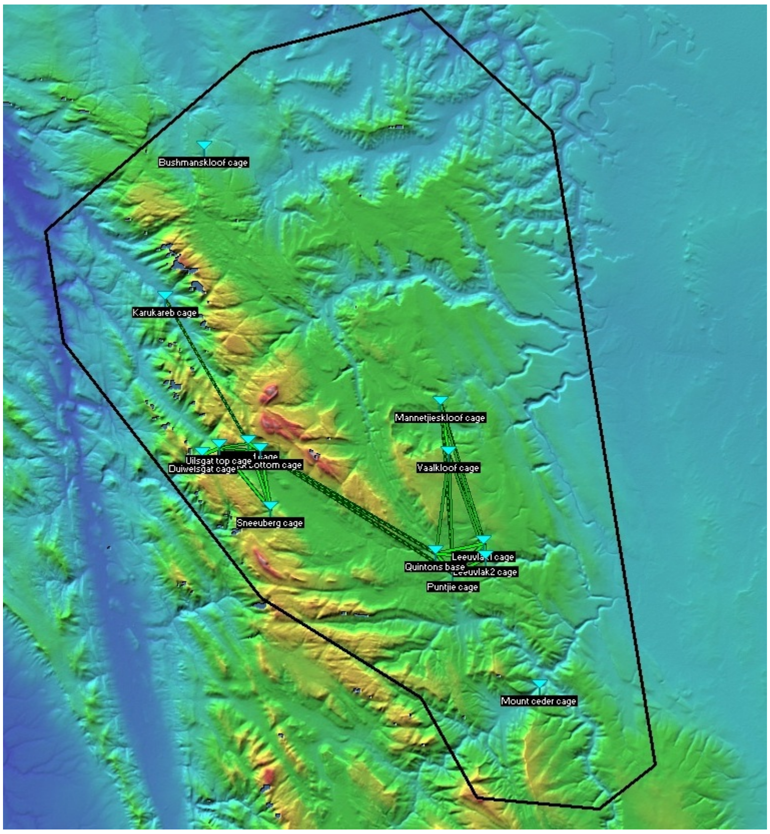

Figure 3.8: Network with units fitted 10dBi antennae and transmitting 37dBm

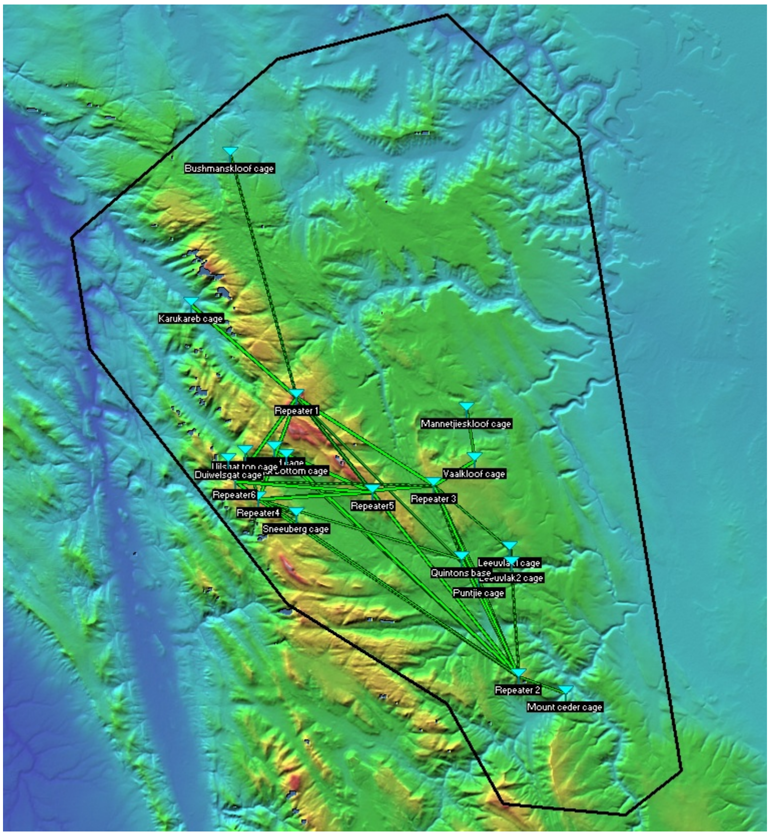

Figure 3.9: Network with all units connected by using 6 repeater nodes

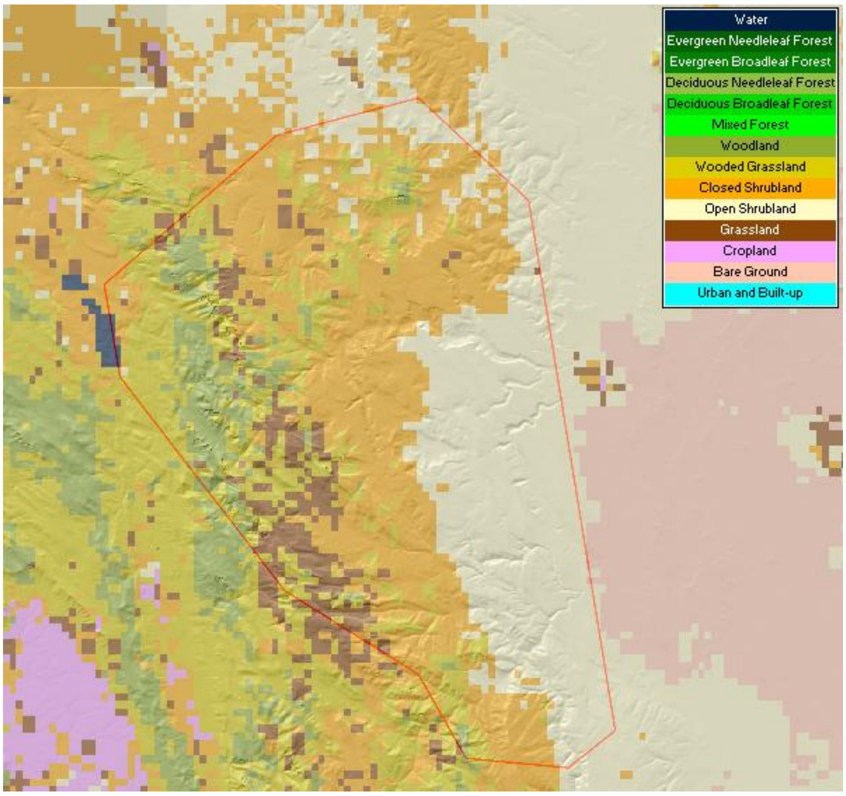

Figure 3.10: Vegetation information

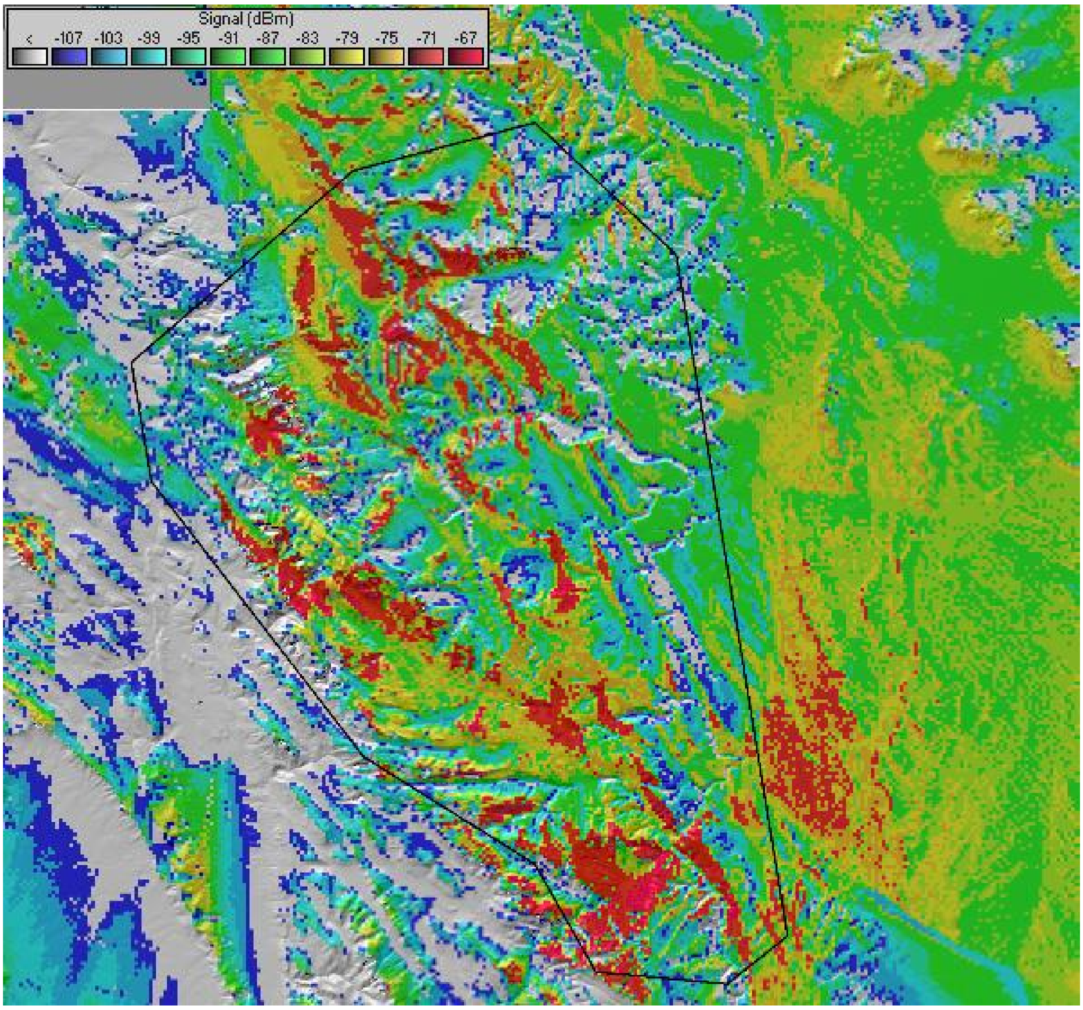

Figure 3.11: Combined Cartesian coverage plot

3.3 Summary

The ICASA specified band for wildlife telemetry tracking was found to be 148 to 152 MHz. The maximum data rate for the parameters specified under channel capacity was found to be 10kb/sec. Throughput is a function of the communication protocols implemented and will be discussed in chapter 6. The link budget was found to be affected by transmit power, distance, height of antennas above the ground, wireless channel effects like fading, topography and vegetation. All of this was accounted for by Radio Mobile which predicted that the network of 13 monitoring nodes, 6 repeater units and the base-station will form a network where all nodes are connected.

In the next chapter we will discuss the details of the MAC and routing protocols that were chosen to be most suited for our ad hoc network.

Chapter 4

Communication Strategy

4.1 Introduction

This chapter discusses the MAC (medium access control) - and routing protocols that were chosen in chapter 2 for the data link and network layers respectively. Each protocol will be described on implementation level.

4.2 Medium Access Control protocol description

The data link layer implements the MACAW protocol as discussed in chapter 2. This protocol deals with controlling access to the shared wireless medium. The main tasks of the MAC protocol is to:

1. Control access to the channel

2. Distribute bandwidth in a fair manner to all nodes

3. Assure efficient use of the bandwidth

Controlling access to the channel This protocol controls access to the channel by making use of a packet-passing scheme between two nodes. Table 4.1 shows all the messages used by the MACAW protocol. The aim of using extra packets other than just DATA packets, is to get a DATA packet to a neighboring node without collisions from DATA packets from other nodes. This is achieved by keeping nodes that overhear the packet exchange silent for a period long enough to complete a data transaction between two nodes. The MACAW protocol dictates that a RTS-CTS-DS-DATA-ACK exchange is done between two communicating nodes. See figure 4.1 for a better understanding. The solid lines represents the data intended for the receiver, while the dashed lines represents overheard packets by other nodes, because of the broadcast nature of the wireless medium. A node that has data to send begins by sending out a RTS requesting to send data to a receiver. Once the receiver receives the RTS, it immediately responds with a CTS, indicating that it is ready to receive data. The transmitter now also knows that the channel is free and it sends out a DS and DATA packet back-to-back. The DS packet indicates to all nodes adjacent to the transmitter that did not receive the CTS, that a data transaction is going to take place, so they should not transmit. Upon receiving the data the receiver will acknowledge it with an ACK packet. Note the difference in propagation time for a control packet and a DATA packet, due to the significant difference in packet

Message	Meaning	Length
RTS	Request to Send	12 bytes
CTS	Clear to Send	12 bytes
DS	Data Send	12 bytes
DATA	Data Message	255 bytes
ACK	Acknowledgement	12 bytes
RRTS	Request to send an RTS	12 bytes
POLL	Polling a collar	12 bytes

Table 4.1: MACAW message types

lengths. The data link layer of relay nodes has two focus areas: getting DATA from leopard collars and sending this data to other relay node using the described protocol. Figure 4.2 exhibits the same message exchange as in figure 4.1, but with relay nodes now sending out POLL messages to collars to invoke the described protocol. A collar will reply with a RTS only if it has DATA messages to send.

Distributing bandwidth fairly Bandwidth is distributed fairly by making use of a random back-off scheme. Each node that has data to send, sets a random timer. Only after this time has expired is the node free to try sending data with the protocol packet exchange. If more than one node starts by sending the RTS, it will collide at the receiver and no CTS packets will be sent back. The nodes now restart the contention period by resetting their random timers, but with time-out values chosen from an increased period (back-off value). This will ensure that the chance of two nodes choosing the same back-off value will decrease, also decreasing collisions. When no two timers time out simultaneously, no collisions will occur and the node with the shortest back-off period will first gain access to the channel. In this case the back-off values at nodes are decreased again. The other nodes receiving RTS, CTS or DS control packets not intended for them will refrain from transmitting and will only start contending again once the previous exchange was terminated by an ACK packet. The base station will need the most bandwidth, since it has to communicate with all other nodes, while the relay nodes only have to communicate data to the base-station. For this reason the base-station is given more bandwidth by keeping its maximum back-off value less than the relay node's back-off values.

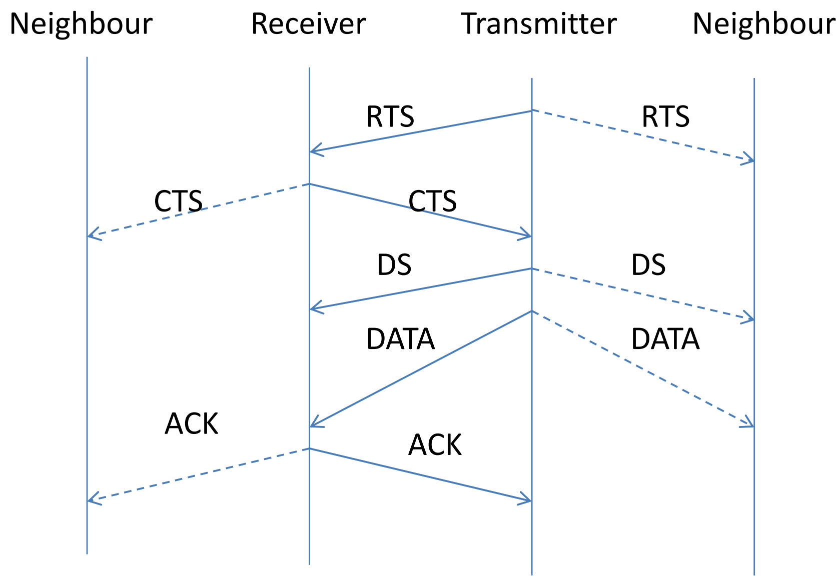

Figure 4.1: MACAW packet exchange between two relays

Efficient use of bandwidth The bandwidth is firstly used more efficiently by not using a scheduling MAC protocol between relay nodes. With MACAW any protocol exchange will only be done when one relay node has data to send to another, with the exception of polling for leopard collars. The bandwidth is also used more efficiently by letting nodes in different regions transmit simultaneously. This means that if a node receives a RTS, but not a CTS, that its transmission will not interfere with that node's receiver and therefore two transmitters can send data to their respective receivers simultaneously. The back-off periods is kept as small as possible and scaled according to the number of nodes in the network so as not to waste time during contention periods.

4.2.1 Detail protocol description

The protocol has three main flows or functionalities which can be seen in figure 4.3 as the left, right and middle flows. The middle flow shows the states for a normal RTS-CTS-DS-DATA-ACK exchange between two relaying nodes. The left flow shows the transaction between a relay and a collar node. The right flow shows the states a node goes through when overhearing packets not intended for itself. A relay node will perform the tasks of both monitoring for leopard collar presence as well as transferring received data messages between relay nodes. Note that all broadcast packets like the POLL packet and

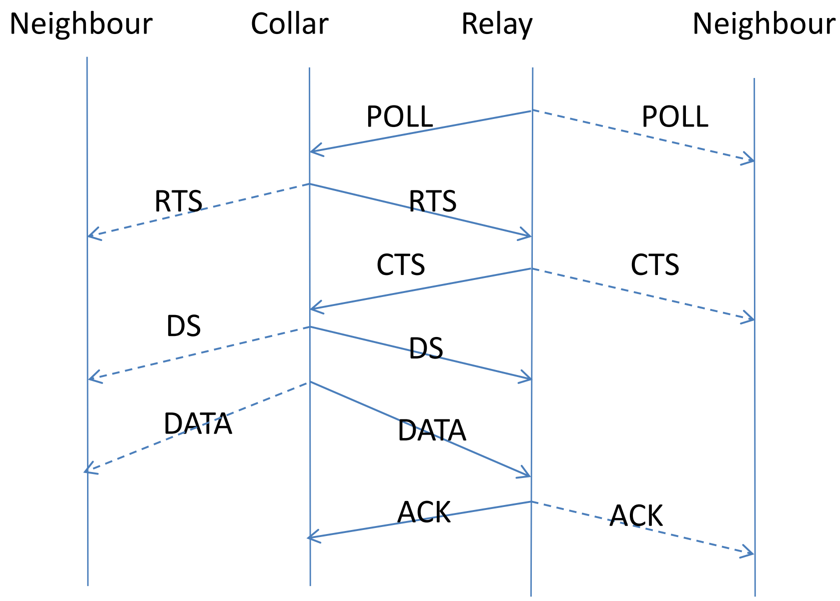

Figure 4.2: MACAW packet exchange between collar and relay

network broadcast messages are sent without the RTS-CTS-DS-DATA-ACK exchange. Only unicast packets from the network layer are transmitted this way, where DATA means any network unicast packet. We will now describe the detail state machine which forms the MACAW protocol for implementation purposes. The main goal of this state machine is to progress through the states by sending and receiving packets in an orderly manner and to return to the right state after a time-out of some sort (a packet got lost) so that protocol exchange can continue in a known state.

Figure 4.3 and 4.4 shows the program structure of this protocol. Note that the protocol for a wireless relay node and a collar node are slightly different. This is because the relay nodes has to poll the collars as well as their basic tasks of forwarding packets between relay nodes.

Communication between two relay nodes: The machine always starts in the IDLE state. When a message arrives from the upper network layer, it goes into the CONTEND_1 state and sets a random back-off timer. When this timer expires it sends a RTS to the next hop neighbor as specified by the network message and goes to the WFCTS state. If a CTS is received in time, it goes to the XMIT state and sends out a DS and DATA packet back-to-back. If a CTS is not received, the machine tries resending the RTS packet three times before it gives up and sends an error message to the network layer. If an

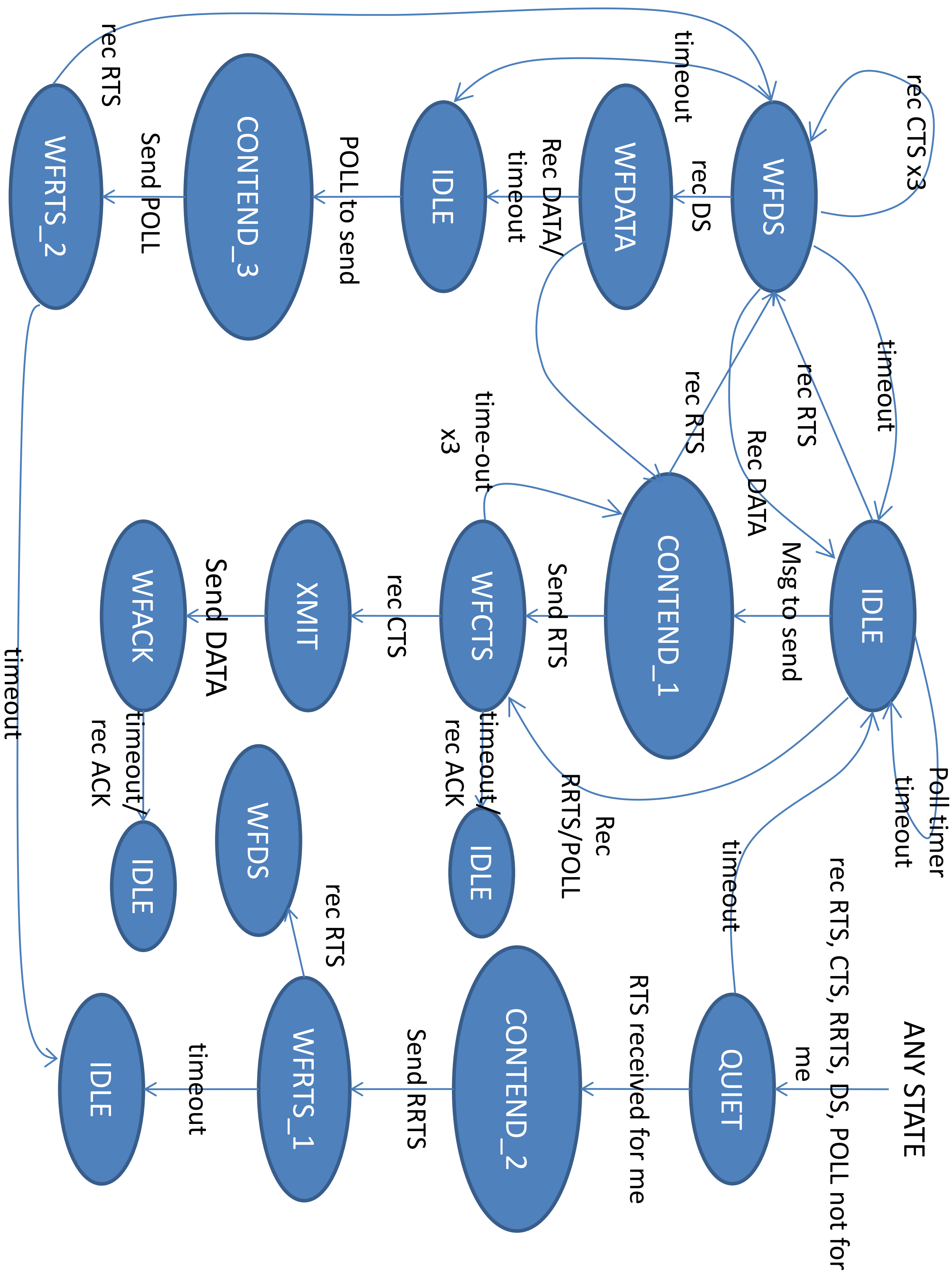

Figure 4.3: MACAW for relay nodes

ACK is received after sending out the DATA and DS packets, the network message can be deleted from the MAC queue. Otherwise it stays on the queue and gets resent when the machine times out and goes back to the IDLE state. Looking at the left flow, when a receiving node is in the IDLE state and receives the RTS from the transmitter, it goes to the WFDS state and sends a CTS back to the transmitter. When the machine times out and no DS packet has arrived, a CTS can be sent up to three times before it times out

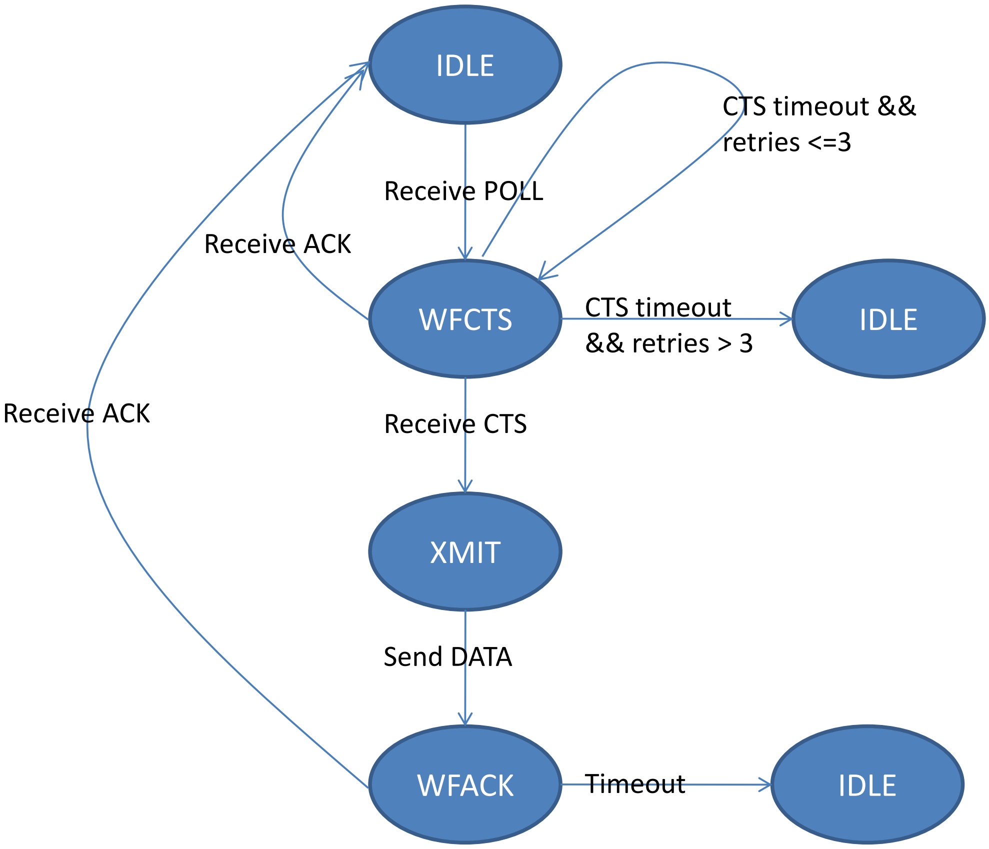

Figure 4.4: MACAW for leopard nodes

and goes back to the IDLE state. However, if a DS has arrived, it goes to the WFDATA state. If no DATA arrives it once again returns to the IDLE state. If DATA arrives, it goes to the IDLE state, but sends out an ACK packet to the transmitter. A packet is passed from the data link layer to the network layer only if the destination address of the packet matches the nodes' network address, or if that field indicates a broadcast packet.

Communication between a relay and a collar node: The MAC layer sets a timer to regularly time out and send a POLL message. This only happens when the machine is in the IDLE state upon timeout, otherwise it sets a flag and sends the POLL as soon as the machine goes back into the IDLE state. If a leopard is in communication distance, it receives the POLL and sends a RTS back to the relay node. Refer to figure 4.4 for the collar node's state diagram. It now follows the normal RTS-CTS-DS-DATA-ACK exchange, except that the collar doesn't have to set a random timer before the RTS, it sends the RTS immediately upon receiving a POLL message. Therefore there is also not a CONTEND_1 state in this state diagram. On the receiving side, the relay nodes' state machine goes into the CONTEND_3 state when a POLL has to be sent. When the random timer times out it sends the POLL and goes to the WFRTS_2 state. From here it follows the same state changes and message passing as discussed above.

Quiet times: Any node, including collar nodes, has to refrain from transmitting when an ongoing transaction is taking place to avoid interference. When a RTS, CTS, RRTS, DS or POLL message is received that is not intended for this node, the node goes into the QUIET state and sets a defined timer to not transmit for. For instance when a CTS is received, the node has to refrain from transmitting for the period of a DS and DATA message. When a RTS is received, it only has to refrain from transmitting for the period of a CTS. This is to prevent the overhearing node of refraining from transmitting the whole time if a transaction failed between two nodes. The overhearing node can then interrupt with its own transmission since the channel is free. It should be noted that in the case that a RTS is received by an overhearing node while in the QUIET state, it sets a flag to send a RRTS when coming out of the QUIET state. This is to give nodes that is always caught in others' conversation a change to also transmit. When this happens the node goes from the QUIET state to the CONTEND_2 state where it sets a random back-off timer. On expiration it sends out the RRTS packet and goes to the WFRTS_1 state. If no RTS is received it simply goes back to the IDLE state. Otherwise it follows the RTS-CTS-DS-DATA-ACK exchange as discussed above. Table 4.2 through 4.4 shows which events triggers which actions in the state machine and which conditions should be met for a certain action to take place. This corresponds with figures 4.3 and 4.4.

Event	Predicate	Action
Receive POLL	State == IDLE	• send RTS • State = WFCTS • Set timer for CTS receive
Receive CTS	State == WFCTS	• Send DS • State = XMIT • Clear timer
DS finished transmit	State ==XMIT	• Send DATA • State = WFACK • Set timer for ACK receive
Receive ACK	State == WFACK	• Delete msg from queue • Clear timer • State = IDLE
Receive ACK	State == WFCTS	• Delete appropriate msg from queue • Clear timer • State = IDLE
Timer times out	State == WFCTS/WFACK	• State = IDLE
Timer times out	State == WFCTS, txAttempts < 3	• Send RTS • Set timer for CTS receive
Timer times out	State == WFCTS, txAttempts >= 3	• State = IDLE • Msg-dropped to network layer

Table 4.2: MACAW event predicate action for Collar

Packet setup When a data stream comes in from the physical layer, it is formatted into frames by examining the first byte to determine the packet type. This byte tells the

Event	Predicate	Action
Message to send	State == IDLE	• Put msg in queue • Set back-off timer • State = CONTEND_1
Back-off timer expires	State == CONTEND_1	• Send RTS • State = WFCTS • Set timer for CTS
Receive CTS	State == WFCTS	• Send DS • State = XMIT • Clear timer
DS finished sending	State == XMIT	• Send DATA • State = WFACK • Set timer for ACK
Receive ACK	State == WFACK/WFCTS	• Delete appropriate msg from queue • Clear timer • State = IDLE
Timer times out	State == WFACK/WFDATA/QUIET	• state = IDLE
Timer times out	State == WFCTS, txAttempts < 3	• Send RTS • Set timer for CTS • Increment txAttempts
Timer times out	State == WFCTS, txAttempts >= 3	• State = IDLE • Msg-dropped to network layer • txAttempts = 0
Timer times out	State == WFDS, txAttempts < 3	• Send CTS • Set timer for DS • Increment rxAttempts
Timer times out	State == WFDS, txAttempts >= 3	• State= IDLE • rxAttempts = 0
Receive DATA	State == WFDS/WFDATA	• Send ACK • Sate= IDLE • Clear timer • Send to network layer
Receive RTS	State == IDLE/CONTEND_1	• State = WFDS • Set timer for DS • Send CTS • Clear timer
Receive RRTS	State == IDLE/CONTEND_1	• Clear timer • State = WFCTS • Set timer for CTS

Table 4.3: MACAW event predicate action for Relay

data link layer what the length of the incoming packet is going to be, so that the receiver can read that correct amount of bytes into a buffer for later error checking and correcting. See figure 4.5 for the MAC layer frame structure, which we will now discuss.

The frame is divided into three sections, the preamble, control and CRC (Cyclic redundancy check) sections. The preamble prepares both the transmitting and receiving radios for the important control and CRC bytes to follow. The data slicer settle bytes is chosen as 10101010 to settle the data slicer in the middle. The same way that Manchester encoding is used to achieve a dc level. It also allows sufficient time for the half-duplex radio to switch between receive and transmit mode. The preamble is followed by the receive USART lock bytes, which triggers the USART to begin reading the bits that follows at the correct position to avoid missing the start-of-message bytes. A random noise pattern can produce the first start of message byte (01h), so a second byte (7Fh) is added to prevent the software from triggering. The two bytes are made complementary to each other to maintain the 50% mark to space ratio [24].

The control section contains all the bytes necessary to constitute a MAC packet. As mentioned before, the pktKind byte tells the receiver how many bytes to expect. The source and destination addresses follows, which are both MAC addresses. Note that since only one byte is used for this purpose, only $2^8 = 256$ nodes can be uniquely addressed. In all MAC packets the exchange sequence number denotes the current transaction taking place. The DATA-length field is to specify the length of a DATA packet if it is broken up into multiple packets which occurs when the DATA packet is larger than 216 bytes. The BO-value field is to share with other nodes the current back-off value at this node.

Event	Predicate	Action
Message not for me	State == any	• Set timer according to message received • State = QUIET
Timer times out	State == QUIET	• State = IDLE
Timer times out	State == QUIET, RTS received	• State = CONTEND_2 • Set back-off timer
Back-off timer times out	State == CONTEND_2	• Send RRTS • State = WFRTS_1 • Set timer for RTS
Timer times out	State == WFRTS_1	• State = IDLE
Receive RTS	State == WFRTS_1	• Clear timer • Set timer for DS • Send CTS • State = WFDS
POLL-flag set	State == IDLE	• State = CONTEND_3 • Set back-off timer
Back-off timer times out	State == CONTEND_3	• Send POLL • State = WFRTS_2 • Set timer for RTS
Timer times out	State == WFRTS_2	• State = IDLE
Receive RTS	State == WFRTS_2	• State= WFDS • Send CTS • Set timer for DS
Receive DS	State == WFDS	• State = WFDATA • Clear timer
Receive RTS	State == QUIET	• Set RTS-received -flag
POLL-timer times out	State == IDLE	• State = CONTEND_3 • Set back-off timer

Table 4.4: MACAW event predicate action for Relay continues

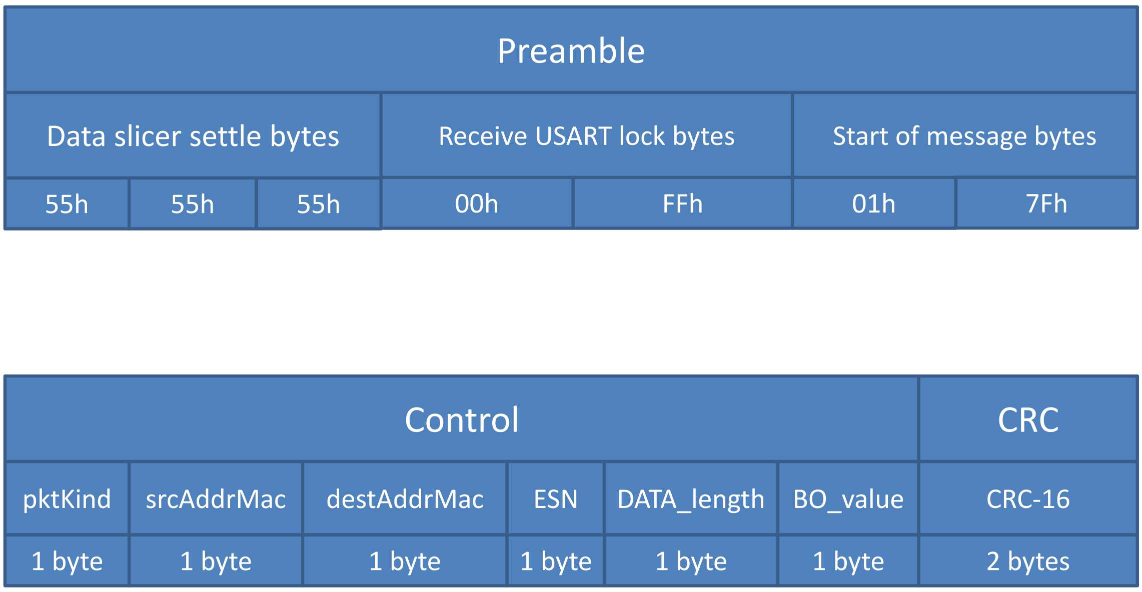

Figure 4.5: MAC Packet

Lastly a 16-bit CRC checksum is calculated on the six bytes of the control section and appended to the packet to be transmitted.

Data Integrity Cyclic redundancy check refers to a technique to check for the occurrence of errors in a transmitted message. It only checks for errors and does not correct them. A checksum is appended to the end of the message to be transmitted. The receiver can use this checksum to determine if errors have occurred and request for the message to be sent again [28]. The message bits are treated as polynomials with coefficients of either 0 or 1. The sender and receiver agree in advance on a generator polynomial. The generator polynomial is used to create codewords from the message bits. A properly designed generator polynomial ensures that codewords have good distance properties and are distributed evenly throughout the code space (see [17] for explanation on code distance properties). In general terms CRC generation is based on computing the remainder of dividing one polynomial by another. For the computation of an r-bit CRC checksum, a generator of degree r must be chosen. The sender should append r 0-bits to the end of the m-bit message. The resulting GF(2) polynomial is of degree m+r-1. This message polynomial is then divided modulo-2 by the generator polynomial to produce the remainder polynomial of degree r-1. The code-vector transmitted is then the m-bit message with the r-bit remainder polynomial appended. The receiver on receiving the data can then compute the checksum of the first m-bits received, the same way the sender did in using the agreed upon generator polynomial. If this computed checksum agrees to the last r-bits received, the transmission was correct [28]. CRC-16 in particular has the following characteristics: According to [27], it can detect

1. All single and double errors
2. All errors with odd-numbered bits
3. All burst errors of length 16 or less
4. 99.997 of all 17 bit errors
5. 99.998 of all errors greater than or equal to 18 bits

CRC-16 is calculated on the packet to determine if bit errors occurred. With MAC packets no forward error correction is done, the packet is only sent again by the transmitter on time-out if bit errors occurred, because the small size of the packet does not justify adding extra bytes for error correction. Flow control forms part of the implemented contention protocol.

4.3 Routing protocol description

The network layer implements the AODVjr protocol as discussed in chapter 2, which is a simplified version of the AODV protocol. This protocol deals with the end-to-end communication between a source and destination node. The main tasks of the routing protocol are to:

1. Find the best route between a source and destination node according to some metric
2. Avoid routing loops
3. Maintain this route
4. Handle link breaks

Discovering a route and avoiding route loops Figure 4.7 shows the operations of this protocol. When a route is required from node 1 to node 5 where the connection line shows which are in range of which, a RREQ packet is broadcast and relayed by all nodes on the path to the destination. Node 5 upon receiving the RREQ unicasts a RREP packet back to the originator of the RREQ. The time it takes from the sending of the RREQ to the receiving of the RREP is the route acquisition delay. Once that initial delay is over and a route is known to the destination, the source unicasts a DATA packet to the destination. The destination upon receiving the DATA packet sends an ACK packet back to confirm that it received the data. Each RREQ is uniquely identified by the parameter pair <source address, broadcast id>. Whenever the source node issues a new RREQ, the broadcast id is incremented. When a RREQ is received by an intermediate node, it increases the hop count and broadcasts the RREQ to its own neighbours. Because a node can receive multiple copies of the same RREQ packet, it's source address and broadcast id is checked against a table of already received messages and dropped if it matches one of the entries. In this way it avoids route loops. In the case of a node forwarding a RREQ, it still keeps track of some information of the message to be able to implement the reverse and forward path setups, to accompany the eventual RREP. This information being: destination network and MAC addresses, source network and MAC addresses and broadcast id.

Maintaining a route AODV-simplified maintains its routes by setting a route-life-time timer once the route is established. This timer is prevented from timing out by packets being received from the destination on the return path. That is RREP's and ACK's resets the timer. The route will remain active as long as the timer doesn't time out.

Handling link breaks Figure 4.8 shows what happens during a route break. When a link break occurs, no packets will arrive at the source node and the route-life-timer will eventually time out. This will delete the current route from the source node. When a route is still required, a new RREQ will be broadcast to set up a new route along a different path. The RREP will be unicast along the new path. A RREQ can be transmitted a maximum of three times if a route is needed, whereafter the network layer will assume that no route exists to the destination if no RREP is received. This mechanism is to avoid wasting bandwidth and energy. Another attempt at finding a route will only be carried out if new data messages arrive from a leopard collar.

Packet setup Figures 4.9a and 4.9b shows the network layer packets. The network control packet is 21 bytes long and the network data packet is 262 bytes long. It consists of a preamble section, control section and CRC section. The preamble which forms part of all packets leaving any node was discussed earlier. In the control section, the first 5 bytes is the MAC layer overhead discussed previously. The netwPktKind byte distinguishes network control packets from network data packets. Network control kinds is the RREQ, RREP and ACK. The srcAddrNetw and destAddrNetw is both network layer addresses and being 1 byte long, can also only address 256 nodes' network layers. The broadcastId is used with RREQ packets to uniquely identify each RREQ from a certain source node, such that route loops can be avoided by not forwarding RREQ's with old broadcastId's. The leopardId uniquely identifies from which collar a certain DATA message was received. The messageNum indicates the sequence of DATA messages. The pair leopardId and messageNum uniquely identifies a certain DATA message to the base station. Hopcount indicates how far a message travelled before arriving at the base station. Both the control and data packets is appended with a 16-bit CRC for error checking. Only the data messages has redundant forward error correction bytes to correct errors. The Read-Solomon error-correction code is used. This code is chosen because it provides for excellent correction of burst-errors. These errors occur due to heavy rain, lightning or other changes in the atmosphere. The specific Read-Solomon code used was designed to correct up to 13 errors. This maximum is used to provide the data with the best chance to arrive correctly at the next node. The data section is 216 bytes long and the data network packet is thus 85% efficient in terms of data ratio to overhead ratio.

Figure 4.6 shows the flow diagram for AODVjr. Once a message is passed from the data link layer to the network layer, the message is identified by checking the netwPktKind field. Valid message types are RREQ, RREP, LeopardDATA, ACKnetw and DATA.

Receiving Leopard DATA All data packets that arrive from a leopard collar is formatted into DATA packets and put in the network queue. If a route is not available to the destination (base station in this case) a RREQ message is flooded throughout the network in the hopes that it will reach the destination eventually after being relayed by intermediate nodes. A *RREP-timer* is set within which a RREP should return, otherwise another RREQ is sent. However, if a route exists in the *forward path table* the DATA message is sent and an *ACK-timer* is set within which an ACK should return. If the *ACK-timer* times out before an ACK is received the DATA packet is sent two more times before the network layer establishes that the network is too busy. If that happens, a *resend-timer* is set to try to resend the data packet in the future.

Receiving a RREP A RREP is a unicast type packet, therefore only the network layers of the intended intermediate nodes along the return path will receive it. If the network destination address of the packet matches this node's network address, then this node was the initiater of a RREQ. The *forward path table* is now updated with the MAC address of the packet for implementing a forward path to the base station. The route-life-timer is reset so that the route will remain active for a specified period. A RREP was received, so the *RREP-timer* can now be canceled such that another RREQ wont be sent again for the same route. All the messages in the network waiting to be transmitted to the base station can now be sent one at a time. The network layer implements a FIFO(first in first out) queue, so the packets that have been wating the longest in the queue are transmitted first.

Receiving a RREQ A RREQ is a broadcast type packet, so all nodes' network layers will receive it. Once it is received, its broadcast id is checked against a table to see whether it was received previously. If it was, it is immediately deleted. Otherwise the *already received table* is updated with this higher broadcast id. Now the *return path table* can be updated with the source MAC address of the packet for implementing the return path. If this node is the base station(network destination address matches node's) a RREP is sent along the return path, otherwise the RREQ is again broadcast.

Receiving DATA For each DATA packet that arrives at the base station a network level ACK is sent back to the originator of the DATA packet, such that the source node will know to delete the packet from its queue and send the next packet in queue. A DATA packet is uniquely identified by the <msgNum, leopardID> pair. So if a packet arrives that hasn't before it is stored on the base station's SD-card for downloading by a researcher onto the computer. If it was received before, this means that the source node never got the ACK for the previous packet, so an ACK is still sent back to the source, but the DATA packet gets deleted so no duplicates will exist.

Receiving an ACK If an ACK arrives at an intermediate node, it is simply reversed to the source of the DATA packet. If and ACK arrives at the source node, this means that the previous DATA packet got through and the next one can be sent to the MAC layer. The *ACK-timer* is cleared so the node wont try to resend the same data message. The DATA packet corresponding to the ACK packet's msgNum is now deleted from the source's network queue.

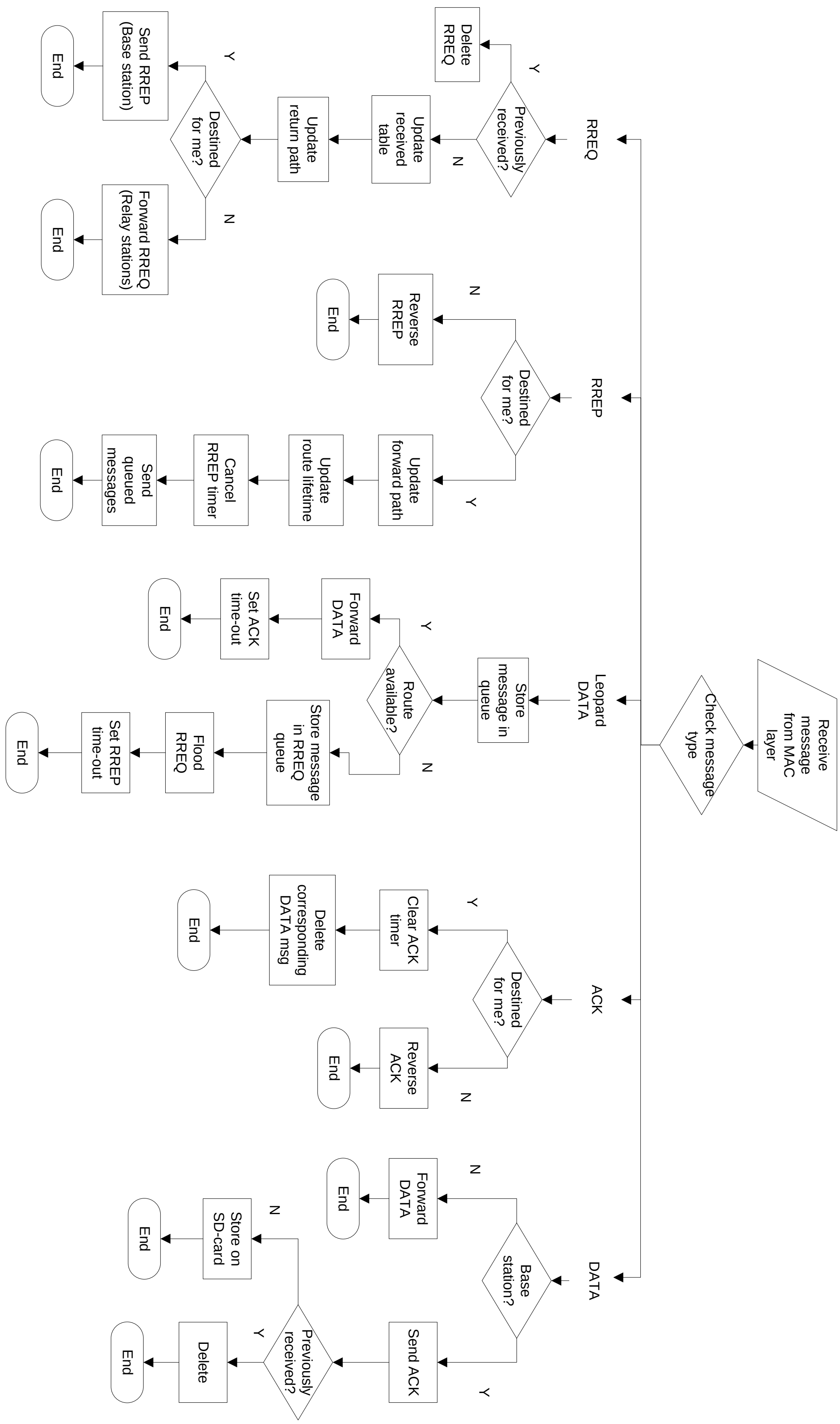

Figure 4.6: AODV

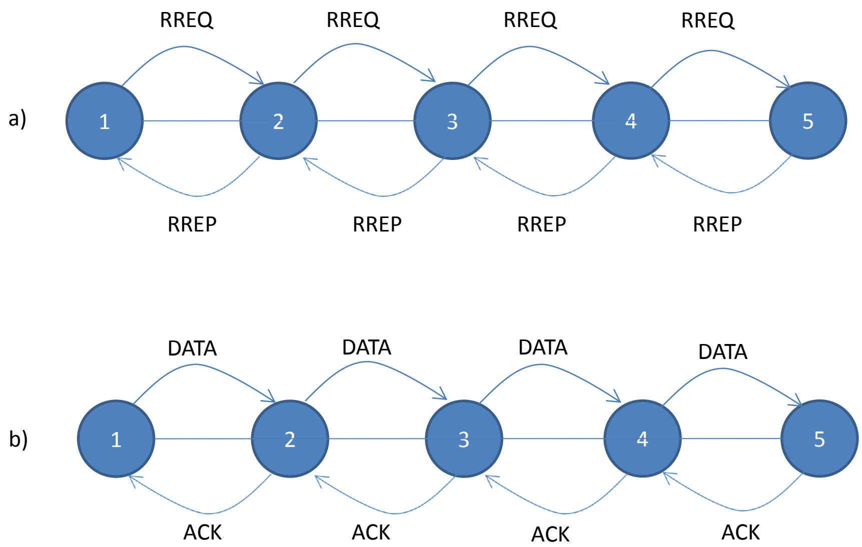

Figure 4.7: AODV operations

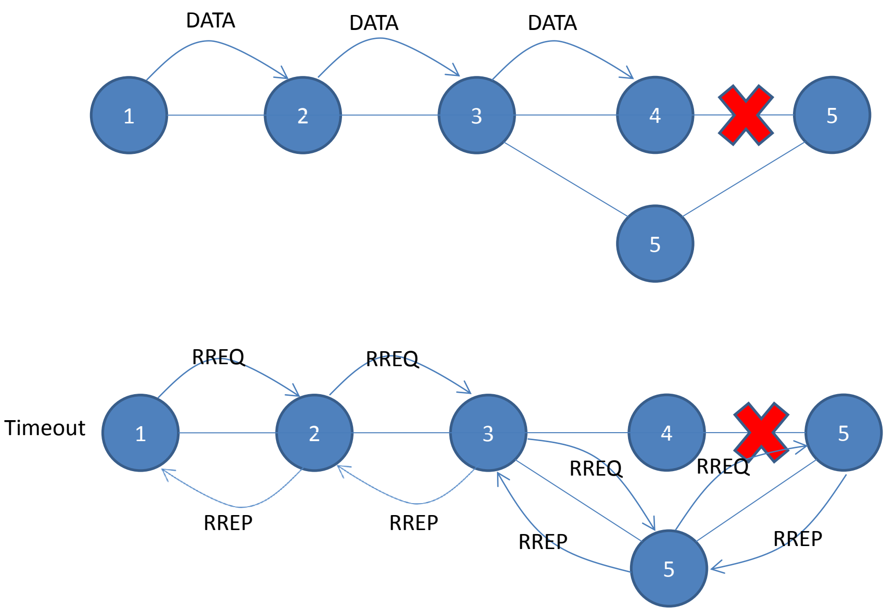

Figure 4.8: AODV route break

Preamble						
Data slicer settle bytes			Receive UART lock bytes		Start of message bytes	
55h	55h	55h	00h	FFh	01h	7Fh

Control						
pktKind	srcAddrMac	destAddrMac	ESN	DATA_length	netwPktKind	srcAddrNetw
1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte

Control					CRC
destAddrNetw	broadcastID	leopardID	msgNum	hopCount	CRC-16
1 byte	1 byte	1 byte	1 byte	1 byte	2 bytes

(a) Network control packet

Preamble						
Data slicer settle bytes			Receive UART lock bytes		Start of message bytes	
55h	55h	55h	00h	FFh	01h	7Fh

Control							
pktKind	srcAddrMac	destAddrMac	ESN	DATA_length	netwPktKind	srcAddrNetw	destAddrNetw
1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte

Control				CRC	DATA	FEC
broadcastID	leopardID	msgNum	hopCount	CRC-16	DATA	Read-Solomon
1 byte	1 byte	1 byte	1 byte	2 bytes	216 bytes	26 bytes

(b) Network data packet

Figure 4.9: Network packets

4.4 Summary

This chapter described the detail of the implemented medium access control protocol MACAW and the routing protocol AODVjr. In the next chapter we discuss the hardware design of a single node in our ad hoc network.

Chapter 5

Hardware Design

5.1 Introduction

Each wireless station consists of a few integrated hardware components which forms the basis of an intelligent node in this ad hoc network. First a high level design is done to determine the functional architecture, then a component selection in which different hardware components are considered to yield the best possible solution for the given design constraints. Thereafter follows the detail circuit design, cost summary and system verification of a single node.

5.2 System design

The operational architecture in figure 5.1 shows all units needed to form a working system. Each unit performs a specific task in the system, hence calling them functional units (FUs). The connections between units are the interfaces via which they communicate or interact. Only FU1 and FU4 are designed as part of this thesis. The other functional units are only drawn to show how FU1 and FU4 fit inside the system.

Functional unit 1 Figure 5.2 shows the building blocks of FU1.

FU1 is the base station which will reside at the researcher's house for downloading incoming data packets to a computer. This unit is dependent upon FU4 (relay station) for delivering data packets. FU1 and FU4 interface via radio frequency communication. This unit is controlled by FU1.5 (collar unit) which integrates all the surrounding units to form an intelligent node. FU1.1 (RF device) is the functional part which makes the interface between FU1 and FU4 possible. FU1.2 (secondary storage unit) is needed to store data packets temporally received from FU4 before they are downloaded onto a computer (FU2). This is made possible by FU1.4 (serial interface unit) which forms the interface between FU1 and FU2. FU1.3 (common clock unit) is needed for supplying the control units with a common time to time stamp data packets, which will be used in determining the end-to-end delay of packets as well as route acquisition times. FU1.6 (power supply unit) supplies FU1.1, FU1.2, FU1.3 and FU1.5 with power. FU1.8 (PCB) is the structural unit for mounting all units, while FU1.7 (casing) will fit all the other units inside it for protection against the weather elements.

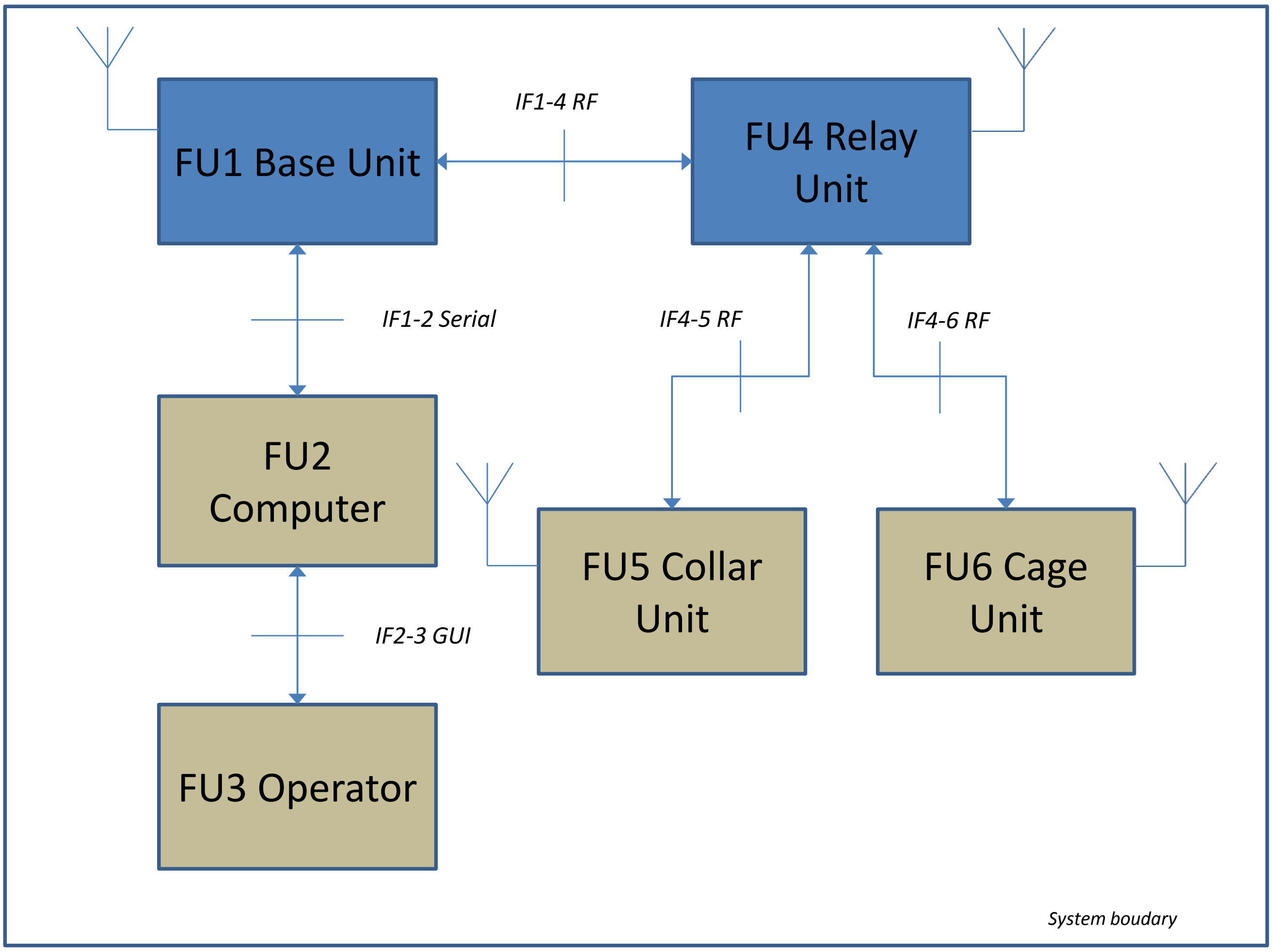

Figure 5.1: System architecture

Functional unit 2 This unit is a computer which interfaces to FU1 via a serial connection for downloading data to the computer's hard disk drive. The computer is loaded with GUI software for displaying the data.

Functional unit 3 This unit is the researcher who monitors the GUI for received data.

Functional unit 4 FU4 is the relay or milking unit, which polls a leopard collar(FU5) or a leopard cage(FU6) for data. Again these interfaces are radio frequency communication made possible by FU1.1 (RF device). FU4 differs from FU1 only by not implementing FU1.4 (serial interface unit) and thus not interfacing to a computer. These units will reside in the field and will deliver all their data to FU1, therefore obliterating the need for FU1.5. Figure 5.3 shows FU4's functional block diagram.

Functional unit 5 FU5 is the GPS collar fitted to a leopard for tracking the leopard's movements. This unit is designed by another student and outside the scope of this thesis.

Functional unit 6 FU6 is the camera monitoring unit residing at a leopard cage which takes photos of the captured animal and sends it to a relay unit (FU4). The design of this unit is also outside the scope of this thesis.

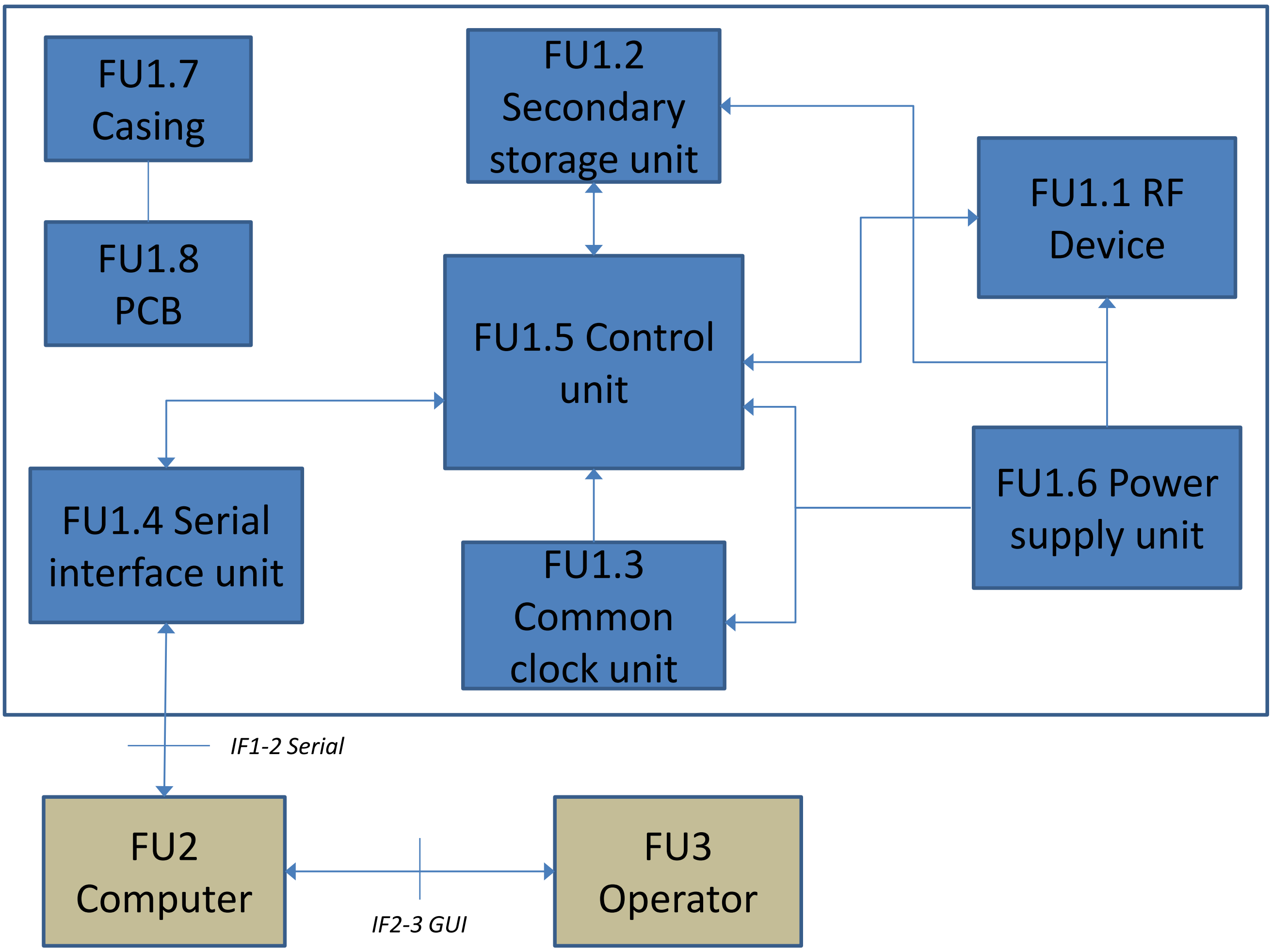

Figure 5.2: Functional unit 1 architecture

5.3 Component selection

In this section we will consider a few existing off the shelf components for each functional unit which yields the functionality as described above. We will consider a few choices on the market and evaluate each one in terms of suitability and cost where applicable.

5.3.1 FU1.1 RF Device

Most importantly the operating frequency has to fall within the ICASA specified range for wildlife telemetry tracking, the 148 to 152 MHz frequency band. Table 5.1 shows all the radios that were found on the market operating in this band. The communication range and the data rate has to be maximized while the power consumption should be minimized so that a smaller inexpensive power source can be used. Chapter 3 shows that a transmitter power of 500mW will deliver a feasible range, which means that compared to a 5W transmitter the power source can be sized 10 times smaller. This eliminates the YS-T86 device. A comparison between the 100mW output power devices (BiM1-151.3-10 and FMTR151R) shows that the BiM1-151.3-10 has a higher maximum data rate and cost less. The competition is now between the BiM1-151.3-10 and the BiM1H-151.3-10 devices. Both have the same maximum data rate, but with 7dB difference in transmit power and R190 price difference. A power source has to be sized 5 times greater for

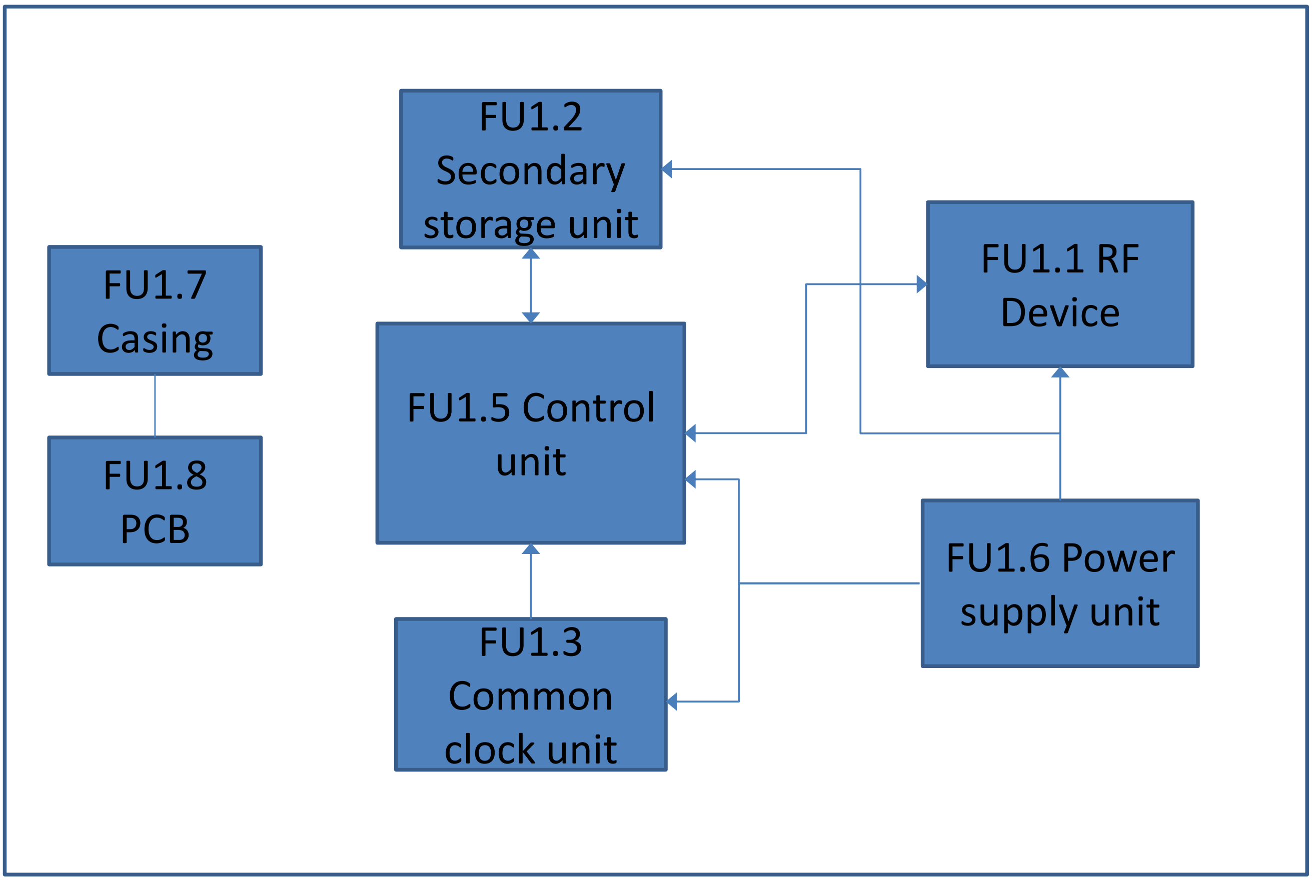

Figure 5.3: Functional unit 4 architecture

the 500mW transmitter. A network connection comparison between the 100mW and the 500mW devices is done in Radio Mobile. Figure 3.9 from chapter 3 shows a network with all units connected using six repeater nodes, whilst figure 5.4 shows that six of the cages are not connected to the network anymore. That is Bushmanskloof cage, Karukareb cage, Mannetjieskloof cage, Sneeuberg cage, Leeuvlak1 cage and Mount Ceder cage. This means that at least six extra repeater nodes will be needed, which will cost a lot more than the price difference between the two devices added to the price difference in battery sizes. Therefore the 500mW BiM1H-151.3-10 transceiver from Radiometrix is chosen.

Device	Manufacturer	Operating frequency	Maximum data rate	Transmit power	Price
BiM1h-151.3-10	Radiometrix	151.3MHz	10kbps	500mW	R 740.00
BiM1-151.3-10	Radiometrix	151.3MHz	10kbps	100mW	R 550.00
YS-T86	Shenzhen Yishi	150MHz	4.8kbps	5W	R 1 425.00
FMTR151R	Elsema	151.6MHz	4.8kbps	100mW	R 1 654.00

Table 5.1: Transceiver options

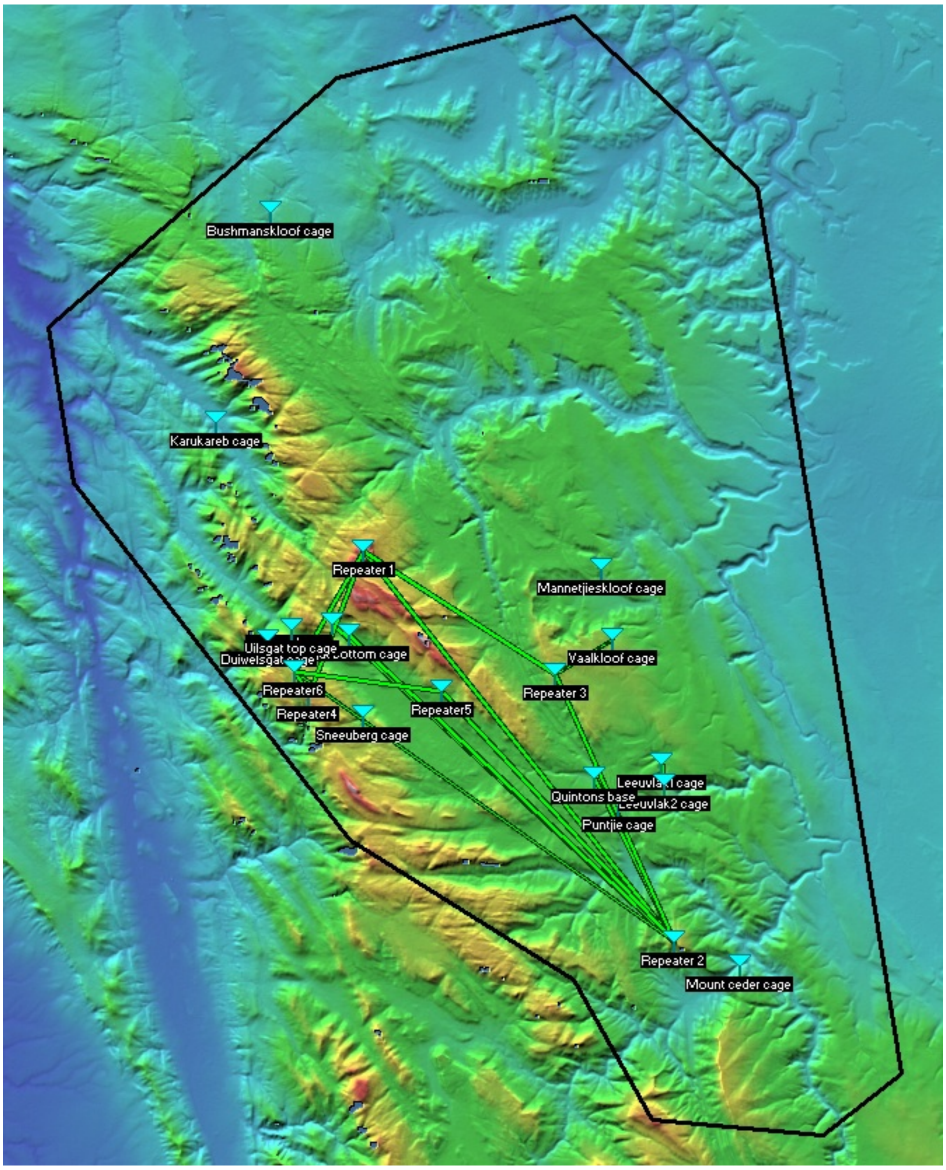

Figure 5.4: Link budget using 100mW transmitters

5.3.2 FU1.2 Secondary storage unit

The memory should be non-volatile and have a capacity to store at least 5000 data packets. This is only an estimate as no data exists to suggest how often a leopard visits the same location, in this case the location of a milking station. If leopards visit a milking station less often, more storage is required to download data packets before sending them to the base station, because more GPS data would have been obtained. To be safe, the biggest possible data storage unit should be used. This will become a data saver in the case that a node gets disconnected from the network due to a link break and data have to be obtained manually. This places another requirement on the data storage unit: it should be accessible by a computer in the field. The easiest way of achieving this is by removing the storage unit temporarily and inserting it into a computer for quick downloading of stored GPS info. This argument leads inevitable to a choice between a memory card and a hard disk drive. A hard disk drive consumes comparably much more energy than a memory card, so the the memory card is chosen. The issue of the maximum storage requirement is an issue related to the file system in use. The FAT-16 file system which will be used places a restriction of a maximum of 2GB on the storage unit. Knowing that a data packet consists of 216 bytes, 5000 data packets needs 1.08Mb of storage. A 2GB memory card however provides space for 9.2 million data packets to be stored, which means that virtually no data will ever be lost because it is assumed that a researcher will have downloaded the data long before the card became full. The secure digital card (SD-card) from San-Disk boasts the advantage over other brands that it uses less power, because it goes into sleep mode automatically when no reading or writing commands is issued in less than 5ms.

5.3.3 FU1.3 Common time unit

The end-to-end delay that a packet experiences in the network is determined by time stamping the packet when it is created at the source node and determining the difference between that time stamp and the current time at the destination node when it is received. For this delay to be accurately determined a common reference time is needed. The global positioning system provides a common time to all GPS receivers. In addition of having accurate common time, the position of each node will also be known so that researcher's can find them easily when they need to be moved. Another reason for using a GPS as both common time and positioning, is for the future implementation of location based-polling. This can save energy consumption in a collar, as a collar only needs to switch on when in the close proximity of a known milking station.

5.3.4 FU1.4 Serial interface unit

The most common serial interfaces found on modern computers are USB, RS-232 and Ethernet. RS-232 has long been the preferred interface for connecting embedded devices to a computer, because of its simplicity. RS-232 is being phased out, as most new computers (especially laptops) don't have external RS-232 ports anymore. Ethernet is a network port for connecting local area networks and it is common to find only one such port on a computer. USB is considered as thé interface to connect peripheral devices to a host controller (computer). Usually more than one such port is found on a computer and up to 127 devices can be connected to a single port, which makes it viable to connect yet another device to the computer and not interfere with other connectivity. Many microcontrollers have the USB specification already implemented, but that requires that the microcontroller also handle the USB stack and the implementation of USB in new designs can be time consuming. FTDI (Future technology devices international Ltd) provides a simple solution for connecting your embedded device to a host computer. The FT232R chip handles the USB stack and converts USART signals from the microcontroller to USB signals and visa versa. The USB port is then emulated as a com-port with an installed FTDI driver to ease the development of integrating a serial port into new computer software, since most computer languages implements a com-port driver. The USB specification also allows up to 500mA to be drawn from a single port by an external device. Using this power eliminates the need for an external power socket to power the embedded device. USB delivers 5V regulated power to the PCB, which will be used by the base station only.

5.3.5 FU1.5 Control unit

Knowing the peripherals which will be used in the design, we can specify the controller's tasks in coordinating these peripherals:

1. Send and receive data to and from the radio
2. Store and retrieve received data in non-volatile external memory
3. Swap data between non-volatile and volatile memory
4. Receive GPS and time info from the GPS module
5. Interact with a computer
6. Run MAC and network protocols
7. Manipulate timers

The charging and discharging of the battery will be handled by a separate charging chip, so no controller intervention is required. The Radio, GPS module and USB interface all need USART interfaces for communication. The SD-Card communicates via a master-slave configuration, thus one serial peripheral interface (SPI) port is needed. To free the microcontroller for protocol related tasks during data transfer between the SD-card and microcontroller's RAM, a direct memory access (DMA) controller is needed. The communication protocols will need a lot of RAM for temporary storage of incoming and outgoing packets, routing tables, queues, machine states, FEC coding etc. Therefore the microcontroller with the largest amount of RAM within a family of controllers should be used. If RAM still proves insufficient in the development stadium, primary-secondary memory exchange can be done, but is not desirable due to speed differences. Six 16-bit timers in total is needed in the operation of the MAC and Network layers. From the above list of microcontroller tasks, the following definite features will be required in the chosen microcontroller:

1. Three USART modules for interfacing with the radio, GPS module and USB chip
2. One SPI module for interfacing with the SD-card
3. A DMA controller for data transfer
4. Sufficient RAM
5. Six timers for driving protocol events

Other considerations in selecting the correct microcontroller lies in the operating voltage, in order that the maximum number of chosen peripherals can be interfaced without the need for voltage level translators.

Table 5.2 shows microcontrollers from each of the existing XMEGA families. Note that the last letter and numeral denotes a family of microcontrollers. Each microcontroller chosen is the top of its family because of its amount of RAM being the largest.

The ATxmega32D4 and ATxmega256D3 are disqualified on the basis of having no DMA controllers. The ATxmega128A4 is disqualified on the basis of having only 5 timers. The ATxmega256A3 and the ATxmega384A1 remain and both these microcontrollers meet the minimum requirements, with the ATxmega384A1 having double the RAM of the

Device	RAM	USART	SPI	DMA	Timers	Operating voltage	Package	Price
ATxmega384A1	32	8	4	Yes	8	3.3V	TQFP100	R 73.00
ATxmega256A3	16	7	3	Yes	7	3.3V	TQFP64	R 97.00
ATxmega128A4	8	5	2	Yes	5	3.3V	TQFP44	R 46.00
ATxMega256D3	16	3	2	No	5	3.3V	TQFP64	R 77.00
ATxmega32D4	4	2	2	No	4	3.3V	TQFP44	R 38.00

Table 5.2: Microcontroller options

ATxmega256A3. The ATxmega384A1 costs R24 less, but will require a bigger footprint and more solder work due to its 100 pin package size as compared to the 64 pin package size of the ATxmega256A3. The ATxmega384A1 was also not available for purchase in South Africa, therefore we have chosen the slightly more expensive ATxmega256A3.

5.3.6 FU1.6 Power supply unit

As mentioned before, the nodes will reside in the field in secluded areas, therefore a power source has to be used that can be replenished. With the Cederberg being in sunny South-Africa, solar energy is a viable option. [15] describes the most difficult part in sizing a system as anticipating the end-user load, which drives solar energy system design.

Table 5.3 lists the power requirements of the major components in the system. Note that the GPS module and microcontroller will always be switched on, but that the radio and SD-card will be switched on intermittently. Therefore we calculate the power requirements of each component in terms of Watts per day, which will depend on how many hours of the day the device is switched on.

The radio will reside in receive mode for the whole day, except for when data and poll packets need to be sent. This will depend on the arrival rate of leopards. The arrival rate is unknown, but we assume the radio will be in receive mode 20 hours per day and in transmit mode for 4 hours per day. The SD-card will only store information when it receives data, we assume its operation time to be 4 hours of the day.

Load estimation From table 5.3 the following can be calculated.

The radio's energy consumption per day:

$$E_{transmitter} = 1450mW \times 4hours = 5.8Wh \tag{5.3.1}$$

$$E_{receiver} = 40mW \times 20hours = 0.8Wh \tag{5.3.2}$$

$$E_{radio} = E_{transmitter} + E_{receiver} = 6.6Wh \tag{5.3.3}$$

The SD-card's power consumption per day:

$$E_{sd} = 330mW \times 4hours = 1.32Wh \tag{5.3.4}$$

The GPS module's power consumption per day:

$$E_{gps} = 180mW \times 24hours = 4.32Wh \tag{5.3.5}$$

Component	Current consumption (mA)	Rated voltage (V)	Resultant power (mW)
Radio transmitter	290	5	1450
Radio receiver	8	5	40
SD Card	100	3.3	330
GPS module	36	5	180
Microcontroller	14	3.3	46.2

Table 5.3: Component power consumption

Component	Input voltage (V)	Output voltage (V)	Efficiency (%)
Solar charging IC	20	6.9	83
3.3V Regulator	6.5	3.3	51
5V Regulator	6.5	5	77

Table 5.4: Regulator efficiencies

The microcontroller's energy consumption per day:

$$E_{uC} = 46.2mW \times 24hours = 1.1Wh \tag{5.3.6}$$

The regulators also dissipate a considerable amount of the total energy. Table 5.4 gives the efficiencies of these components. The microcontroller and SD-card receive energy from the 3.3V regulator and the radio and GPS module receive energy from the 5V regulator. All of the energy flows through the solar charger IC. This means that the energy dissipated by the 3.3V regulator is the voltage drop times the total current flowing through it.

The energy dissipated by the 5V regulator is the sum of the power consumptions of the GPS module and the Radio times the voltage drop across the regulator.

$$E_{5V} = (6.5 - 3.3) \times ((290 \times 4) + (8 \times 20) + (36 \times 24)) = 3.28Wh \tag{5.3.7}$$

The power dissipated by the 3.3V regulator is:

$$E_{3.3V} = (6.5 - 3.3) \times ((100 \times 4) + (14 \times 24)) = 2.36Wh \quad (5.3.8)$$

The total energy dissipated by all of the on-board components is thus:

$$E_{subtotal} = E_{radio} + E_{sd} + E_{gps} + E_{uC} + E_{5V} + E_{3.3V} = 18.98Wh \quad (5.3.9)$$

Because the solar charger IC is a switched regulator and not a linear regulator, its energy dissipation is given in terms of efficiency. The efficiency of the solar charger IC is 83 %, which means that it will dissipate 17 % of the total energy itself. Thus it dissipates:

$$E = 0.17 \times 18.98 = 3.23Wh \quad (5.3.10)$$

The total system energy requirement for one day is:

$$E_{total} = E_{subtotal}/0.83 = 22.87Wh \quad (5.3.11)$$

Now that the load is known, it is possible to determine the size of the power source. [15] gives the following approximations to estimate the electrical energy expected from a solar panel:

- The real capacity of a panel is 15% less than the nominal rating, due to rising temperatures. The effective capacity being 85% of the nominal capacity.
- The expected electrical energy depends on the insolation (peak sun hours) and season, since insolation levels differs from month to month.
- Energy production can be increased by up to 25% if using a sun tracker.

[3] gives the average sun hours for the Western Cape for July(worst) and January(best) as 6.4 hours and 11.3 hours per day. The total number of rainy days during July is 12. Thus it rains roughly a third of the month. We should size the battery supply to last for 3 consecutive days.

Thus, the critical design month is July with the least amount of sun hours(6.4). The battery should be designed for 3 day's autonomy, not exceeding 50% depth of discharge and with a round-trip derating efficiency of 75%. The load is 22.2Wh.

Battery storage requirement Total daily load Ah requirement = daily energy Watt-hours/battery nominal voltage = 22.87Wh/6V = 3.8Ah

Required battery capacity = (days of autonomy * daily load Ampere-hours) = 11.44Ah

But, in order to prolong the life expectancy of the battery, its full charge should not be used between charging cycles. Fig 5.5 shows that for a battery life of 480 cycles or 1.3 years, the battery should only be discharged down to 50% of its capacity. Another consideration is the derating for round-trip efficiency (battery efficiency), which will be taken as 75%.

Thus, the required battery capacity = (days of autonomy * daily load Ampere-hours)/(derating for round-trip efficiency * depth of discharge) = $30.49Ah \approx 30Ah$

Average daily depth of discharge = (total daily load Ampere-hours)/(total battery capacity) = 3.8Ah / 29.6Ah = 12.8%

Because discharge down to 50% will only happen during the winter months, the life expectancy will be much better than 1.3 years. From 5.5, it will be more than 1200 cycles, which is more than 3.3years.

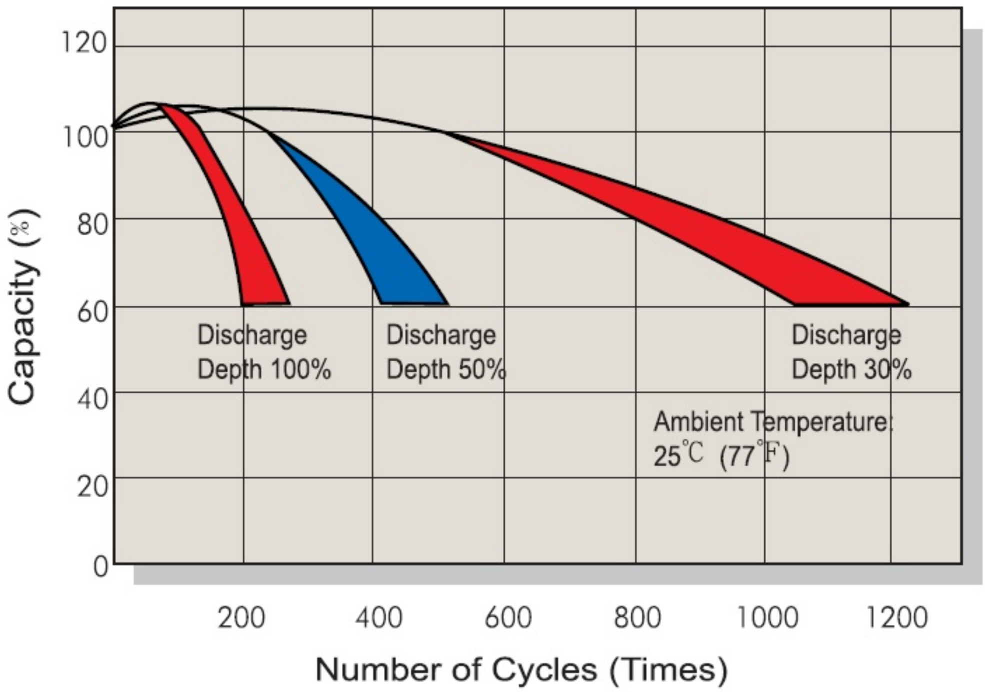

Figure 5.5: Depth of discharge vs life expectancy

Solar panel size estimation We will take the solar panel system efficiency as 50%, in accordance with what [15] estimated. The solar panel size is then: total energy required/(peak sun hours * system efficiency) = 22.87Wh /(6.4 * 50%) = 7.15Wh

The difference in insolation levels from Summer to Winter differs. The winter insolation levels are only 40% of the maximum (during Summer). Thus the solar panel energy requirement should be : 7.15Wh/40% = 17.9Wh ≈ 20Wh

System summary

- Total Watt-hour requirement: 22.87Wh
- Solar panel size: 20Wh
- Nominal battery voltage: 6V
- Battery capacity: 30Ah
- Battery type: SLA deep cycle
- Autonomy: 3 days
- Average daily depth of discharge 12.8%
- Battery life time: More than 3.3 years

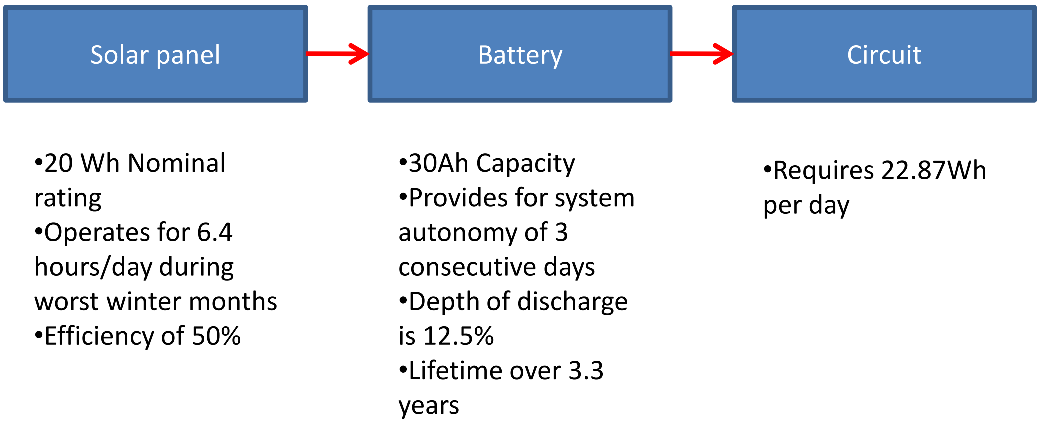

Figure 5.6: Solar energy system sizing

5.3.7 FU1.7 Casing

The casing protecting the sensitive electronics inside should have an IP rating of 54. The IP rating or International Protection Rating specifies an enclosure's ability to withstand solids and liquids in differing degrees. The first numeral indicates the protection that the enclosure provides against solid objects like tools, wires, fingers, dust etc. To ensure the continuous operation of a node in the field, the electronics must be protected against contact with foreign objects and an excess of dust that disrupts the satisfactory operation of a node. The numeral for this degree of protection is 5, whilst 4 only protects against object sizes of greater than 1mm. The numeral 6 indicates a dust tight enclosure. The second numeral specifies the protection against varying degrees of water contact ranging from dripping water to immersion beyond 1m. We only need protection against rain, so the rating of 4 is chosen, which is defined as protection against splashing water from any direction. The enclosure should be see-through. To be able to check the status of the node without opening the casing by viewing the status LED's, the see-through enclosure from Hammond Manufacturing is chosen with its IP rating of 54.

5.3.8 FU1.8 PCB

The printed circuit board's characteristics to be defined are:

1. Material
2. Number of layers
3. Copper thickness

The standard material used is FR4 with a thickness of 1.6mm.

The number of PCB layers depends on the complexity of the track routing and the board space restrictions. Another factor to consider is the necessity of a ground and power plane. In this design there is no space restrictions as the finished unit will reside in the field with plenty of space. Thus the minimum number of layers can be used as all track routing can be done on a single layer to take up as much space as required. The advantage of using less layers is the reduction in cost. The manufacturing cost increases incrementally with increase in layers. A dedicated ground plane is needed since a component operating at radio frequency is part of the design. Thus a two layer board will be used with the top layer the routing and component layer, and the bottom layer the ground layer.

The copper thickness depends on the magnitude of the maximum current a track with a specified width has to carry and the resistance of a certain length of this track. This is determined by the power requirements of the design since this is where the highest currents flow. The single solar panel allows a maximum current of 1.2A, although the LT3652 solar charger IC allows a maximum current of 2A. We choose to use the maximum current of 2A so that future use of this PCB will not be restricted by the track width. The footprint of the LT3652 IC has a maximum width of 0.42mm per leg. The PCB track width calculator from [4] determines that for a 2A current and 35um copper thickness, the track width has to be 0.781mm. This is larger than what the footprint allows. Using the next copper thickness of 70um gives a track width of 0.391mm which is under the maximum allowable footprint width. The 70um copper thickness of the PCB yields a resistance of 0.008Ω per 1 cm, which is an order of 10 smaller than the smallest resistor used (current sense resistor) and will have negligible effect.

To summarize: A double sided FR4 PCB with 70um copper thickness is used for manufacturing.

5.4 Circuit design

Figure 5.7 shows the block diagram for a base station and relay node derived from the system level design (and components selection from the previous sections). Communication interfaces between components are also shown. Using this we will discuss the design of the circuit that connects all components in the diagram.

5.4.1 Solar circuit

The LM3652 solar battery charger chip from Linear Technology forms the heart of this circuit. The chip is specifically designed to regulate the current/voltage relationship of the input from the solar panel to tap the optimal power performance from the solar panel. Connectors P8 and P9 on the right and left of figure 5.8 connects the solar panel and battery respectively. Connecter P10 disconnects the power drain from the power source temporarily to ascertain the correct voltage output in order to avoid damaging the PCB. This is also used as a point to measure the total current drawn from the drain circuit. The resistors, capacitors and inductor on either side of the LM3652 chip is carefully selected to yield the correct input voltage, output voltage, maximum current drain and maximum ripple current allowed. The chosen solar panel operates at 16.8V giving the input voltage to the circuit. The chosen battery has a nominal voltage of 6V. The battery can be either float or fast charged. With fast charging the voltage across the poles of the battery is set higher in comparison with float charging in order to rush more current into the battery in a shorter amount of time. Continuously fast charging a lead-acid battery shortens its life time, while the battery can operate an indeterminate length of time using float charging. The recommended voltage per cell for float charging is 2.3volts. Thus for the three cell

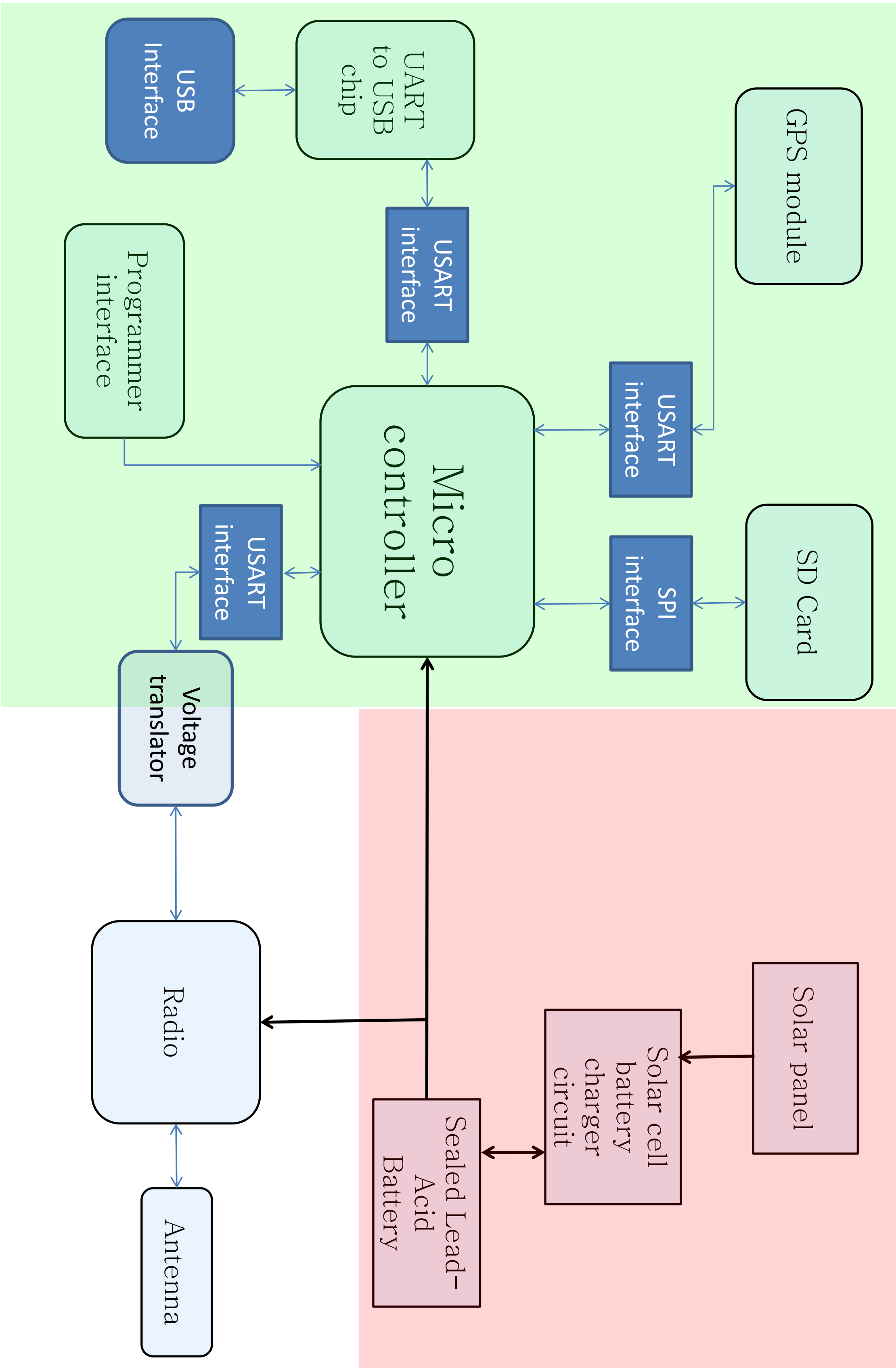

Figure 5.7: Hardware block diagram

battery the output voltage from the circuit is 6.9V. LED's D9 and D10 indicates the current state of the charging circuit. D9 will light green when a battery is connected and charging. D10 will light red when some voltage fault occurred.

The values of the components surrounding the LT3652 is now determined from equations given in the data-sheet [7]. The following parameters are used:

- Battery float charging voltage: 6.8V
- Solar panel output voltage: 16.8V
- Solar panel maximum charge current: 1.2A

Input supply The input capacitor C_{in} has the function of minimizing voltage glitches on V_{in} and reducing ripple current in the charger. A ripple voltage ΔV of 0.1V is recommended by the data-sheet.

$$C_{in} = I_{chg(max)} \times (V_{bat}/V_{in}) \div \Delta V_{in} \tag{5.4.1}$$

$$= (1.2 \times (6.8 \div 16.8)) \div 0.1 = 4.85uF$$

We choose a standard capacitor value of 10uF, yielding an even smaller ripple voltage.

Charge current programming Programming the maximum charge current is done through a very small valued resistor called a current sense resistor.

$$R_{sense} = 0.1 \div I_{chg(max)} \tag{5.4.2}$$

$$= 0.1 \div 1.2 = 0.083\Omega$$

A standard 0.082Ω current sense resistor is chosen.

Inductor selection The criterion for selecting the inductor depends on the maximum ripple current created in that inductor. The ripple current is typically set to 25% of the maximum charge current. Thus $\Delta I_{ripple} = 0.3A$

$$L = (10 \times R_{sense}/\Delta I_{ripple}) \times V_{bat} \times (1 - (V_{bat}/V_{in})) \tag{5.4.3}$$

$$= (10 \times 0.082 \div 0.3) \times 6.9 \times (1 - (6.9 \div 16.8)) = 11.1uH$$

We chose the standard 22uH which yields even smaller ripple current. Another important selection criterion for and inductor is the saturation current which should be equal to or exceeding the maximum current in the inductor.

$$I_{saturation} \geq (1 + \Delta I_{ripple}/2) \times I_{chg(max)} \tag{5.4.4}$$

$$\geq (1 + 0.3 \div 2) \times 1.2 \geq 1.38A$$

Rectifier diode selection The rectifier diode has to meet forward voltage drop, reverse voltage and maximum current specifications.

The maximum reverse voltage of the diode has to be greater than the maximum output voltage of the solar panel of 20.5V. The forward voltage drop has to be as small as possible, to yield the lowest power loss and thus the greatest efficiency. The maximum current is determined as:

$$I_{diode(max)} > I_{chg(max) \times ((V_{in(max)} - 0.7 \times V_{bat})/V_{in})} \tag{5.4.5}$$

$$> 1.2 \times ((20.5 - 0.7 \times 6.9) \div 20.5) > 0.92A$$

The MBRS340 schottkey diode meets these criteria.

Battery float voltage programming The float voltage programming is done by a simple resistor divider circuit. The two equations used to determine the two resistor values are:

$$R_1 = (V_{bat} \times 2.5 \times 10^5)/3.3 \tag{5.4.6}$$

$$R_2 = (R_1 \times (2.5 \times 10^5))/(R_1 - 2.5 \times 10^5) \tag{5.4.7}$$

$R_1 = 6.9 \times 2.5 \times 10^5 \div 3.3 = 522.7k\Omega$ Choose R_1 to be $530k\Omega$ so that the value can be approximated by a $510k\Omega$ and a $20k\Omega$ in series.

$R_2 = (530k \times 2.5 \times 10^5) \div (530k - 2.5 \times 10^5) = 473.2k\Omega$ which can be approximated by a $470k\Omega$ and a $3k\Omega$ resistor in series. The tolerance on the resistor values is 0.1%, so the float voltage should be reasonably accurate.

The output voltage now yields 7V, which is a bit higher, but still under the battery manufacturer's specification for cycle charging (7.2V).

Input supply voltage programming The input voltage is also programmed by a resistor divider network. This is done so that the input voltage regulation loop has a reference for the voltage used to drive the circuit for the optimal performance of the solar panel by regulating the voltage/current characteristic. We choose R_{in2} to be $100k\Omega$ and determine R_{in1}.

$$R_{in1} = ((V_{in} - V_{forward(D1)-2.74}) \times R_{in2})/2.74 \tag{5.4.8}$$

$$R_{in1} = (16.8 - 0.5 - 2.74) \times 100k \div 2.74 = 494.9k\Omega$$

5.4.2 Power circuit

Linear regulators Reg113-5 and Reg113-3.3 from Texas Instruments respectively source the 5V and 3.3V components on the PCB. Both regulators include capacitors ranging from 1000uF to 10nF to filter out low and high frequency components from the solar charging circuit, since the charging circuit uses a switching regulator and thus adds ripple to the power rail. The 1000uF also serves as a power reservoir in case the peak power drawn from the PCB spikes, such that the voltage will not drop, but current can be drawn from this capacitor. Header P1 allow manual switching of power source between the 6V from the battery or the 5V from the USB port. This is so that a single PCB design could be used for both the base station and the relay stations.

5.4.3 Transceiver interface

Figure 5.10 shows the radio with antenna connection and data connections to the micro-controller. The antenna connection is an SMA screw connector, connected from the radio RF pin to the SMA connector by a 50Ω microstrip line to match the 50Ω impedance antenna. The width of this strip line was calculated knowing the copper thickness on the PCB to be $70\mu m$ and distance between the strip line and ground plane as dictated by the thickness of the PCB insulator material as 1.6mm. The relative permittivity of the FR4 material is 4.9. The calculation was done with the web-base calculator from [22] and the width was calculated to be 2.74mm. There is however only space for a 2.4mm microstrip line between the pins of the radio. This yields a 54.4Ω characteristic impedance on the microstrip line, which will have some reflections.

The radio's power rail has a series ferrite bead, which is a magnetic device that attenuates all frequencies in the MHz range by dissipating them acting as a 30Ω resistor. This stops spurious frequencies on the power rail from introducing interfering noise to the radio.

The radio and micro-controller work at different logic levels. To interface the two, a voltage level translator is introduced to switch signals from 3.3V to 5V. This is however only done on the transmitting side, as the receiving side of the radio outputs 2.5V signals directly to the microcontroller, which is still above the minimum level recognizable by the micro-controller. A line filter is also put on the transmitting line from the micro-controller to the radio to reduce switching noise. Small sized capacitors is put on all components' power lines to reduce the effect of a sudden voltage drop.

5.4.4 Programmer interface

The programmer uses the universal JTAG interface to program the microcontroller. This interface uses 5 communication lines, power and ground lines. The 5 communication lines are data-in, data-out, clock, mode select and reset.

5.4.5 Serial interface

The FT232RL chip from FTDI converts USART signals from the microcontroller into USB signals and back for communication between a computer and the microcontroller. LED D4 and D5 respectively signals a transmit and receive event. The external power switch cuts power to the PCB when the computer goes into sleep mode to comply with the USB specification of not drawing more than $500\mu A$ from the port. Header P2 can be manually switched such that the PCB draws power from either the USB port or the 5V regulator coming from the battery, depending on whether the PCB is used as a base station or relay station. The ferrite bead on the USB port's power line dissipates unwanted high frequency noise.

5.4.6 GPS interface

The GPS module can communicate by either RS232 or TTL signals. For conveniently interfacing directly to the microcontroller's USART port, the 3.3V TTL interface is used. The GPS module inputs 5V power, but has an on-board 3.3V regulator for the TTL signals to and from the microcontroller.

5.4.7 SD-card interface

The SD-card communicates via the microcontroller's SPI port, which uses four lines. A chip select(CS) for activating the SD-card. A Clock signal and two data lines: master-in-slave-out(MISO) for communication from the SD-card to the microcontroller and master-out-slave-in(MOSI) for communication from the microcontroller to the SD-card. The $50k\Omega$ resistors connected between these lines and the 3.3V power rail, ensures that the lines don't float when inactive and thus don't consume unnecessary power.

5.4.8 Microcontroller circuit

The microcontroller is at the heart of the PCB, coordinating the operation of all the peripheral modules. All communication connections are made to and from the microcontroller. The reset circuit, consisting of a switch and a resistor, draws the microcontroller's external reset line to ground, to signal a reset event. LED's D1 and D1 signals transmit and receive events for the radio. An external crystal is connected as clock source clocking at 7.3728MHz. This frequency is specifically chosen so that the USART module on the microcontroller can accurately operate at the standard baud rates by dividing the crystal frequency without a remainder. 100nF capacitors is placed on all the power to ground connections to keep the power rail always high at 3.3V.

5.4.9 PCB layout

The most important consideration for the layout is to keep the fast switching digital devices and power circuits far away from the analog radio. This is done to minimize interference on the radio channel. Digital logic ground currents can also interfere with analog circuitry, therefore the two different currents should be isolated. One approach is to split the ground plane of the analog part and the digital part and only connect it at one point, since a common reference is still needed. However, this causes problems when routing traces over the split in the plane. This will mean that the return digital current will still have to flow through an analog ground plane or visa versa. Digital ground currents, which is usually high frequency, want to return directly underneath the signal trace and therefore have no desire to flow through analog portions of the ground plane [23]. It is important to separate the analog and digital sections and keep in mind where return currents flow.

5.5 Cost

Table 5.5 shows the total cost of one stand-alone wireless station. The costly single components are the radio, battery, solar panel, microcontroller, GPS-module, SD-Card and PCB.

5.6 System verification

The system consists of five mayor functional blocks. That is the radio communication, computer communication, GPS communication, SD-card storage and power supply. The following paragraphs describes the verification tests that was performed on each block.

Component	Description	Price
Radio Transceiver	BiM1H-151.3-10	R 741.00
Antenna	ZARA-130	R 340.00
Antenna mount	Dropper	R 100.00
Antenna connectors	Male and female	R 35.00
Microcontroller	XMEGA-256-A3	R 200.00
Battery	Sealed Lead Acid 6V 12Ah	R 110.00
Solar panel	20 Watt	R 640.00
Solar battery charger chip	LT3652	R 53.00
USART to USB chip	FT232RL	R 36.00
USB Connector	mini B	R 8.00
GPS Module	LEA-4P-SMART	R 375.00
SD-Card	San Disk 2Gb	R 115.00
SD- Card Connector	Standard type	R 25.00
Voltage level translator	TXS0104	R 10.00
Linear Regulator 5V	REG113EA-5	R 32.00
Linear Regulator 3.3V	REG113EA-3.3	R 32.00
Crystal Oscillator	7.3728MHz	R 5.00
T-Filter	surface mount	R 10.00
p-channel mosfet	IRLML6401	R 3.00
Power Inductor	2A	R 12.00
Push-button	surface mount	R 4.00
Miscellaneous	Diodes, LED's, resistors, capacitors, connectors	R 500.00
PCB Manufacturing	Double sided, FR4, 70um	R 572.00
Enclosure	See through IP54 rating	R 90.00
	Total:	R 4,048.00

Table 5.5: Total cost of one station

Radio Communication We verify the following for radio communication:

1. Operating frequency
2. Transmit power
3. Data rate
4. Two-way communication

The carrier frequency was verified to be 151.3MHz by means of a spectrum analyzer. It requires the RF pin of the radio to be connected through an attenuator to avoid exceeding the spectrum analyzer's maximum input power. The radio was transmitting 1's and 0's interchangeably. The spectrum analyzer showed two maxima on either side of the carrier frequency, representing the two frequencies used to modulate 1's and 0's. 151.3MHz was the middle frequency.

If the transmit power is lower than rated or there is too much reflection in the connectors and antenna, the expected range will be decreased. As shown in chapter 6, a radio range test was done in the Cederberg and yielded a maximum distance of 12.42km. This is in accordance with the data sheet, stating that a radio link of more than 10km can be established.

The maximum data rate possible with a bit error rate of one in a million should be 10 kbits/s. This was tested by the micro-controller clocking out data packets to the Radio-USART port at 10 000 baud. 100 % of 200, 64-bit packets was received correctly with the two antennas 20 meters apart.

Verification of two-way communication is the same as the data rate test, only this time the receiver was made to transmit and the transmitter to receive.

Computer communication The PCB was connected to the computer through a USB cable. A set of characters was sent through the USART connected to the USART to USB chip. All characters was received correctly by inspection through hyper-terminal.

GPS communication Time information was verified against a watch and GPS information against a Garmin GPS handheld device.

SD-Card Storage Text files with known data was stored by the microcontroller on the SD-card which implements a FAT-16 file system. The SD-Card was removed and read on a computer running Windows. All data was read correctly. Text files were again stored by the computer on the SD-card. The microcontroller read the files and sent it through the USB interface to the computer's hyperterminal to be verified correctly.

Power We verify the following aspects of the power module:

1. Charge voltage
2. Charge current
3. Regulator voltages

The solar battery charger circuit was designed to charge a battery at 6.8V with a charging current of 1.2A. Both these values were obtained correctly with a multimeter. The 5V and 3V regulators should of course deliver that respective voltages, which it did.

5.7 Summary

This chapter described the system level design of both a base station and relay stations for use in the leopard tracking project. Each block of the system design was discussed in terms of its functional use. The selection of hardware components was discussed with the following results: the BiM1H-151.3-10 transceiver from Radiometrix was chosen as RF communication unit, the 2GB SD-card from San-Disk was chosen as secondary storage unit, the LEA-4P GPS module from RFDesign was chosen as both the common clock unit and positioning unit, the FT232R chip from FTDI was chosen as computer serial interface unit for the base station, the ATxmega256A3 from Atmel was chosen as control unit, the LT3652 chip from Linear Technology was chosen as the solar battery charger for the relay stations and see-through enclosures was chosen from Hammond Manufacturing for all stations. Detailed calculations showed the power supply sizing design for a relay station using a solar panel and SLA battery. All units was verified to work correctly. The total cost of one stand-alone station was calculated to be R4048.

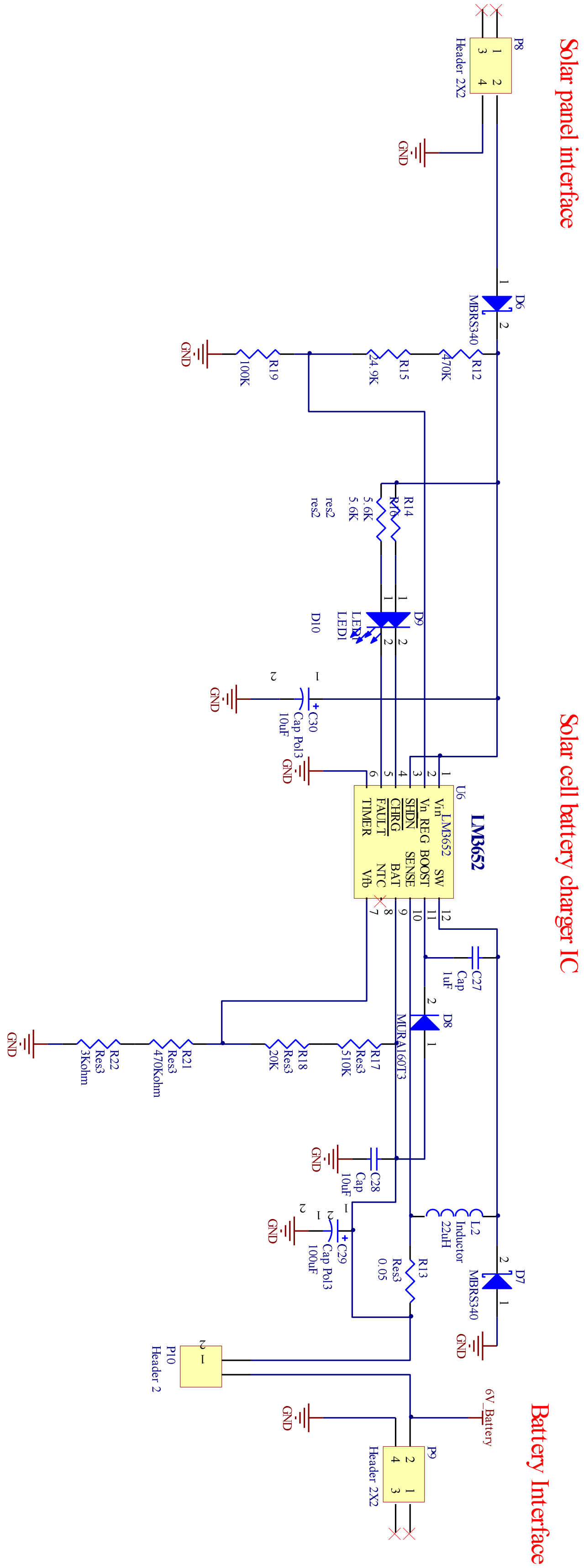

Figure 5.8: Solar battery charger circuit

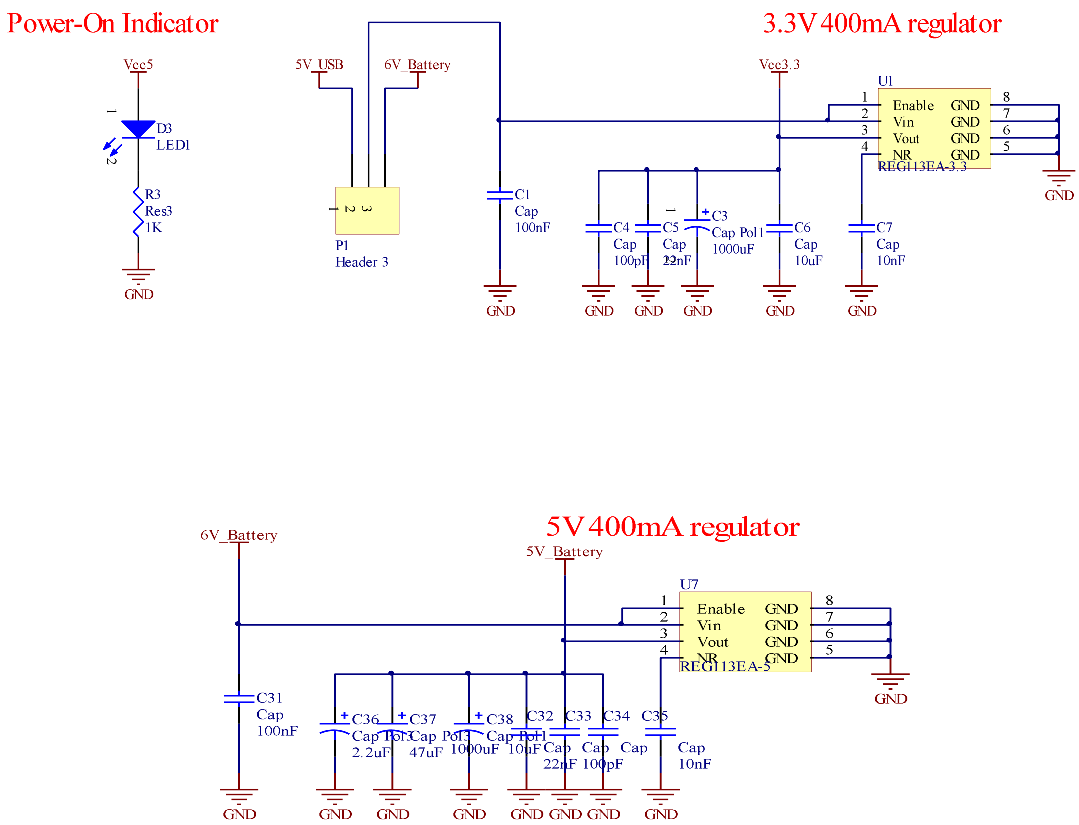

Figure 5.9: Power circuit

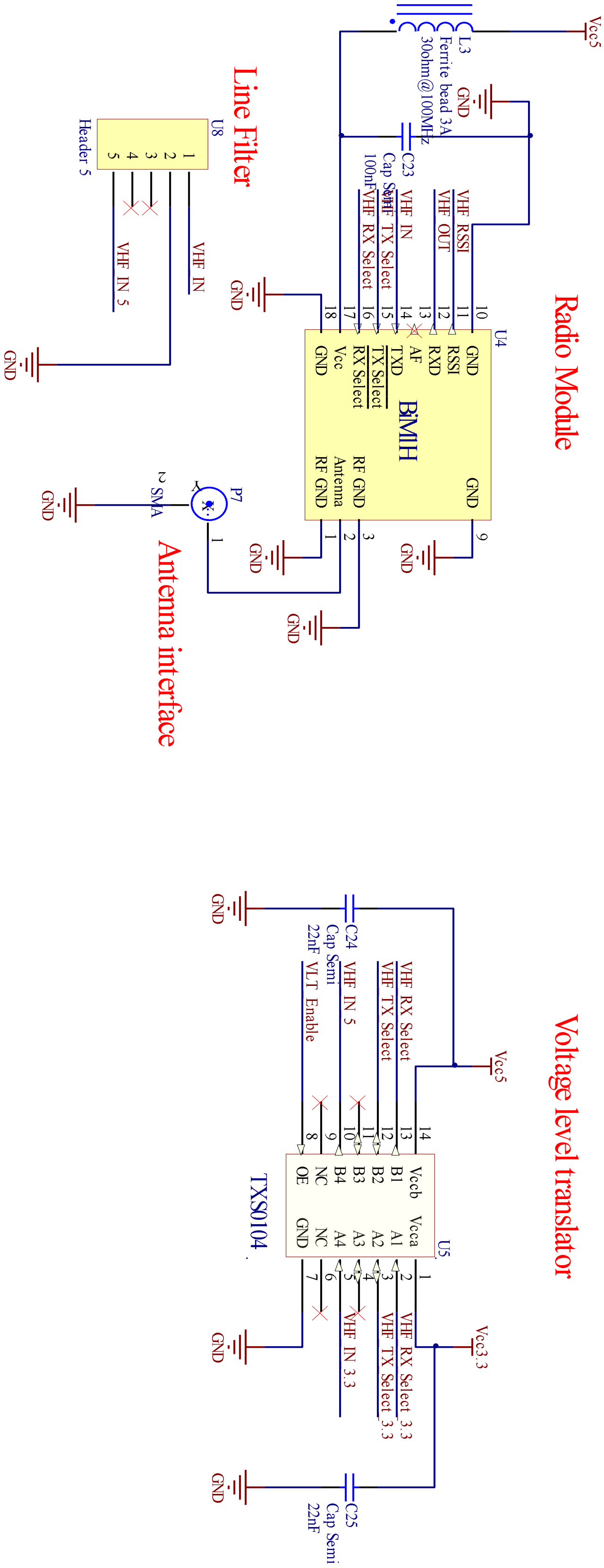

Figure 5.10: Transceiver circuit

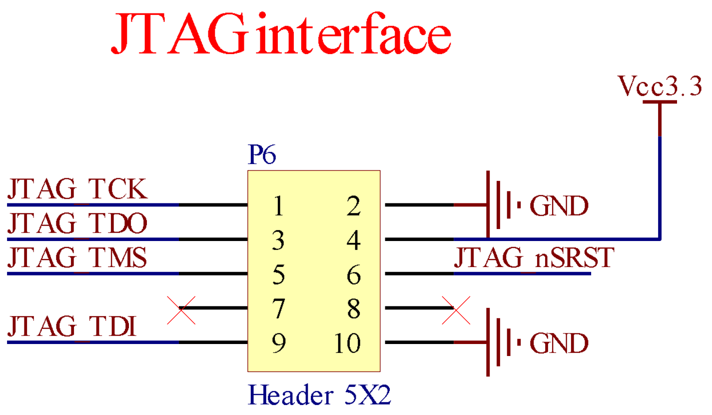

Figure 5.11: JTAG interface

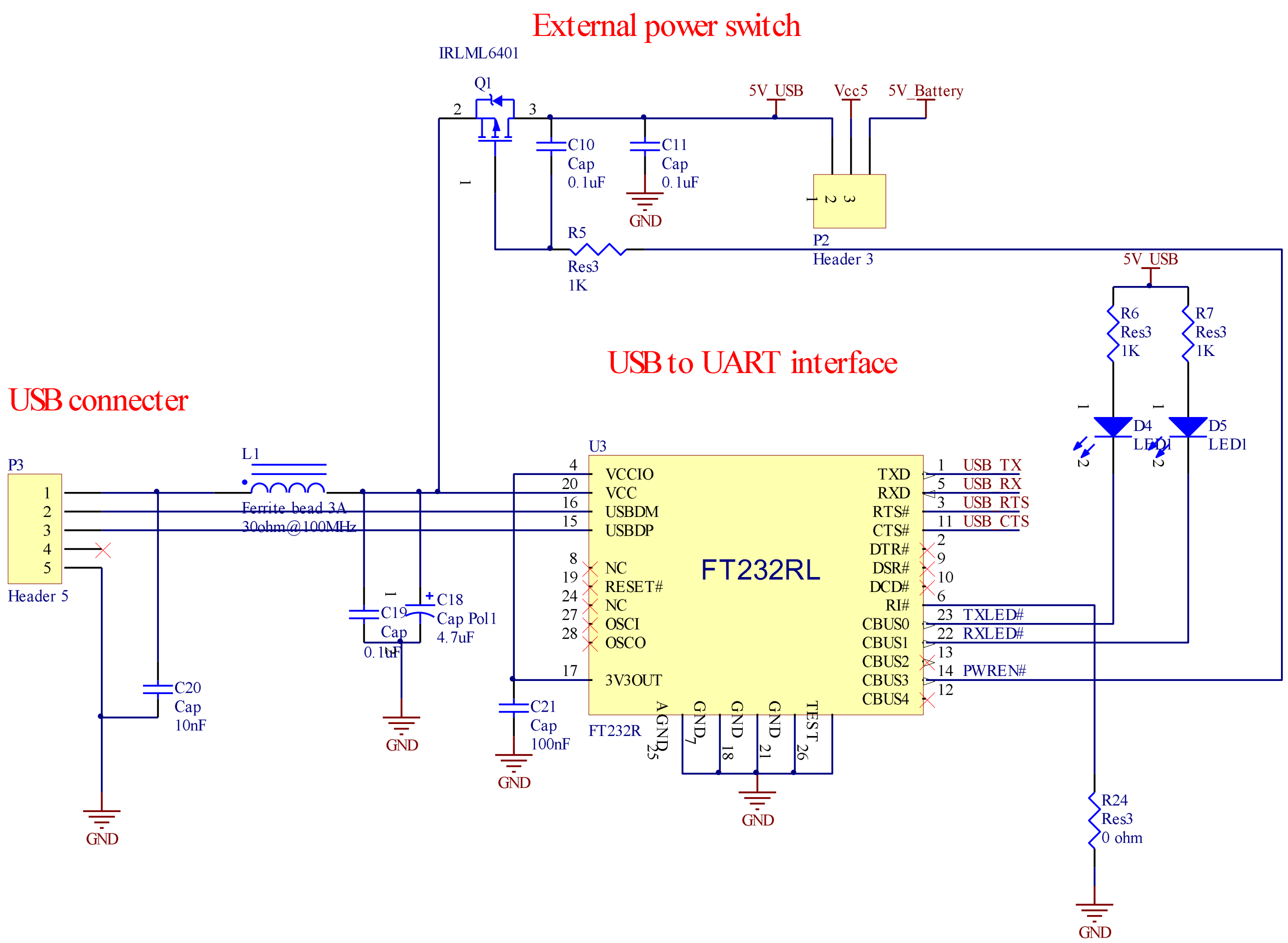

Figure 5.12: USB interface

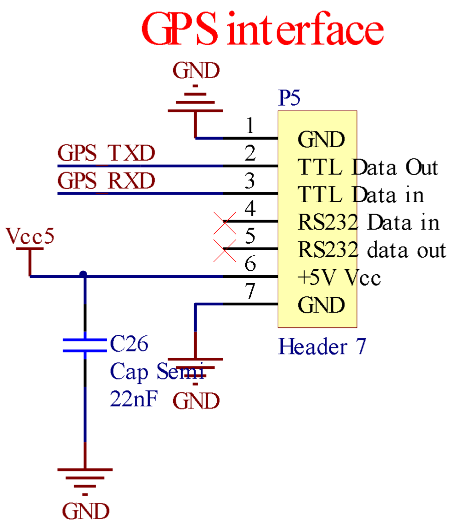

Figure 5.13: GPS interface

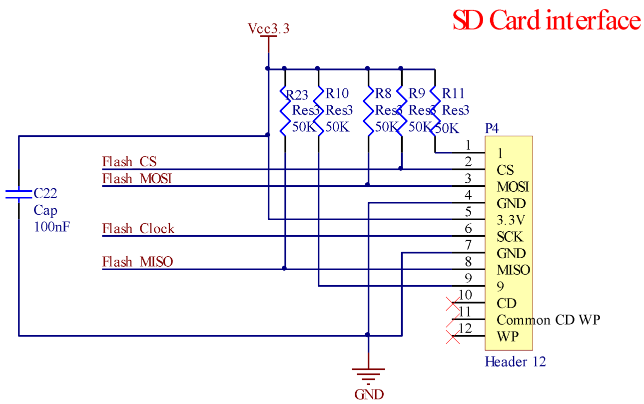

Figure 5.14: SD-card interface

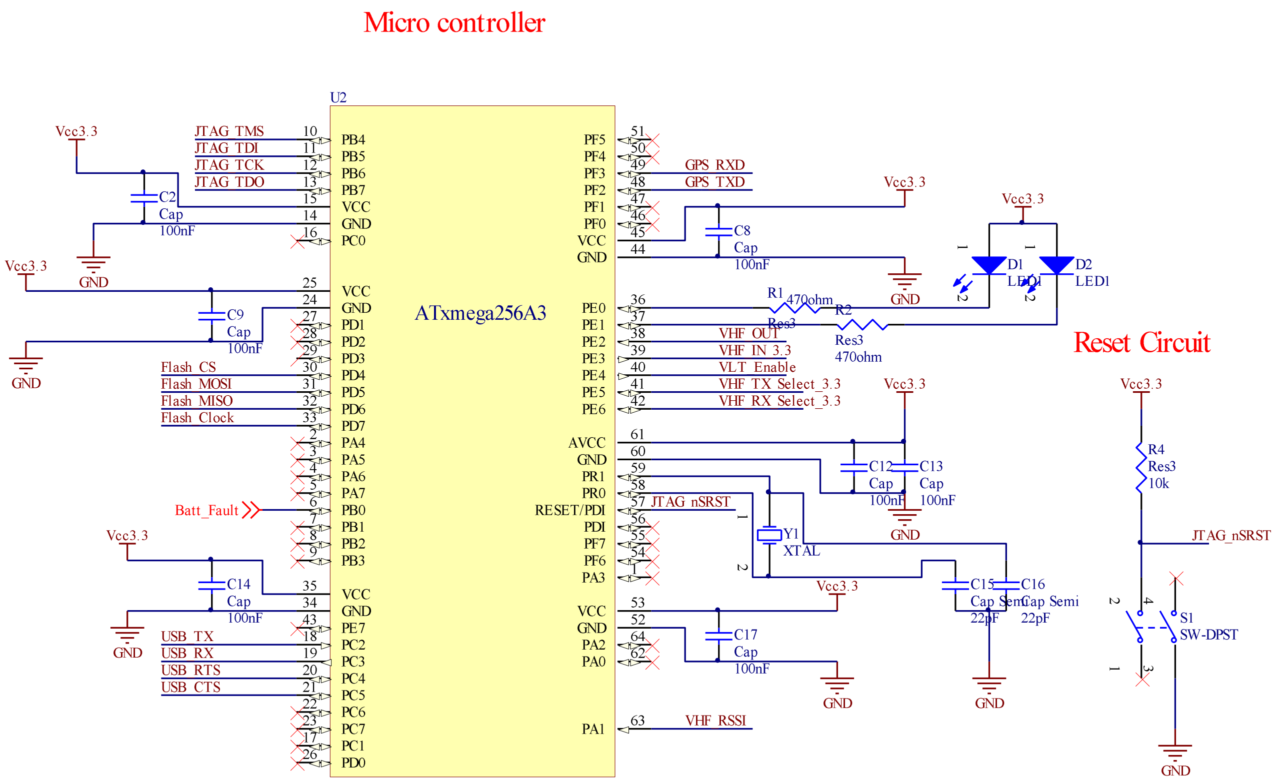

Figure 5.15: Microcontroller circuit

Chapter 6

Experimental investigation

6.1 Introduction

The aim of this chapter is to give results in terms of what the hardware and thereby formed network is capable of. It is important to give an idea of the performance of the network so that the end-user can know what to expect from the network. In experimenting with a range of parameters for each test, it is possible to determine the limits or bounds of the system, so that one can operate the network well beneath it to achieve reliability of operation.

6.2 Error performance of radio

6.2.1 Motivation

It is necessary to determine the optimal baud rate at which the radios can communicate for a certain packet error rate. Literature suggests that a higher baud rate will introduce more errors, however [24] determined a baud rate of 9600bps to be optimal for a similar BiM-UHF transceiver from Radiometrix, while a lower baud rate of 4800bps performed worse. It is attempted to do the same experiment, but for the BiM-VHF radio transceiver. The BiM1 transceivers' data sheet suggests that the lower the baud rate the more range the radios have. Baud rate influences the end-to-end delay of packets, which determines that for a lower baud rate, the network will become congested faster.

6.2.2 Experimental setup

The baud rate of communication is changed from 600bps to 9600 bps. A dummy packet with 8 bytes of data is sent 500 times, and the receiver stores every packet that was received without error. Each measurement is done 3 times and the average packet error rate is used.

6.2.3 Results

Figure 6.1 shows that for a signal strength of -95dBm(which is a fairly strong signal) the baud rate does not influence the packet error rate i.e. there is no loss of packets. With a signal strength of -108dBm(close to the receiver threshold) for the highest and the lowest baud rates, the performance is worst, while for 1200, 2400 and 4800, the packet error rate is effectively the same. At 4800bps the packet error rate is 5% less than the maximum of 9600bps.

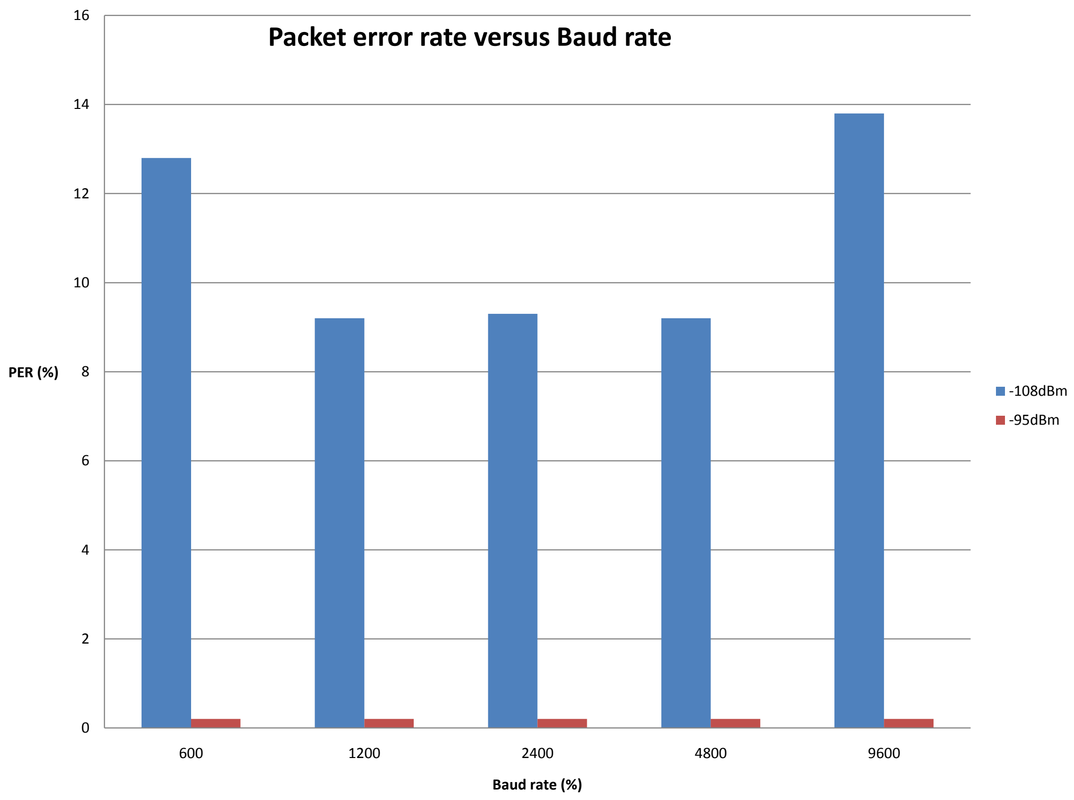

Figure 6.1: Baud rate vs PER

6.2.4 Interpretation

A good choice for communication speed would be 4800bps, as its performance is the same as 1200 bps, with the advantage that data will be sent four times faster.

6.3 Throughput

6.3.1 Motivation

Network throughput is defined as "..the average rate of successful message delivery over a communication channel" [30]. For this network it is important to know the throughput at the base station, since the base station is the sink, meaning all nodes send their packets to the base station. We distinguish between maximum theoretical throughput, peak measured throughput and maximum sustained throughput. The maximum theoretical throughput is closely related to the data rate of the channel, but also taking overhead into account. The peak measured throughput is the instantaneous throughput measured over a very short period of time, while the maximum sustained throughput is measured and averaged over a longer period of time. The maximum throughput is the minimum message arrival rate that will cause the delay of packets in the network to increase to infinity and thus make the system unstable [30]. We are interested in the maximum sustained throughput, since we want to find the message arrival rate at which the network becomes unstable and increases delay to infinity. When the delay goes to infinity, the throughput goes to zero. We do this by measuring the delay that packets experience in the network, since delay is the inverse of throughput.

6.3.2 Experimental setup

Five test units were built for testing the protocols and measuring the performance thereof. One unit has to act as a base station, while at least one has to act as a leopard collar and the rest should be relay stations for testing the multi-hop. Figures 6.2 and 6.3 show the two topologies that has been created using the five units.

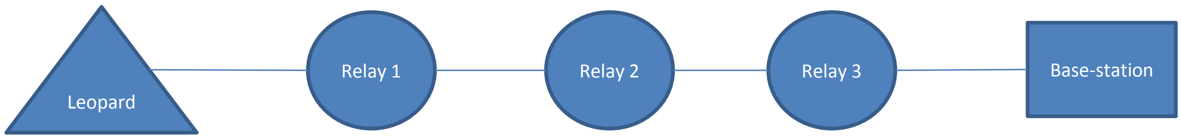

Figure 6.2: Network topology 1

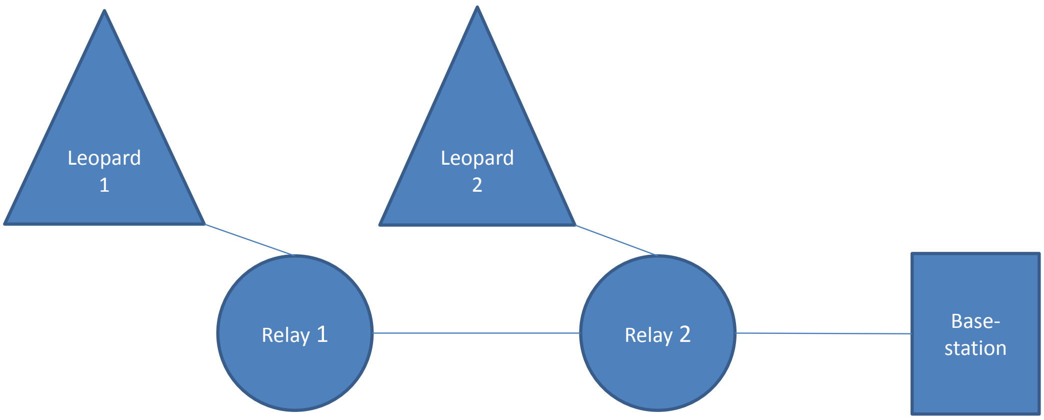

Figure 6.3: Network topology 2

Figures 6.4 and 6.5 show screen captures of the two topologies as done in OMNET++ with the MIXIM framework. The simulation software can be found on the enclosed DVD.

To measure the end-to-end delay that a packet experiences in the network, it is necessary to time stamp the packet at creation time and subtract that time from the time that the packet arrives at the base station. Once 50 packets have arrived, their end-to-end delays are averaged. This is done for both simulation and measurements to be able to compare the results to see how accurate the simulation models the network.

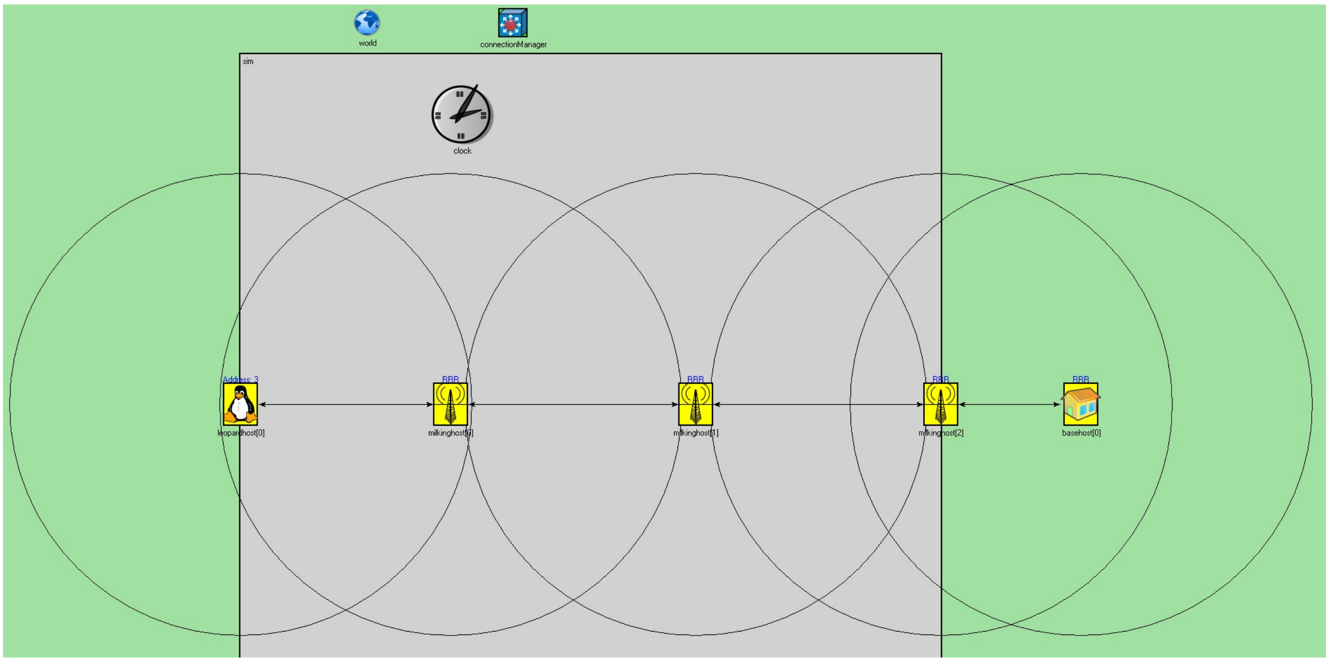

Figure 6.4: Screen capture of topology 1 as done in OMNET++

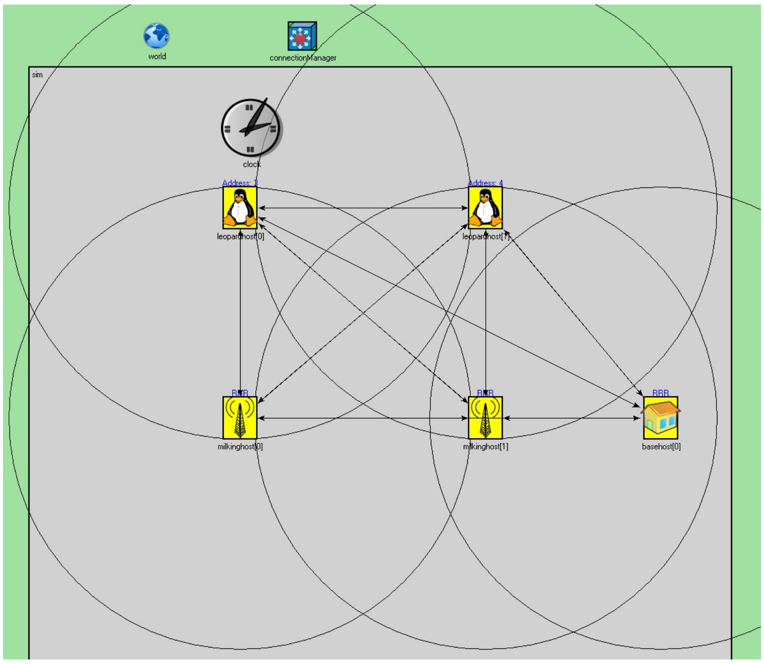

Figure 6.5: Screen capture of topology 2 as done in OMNET++

6.3.3 Results

Figure 6.6 shows the results for topology 1. The increase in delay at the increase in message arrival rate is to be expected, since the wireless channel has a finite capacity. Once messages arrive from a leopard collar faster than the network can send them to the base station, packets start queuing up at the first relay station. The average increased delay portrays the waiting time at the relay station's network queue. Notice how closely the simulation values resemble the actual measured values(all measured values fall within the standard deviation of the simulation values). Notice also how the standard deviation of the simulation values starts to increase at the increase in message arrival rate. This can be explained because of the network that becomes unstable with delay values approaching infinity.

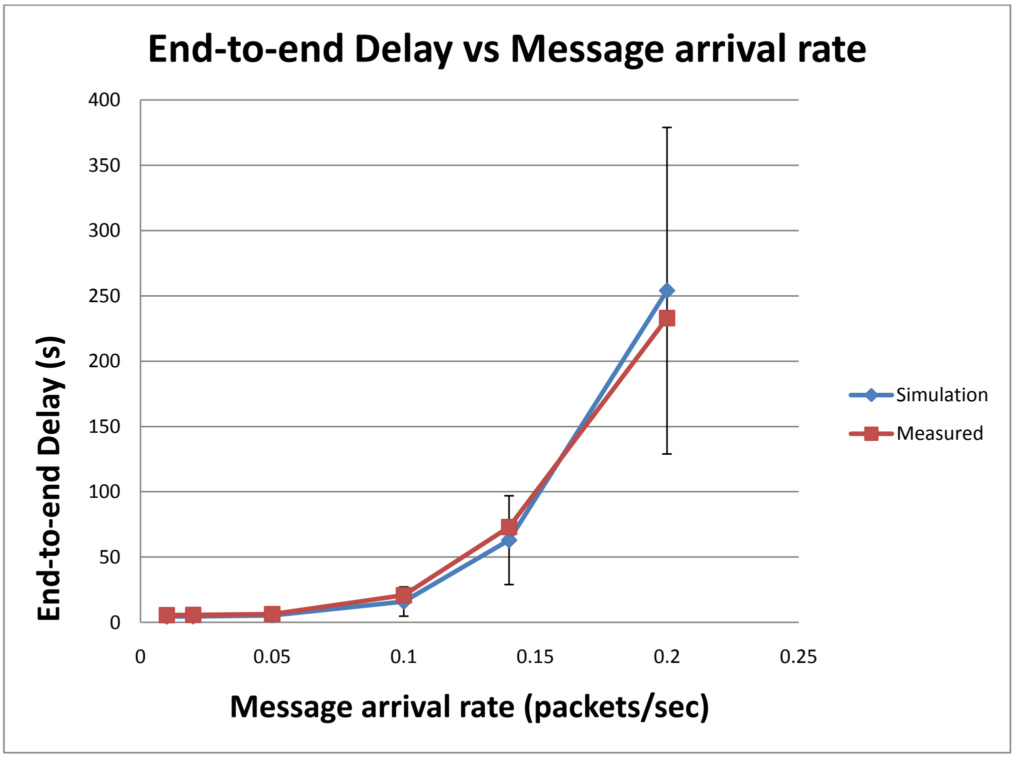

Figure 6.6: End-to-end delay for topology 1

Figures 6.7 and 6.8 shows the difference between a packet arrival rate that leads to sustained throughput and one that approaches zero because the end-to-end delay approaches infinity.

Figure 6.9 shows the end-to-end delay for topology 2. The same trend is observed as with topology 1, however here the end-to-end delay does not approach infinity as fast as with topology 1. This is because the parameters for both were kept the same, but topology 1 has only 2 hops and thus the packets spend less time in the network.

6.3.4 Interpretation

At a message arrival rate of 0.2 packets per second (1 packet in 5 seconds), the network becomes congested and the throughput at the base station approaches zero (end-to-end delay approaches infinity). The maximum message arrival rate should thus be 0.1 packets per second (1 packet in 10 seconds). This is feasible, since it is expected that the leopard arrival rate will be once per day with the collar sending a maximum of 2 data packets. One position fix takes 4 bytes and one data packet allows for 223 bytes to be sent. Thus a total of 111 position fixes will be sent over two data packets. This will take roughly 40 seconds (20 seconds per packet) to send through 3 hops. The message arrival rate of 0.1 packets per second will give the network enough time to deliver leopard packets to the

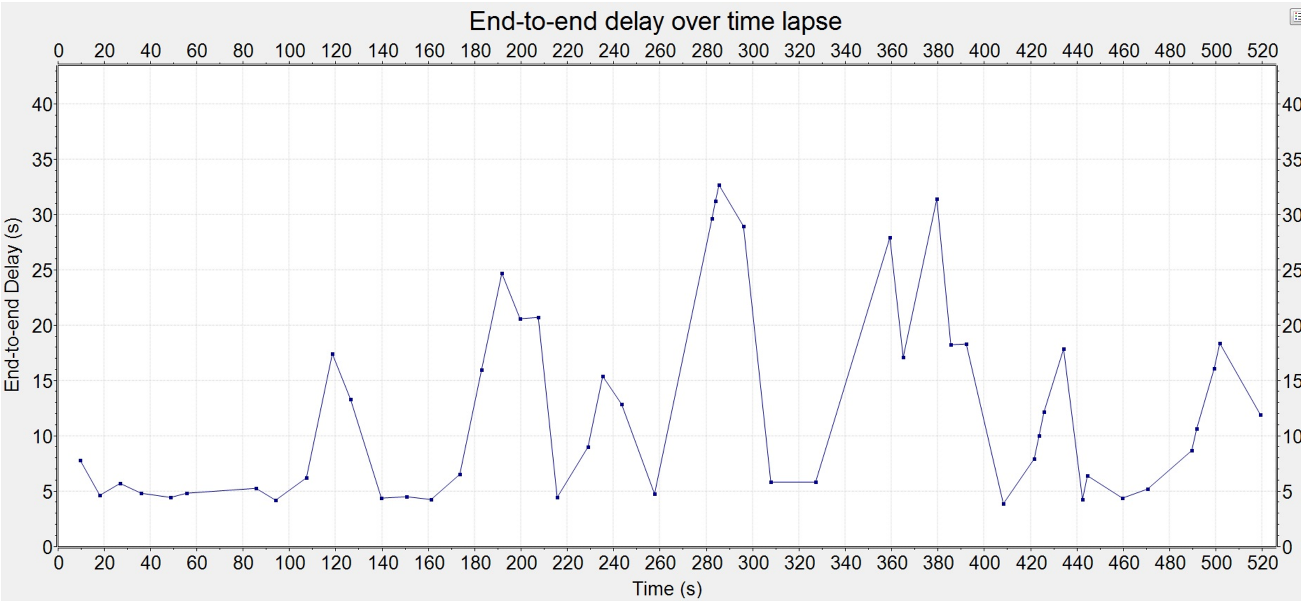

Figure 6.7: End-to-end delay over time lapse for 0.1 packets per second arrival rate

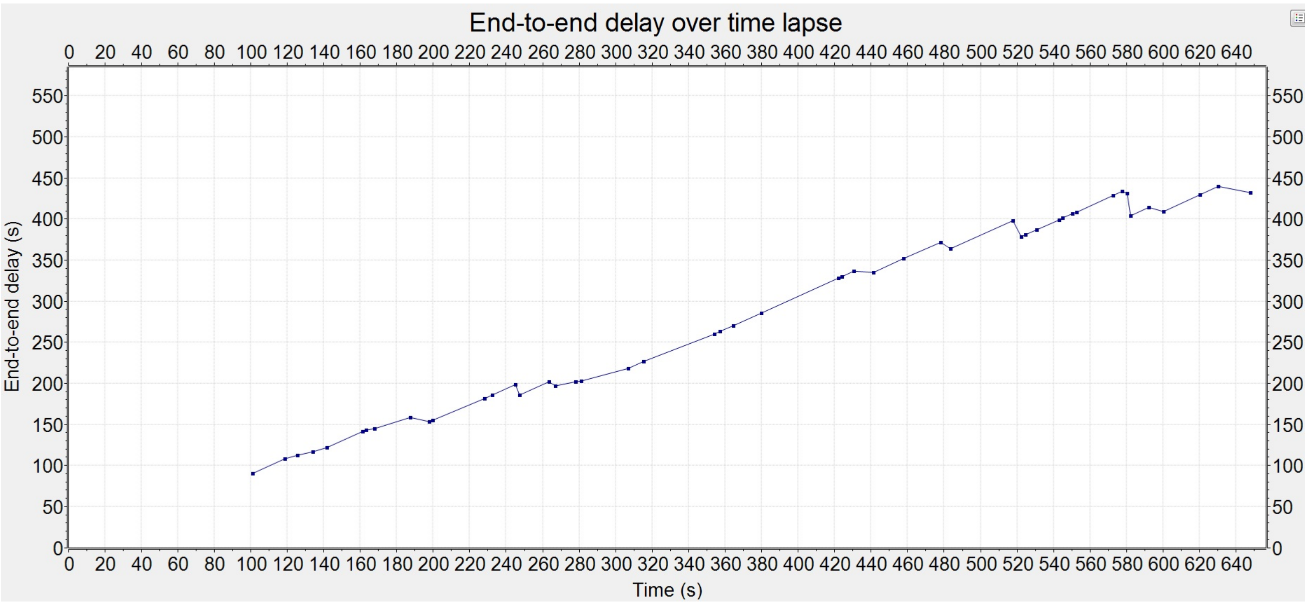

Figure 6.8: End-to-end delay over time lapse for 0.2 packets per second arrival rate

base station without becoming congested. A photo will be approximately 10kB, so has to be sent in 45 packets. The leopard cage station can be made to do flow control in which it sends 0.1 packets per second, so from Figure 6.6 it will take 20 seconds per packet and 15 minutes for the entire photo to arrive at the base station. Comparing this to the 3 hours and more it takes to manually go and download a photo in the field (depending on the location of the cage), the network provides a much faster solution.

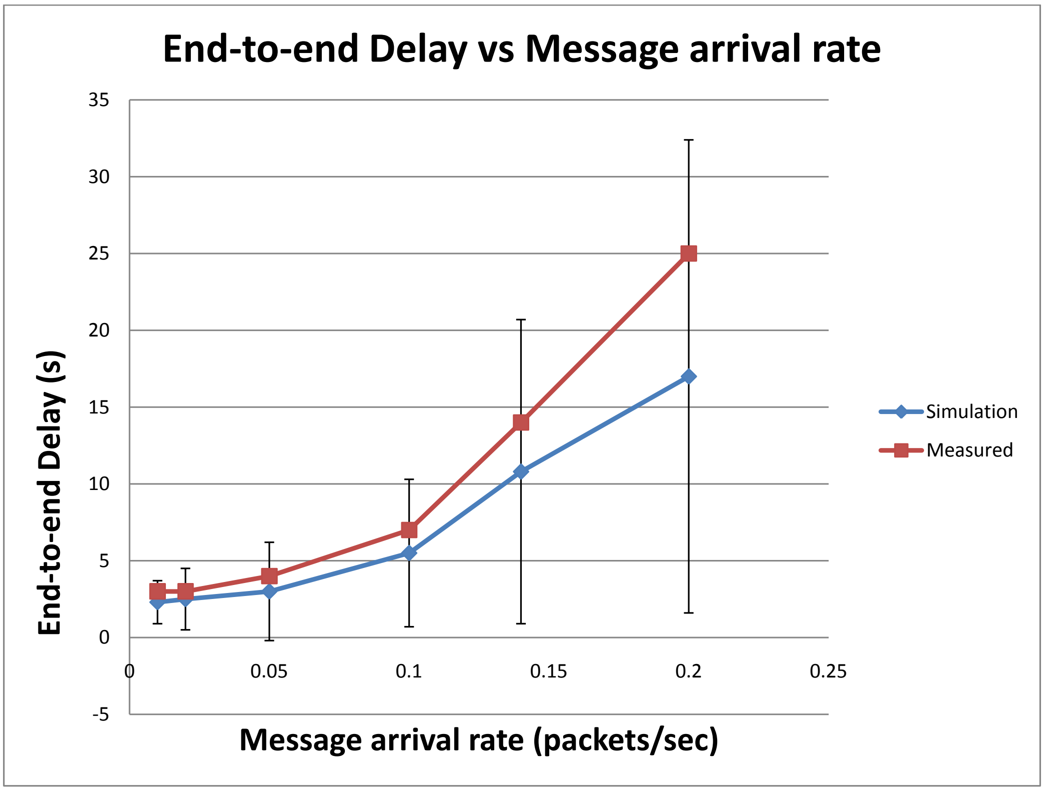

Figure 6.9: End-to-end delay for topology 2

6.4 Route acquisition delay

6.4.1 Motivation

The route acquisition delay is the time it takes to discover a route to the destination (base station) once a leopard packet has arrived at a relay station. It is necessary to see what the effect on the number of hops is, to determine what the delay would be from the time that a packet arrives from a collar to the time that the first packet arrives at the base station.

6.4.2 Experimental setup

A timer is started once a RREQ is broadcast and stopped once a RREP arrives in reply to that RREQ. Fifty of these measurements are made and the average taken to yield average route acquisition delay. This is measured with an increase of one hop each time. The maximum number of hops that the five node network can form is 3 (leaving one for the base station and one for a leopard collar). The simulation is run for more than three hops however, to show the trend in the route acquisition delay.

6.4.3 Results

The graph in figure 6.10 shows linear increase with an increase of about 2.5 seconds for each hop added. The measured results follows the simulation results closely. The standard deviation is rather large, which reflects the contention that RREQ packets have with RTS and POLL packets from other nodes. Sometimes RREQ packets goes through without any collisions (yielding a small value for route acquisition delay) and other times they collide with RTS and POLL packets, requiring a relay station to send out another one and adding more delay to a route being found (yielding a large value for route acquisition delay).

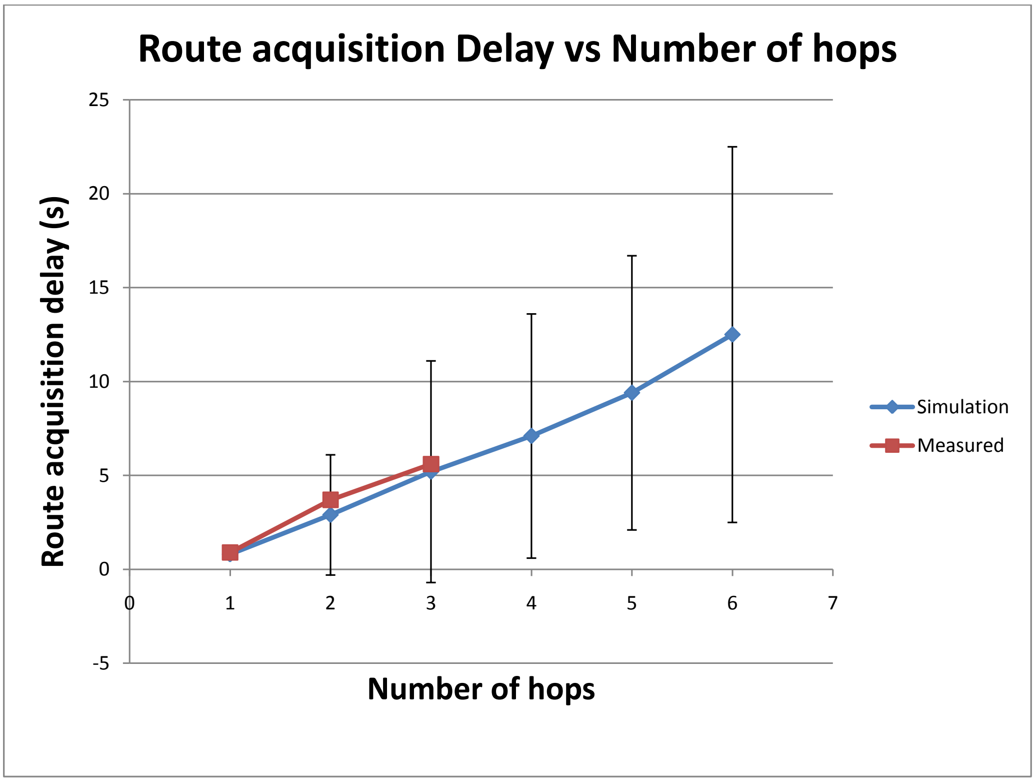

Figure 6.10: Route acquisition delay

6.4.4 Interpretation

Longer routes will have a greater impact on the initial delay that packets will experience if no route exists to the base station. The greatest number of hops in the network is 4 (refer to figure 3.9 in chapter 3), so this should be about 7.5s as seen on figure 6.10.

6.5 Range tests - fieldwork

6.5.1 Motivation

In order to determine the feasibility of a land-based radio network in an environment like the mountainous Cederberg, it was necessary to do actual field tests. This can now be compared with the theoretical and simulation results from Radio Mobile from chapter 3 to draw a better model for this area and predict the link quality at other sites not measured.

6.5.2 Experimental setup

The range tests are done incrementally. Two radios are placed first 100m apart, checked for communication and then the distance between the two gets incremented and again checked for communication. A GPS is used to mark the spots where the antennas are placed so that it can be plotted on Radio Mobile to compare the results. First line-of-sight tests are done, and later non-line-of-sight tests. For the non-line-of-sight test two radios are placed on either sides of a hill where Radio Mobile predicts a working communications link.

6.5.3 Results

After having success with some minor distances, a link of 2.6km is established with success as depicted by figure 6.11.

Figure 6.11: 2.6km line-of-sight link

Next a distance of 10.43km is attempted as depicted in figure 6.12 with success. Note that this agrees with the data sheet for the used radio, which suggests that a line-of-sight radio link of over 10km can be established.

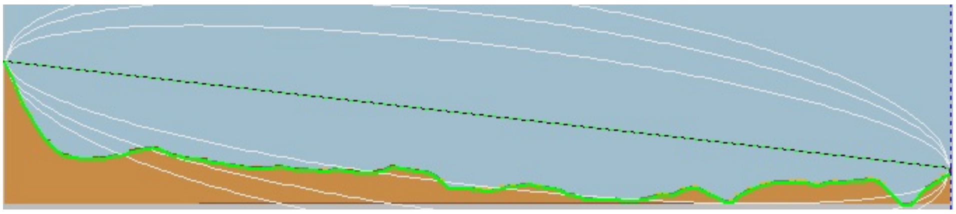

Figure 6.12: 10.43km line-of-sight link

Next a longer link is attempted where the line of-sight-path just scrapes the top of a hill as depicted in figure 6.13 with moderate success as only half of the packets sent came through. The distance is 12.42km.

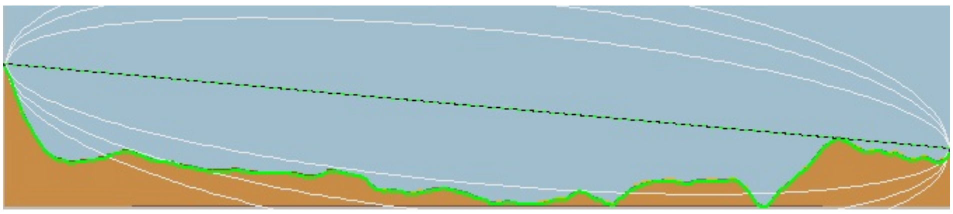

Figure 6.13: 12.42km link

Now two non-line-of-sight tests are done, one long-distance and one short-distance. Figure 6.14 shows the hill to the right of the picture blocking the direct communication link. Radio Mobile does predict a strong link of 21.1dB beyond the receive signal strength margin. No communication is established however.

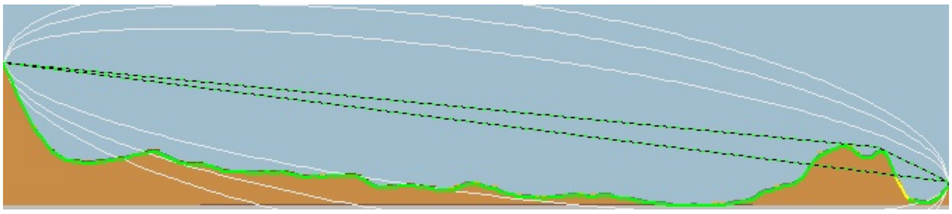

Figure 6.14: 10.29km non-line-of-sight link

For the short distance line-of-sight link, a distance of 3.73km is used between radios as depicted by figure 6.15 without success. Again Radio Mobile predicted a strong link.

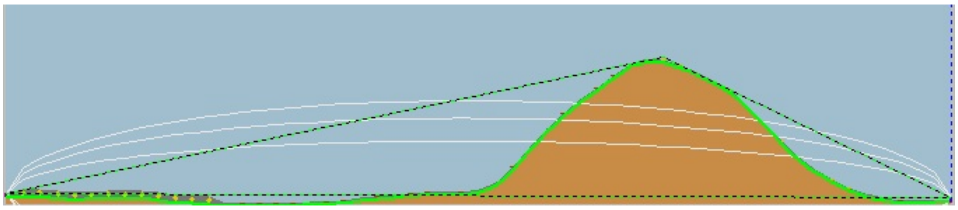

Figure 6.15: 3.73km non-line-of-sight link

6.5.4 Interpretation

For reliable communication with a carrier frequency of 151.3MHz, direct line-of-sight links have to be used, because with the non-line-of-sight links no communication was established. Radio Mobile's predictions seem to be inaccurate for non-line-of-sight links. This is ascribed to ground reflections and scattering which Radio Mobile does not take into account. It is desired to have a model that resembles the field tests more closely, so that Radio Mobile can be used to do accurate predictions of links for which field tests were not done due to time restrictions. Radio Mobile is set up to predict only where line-of-sight links will be feasible, thus using the terrain data to ignore links where any obstacles block a direct line-of-sight. This is done by introducing extra losses to account for these unaccounted effects in Radio Mobile. This changes the predictions made in chapter 3 considerably, because using the new line-of-sight-only-model, Bushmanskloof cage, Karukareb cage, Mannetjiekloof cage, Vaalkloof cage, Leeuvlak1 and 2, and Sneeuberg cage are not connected to the network. This is to be expected as all of these cages lies in dips, so more repeater units should be placed on strategic places to connect them to the network as well.

Figure 6.16 shows the network for the line-of-sight model in Radio Mobile. Three extra units are included and some of the cages are moved to more line-of-sight positions. This adds up to a total of 9 repeater units to connect all 13 cage monitoring nodes to the network. These repeater units will also serve as monitoring units for leopard collars..

Figure 6.17 shows a combined Cartesian coverage plot. Compare this with Figure 3.11 from chapter 3. The area that is covered under radio reception is considerably less. This

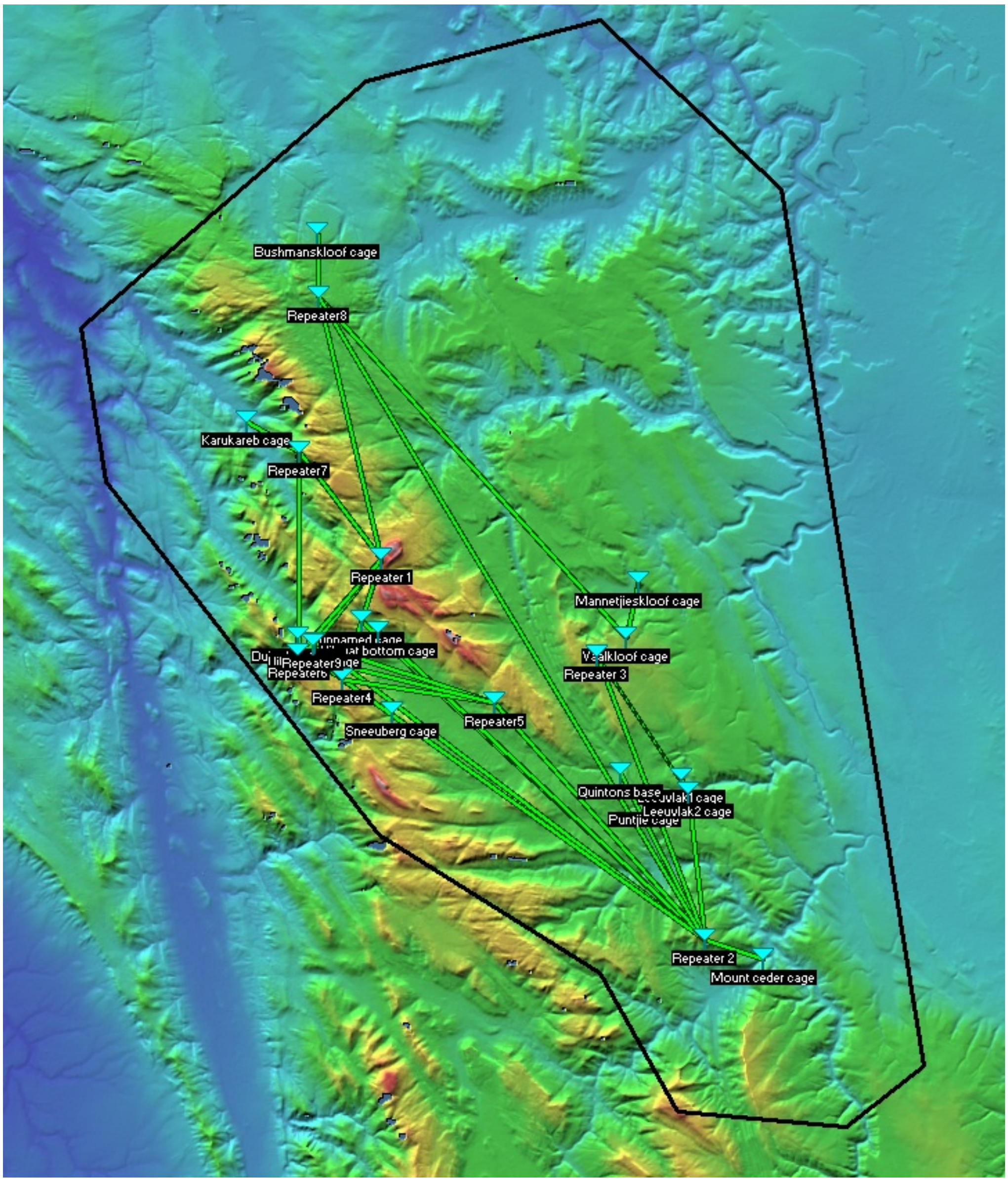

Figure 6.16: Network showing all nodes connected for the line-of-sight model by using 3 extra repeater nodes and moving the cages out of the dips

is due to the many valleys shaded away from radio coverage where line-of-sight links do not reach.

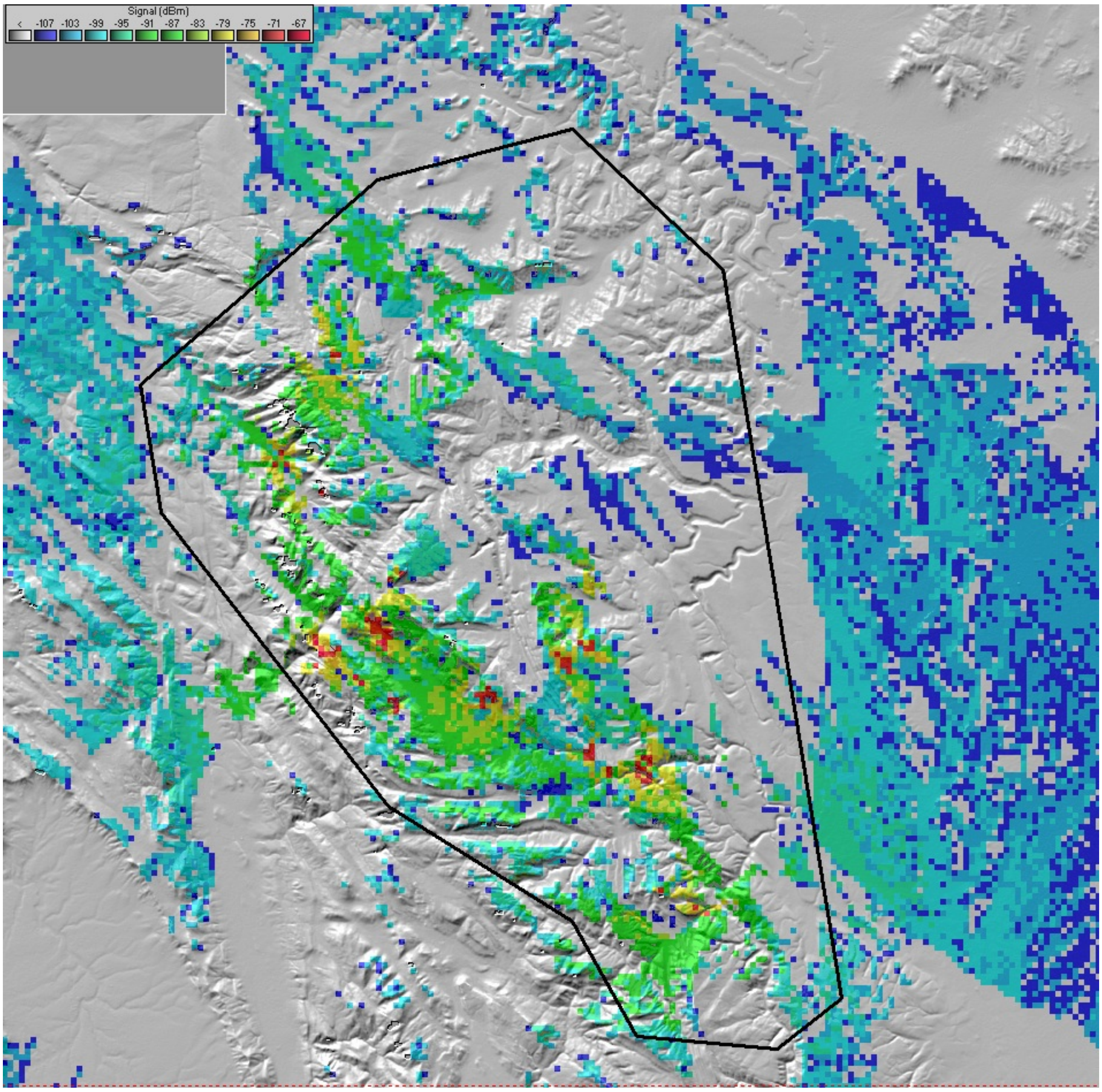

Figure 6.17: Combined Cartesian coverage plot

6.6 Power performance

6.6.1 Motivation

It is necessary to compare the power consumption of all the components given from their respective data sheets to actual measured values, so that an accurate power design can be done. Thereafter a node should be tested for three consecutive days of autonomy in the case that the sun does not shine and the node will rely entirely on its battery. This will assure reliability.

6.6.2 Experimental setup

In chapter 5 the maximum current draws for each component was given from their respective data sheets. The maximum current that the board will draw in any given situation will be when the radio is in transmit mode. The maximum power dissipated would be:

$$P_{max} = P_{radio-t} + P_{GPS} + P_{uController} + P_{3.3V-regulator} + P_{5V-regulator}$$

$= (290 \times 5) + (36 \times 5) + (14 \times 3.3) + (14 \times (6.5 - 3.3)) + (326 \times (6.5 - 5)) = 2,21W$

The total current drawn from the battery will now be measured with a multimeter with the respective components turned on. For the autonomy test a node is made to transmit a data packet every 10 seconds for 3 consecutive days without a solar panel connected to charge the battery.

6.6.3 Results

The measured current is 325mA with the battery at 6.5 V. Thus the total maximum power that the PCB can draw is 2,113W. The node with its 30Ah battery as sized in chapter 5 lasted for three days without completely draining the battery.

6.6.4 Interpretation

The measured power consumption of the components is a bit lower than predicted, which should be due to manufacturing variations of components. The node's battery as expected lasted the three days it was designed for. This shows that the power predictions is not optimistic and the power source of the system is adequate.

6.7 Summary

The packet error rate test showed that 4800bps is the optimal baud rate for communication. This baud rate is justified since it has 5% packet success over the maximum baud rate of 9600bps. The throughput test showed that the maximum sustainable throughput is achieved at a message arrival rate of 0.1 packets per second (1 packet in 10 seconds). Message arrival rate beyond this number will result in the network becoming congested (unstable). For the current network configuration as in Figure 6.16 the longest path of 6 hops will result in an initial route acquisition delay of 12.5 seconds as read from Figure 6.10. Range tests in the Cederberg discovered that no non-line-of-sight links are possible at 151.3MHz, which is in contrast with the Radio Mobile predictions. A maximum reliable link distance of 10.43km line-of-sight was found. The new predictions from Radio Mobile using the line-of-sight model yields a study area with just below 50% radio coverage. The power test showed that the total predicted power consumption by all components almost equals the measured power consumption, so a power source sized from that predictions should be adequate. This was also shown to be adequate by a three day autonomy test.

Chapter 7

Conclusions and recommendations

7.1 Summary and conclusions

This study in ad hoc networks for the application of acquiring wildlife tracking data in the Cederberg proved to be a viable alternative solution to the current manual techniques employed (provided that more than 22 stations are deployed for covering more than 50% of the study area). The results in chapter 6 showed a great improvement in time efficiency over the manual techniques used in the past to obtain data. Compared to the several hours it takes manually, the network will save a lot of a researcher's time. Chapter 1 discussed the available solutions for obtaining tracking data over considerable distances. With cost and automation needs in mind, an ad hoc network was deemed to fit the project specifications with one unit costing R4048. In chapter 2 the MACAW protocol was chosen to be most suitable for the data link layer of the communication system and AODV was the chosen protocol for the network layer. These protocols were simulated in OMNET++ and the results obtained were compared with measured results from the network. The simulation results agreed closely with the measured results. The range tests in the Cederberg yielded somewhat disappointing results compared to the initial Radio Mobile prediction. No non-line-of-sight links are possible at 151.3 MHz. The hardware design yielded a functional PCB which were deployed in the field and showed correct protocol operation.

7.2 Comparison to prior work

Prior work using ad hoc network architectures for obtaining animal tracking data includes Zebranet from [1] and EcoLocate from [19]. Both these networks make use of only mobile nodes (collars) where the network is highly dynamic since animals move around a lot, changing the topology of the network constantly. In this thesis milking stations are nomadic, thus residing at fixed locations for extended periods of time. Animal collars and relaying stations are two distinct designs, where collars only has the task of obtaining location information and sending it to milking stations once polled. Milking stations only have the task of obtaining this data and relaying it to a base station. With EcoLocate different species of animals are fitted with collars to incorporate a broad spectrum of the animal kingdom into the network. Zebranet and this work considers only one kind of species, or similar sized animals, whilst this network can be used to relay data from any type of animal to a base station. EcoLocate fits different sized batteries to different kind of animals, hence they use a hierarchical approach to routing data in the network, giving larger animals with larger batteries more traffic to route. Mobility influences the the routing of packets in EcooLocate. Zebranet uses no routing, all data from collars is flooded from one collar to the next so that each collar will have information from every other collar. This work uses a reactive routing protocol where the routing metric is simply the shortest path to the destination. Solar panels are used by all projects to replenish a battery which powers collars or relay milking stations. The main difference between this work and the above mentioned is that a dedicated network is used to gather animal location information and photos (from collars and camera trap cages) to deliver it to a base station. Whereas Zebranet and EcoLocate gathers only location and sensor information from animals and only collars are used to form the network.

7.3 Outstanding issues

The following lists all issues that still needs to be addressed for a reliable network:

- A watchdog timer should be implemented to reset each node if something goes wrong and the system does not recover by itself
- Nodes should be placed on all positions as predicted with Radio Mobile to confirm the absolute correctness of the line-of-sight model
- A full-fledged network should be employed in the Cederberg with leopard collars and trap cages actively generating traffic as a final network test

7.4 Recommendations for future work

While the network and hardware worked fine, several improvements can be made to make the system work more efficiently. This includes the following:

- Incorporate the camera from the leopard trap cage into the milking station design for immediate transferring of photos to the base station, without a milking station needing to poll a camera trap cage for data as with leopard collars.
- Change the MACAW protocol to allow for multiple data packets to be downloaded from a collar by one POLL packet from a milking station.

Appendices

Appendix A

PCB layout

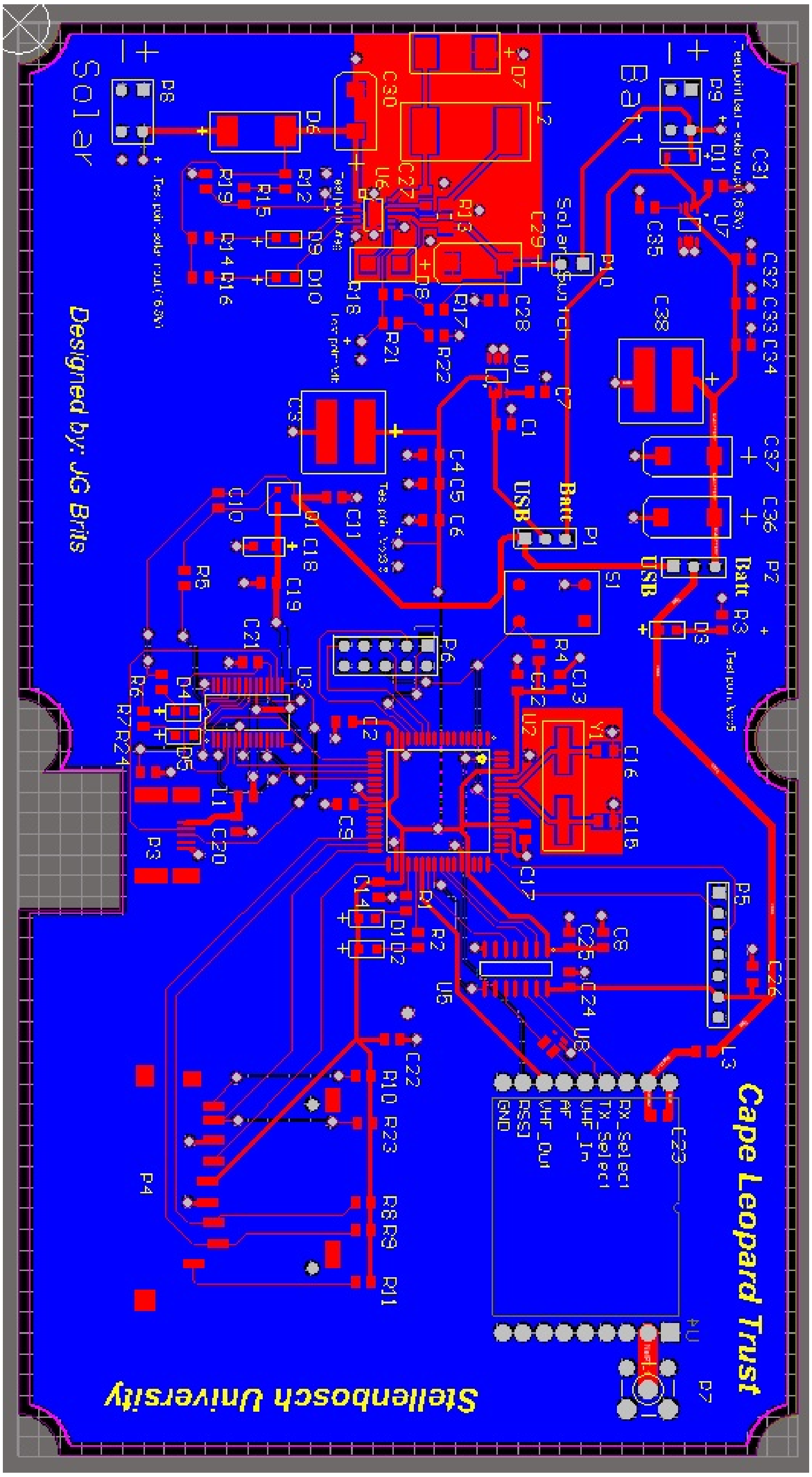

Figure A.1: PCB top layer

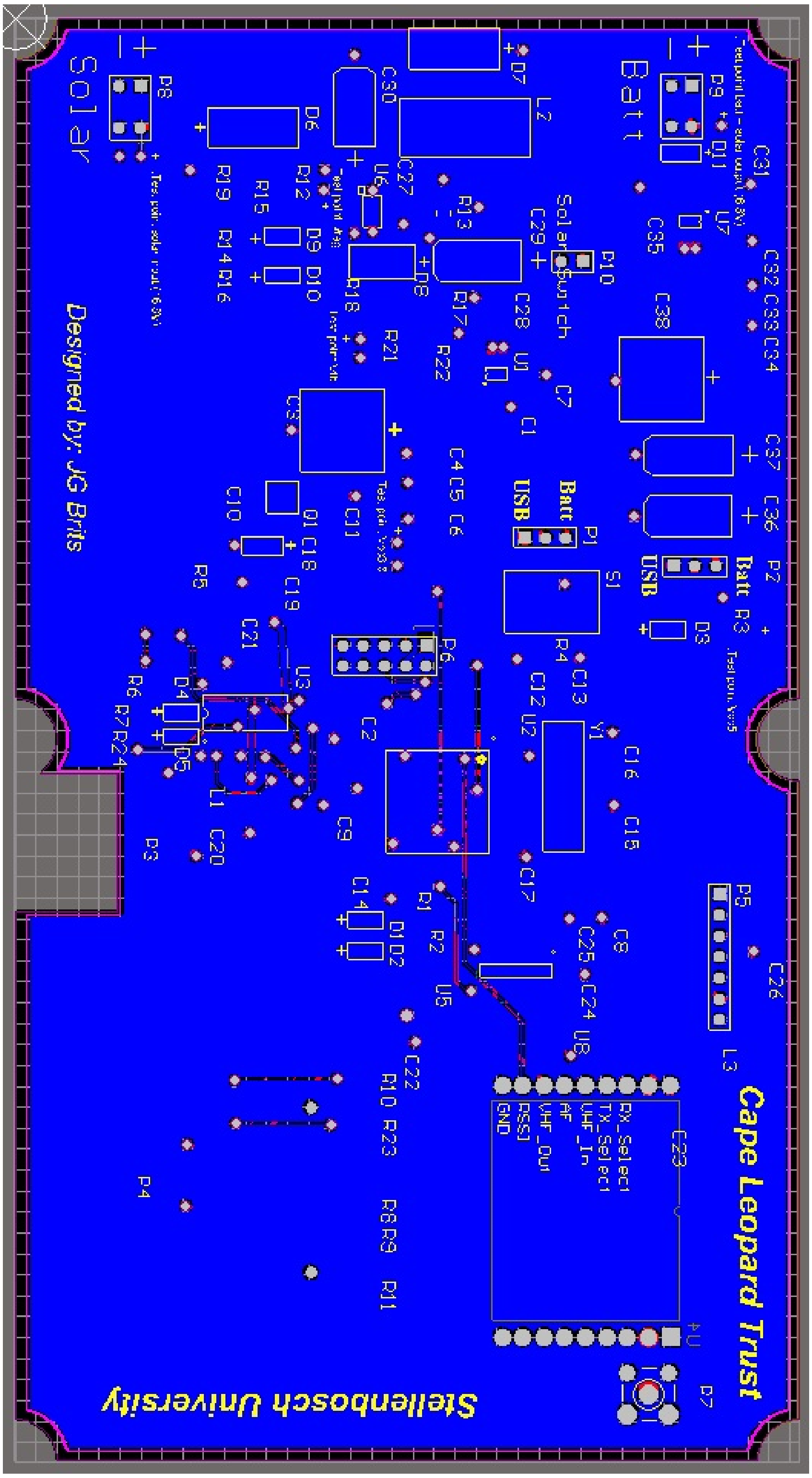

Figure A.2: PCB bottom layer

Appendix B

Project Pictures

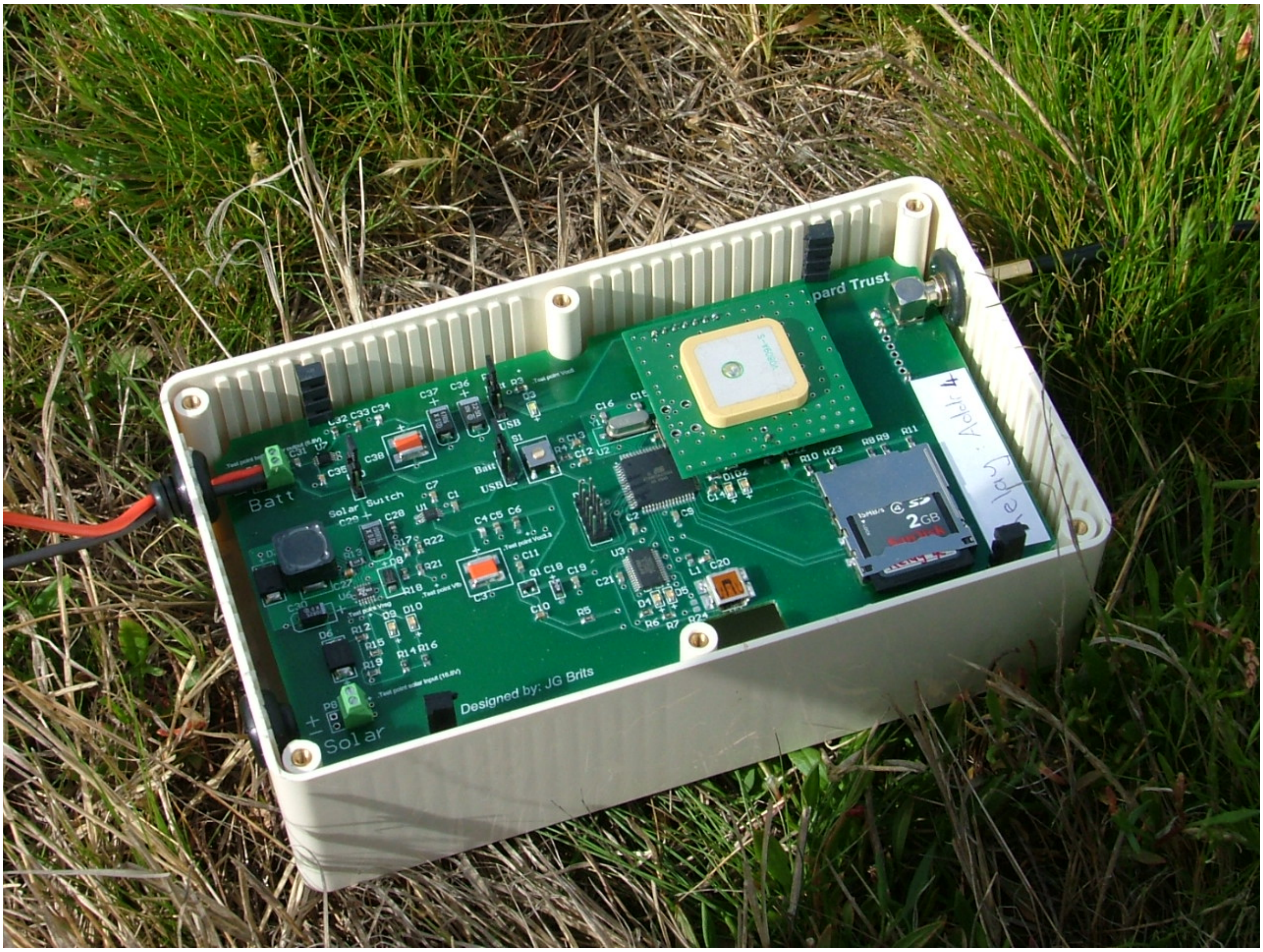

Figure B.1: PCB photo

Bibliography

[1] (2002 November). Engineers and biologists design wireless devices to unlock secrets of animal kingdom.
Available at: http://www.princeton.edu/pr/pwb/02/1111/1a.shtml, [2009, May 8]

[2] (2004 March). *General Notice 533*, vol. 465. Department of Communications, Government Gazette.

[3] (2006 February). Average temperatures and hours of sunshine in south africa.
Available at: http://www.southafricalogue.com/travel-tips/average-temperatures-and-hours-of-sunshine-in-south-africa.html, [20 October 2009]

[4] (2006 January). Pcb trace width calculator.
Available at: http://www.circuitcalculator.com/wordpress/2006/01/31/pcb-trace-width-calculator/, [2010, February 3]

[5] (2007 November). *VHF Narrow Band FM 500mW transceiver*. Radiometrix, 1st edn.

[6] (2009). Gps pet tracking devices.
Available at: http://www.gps-practice-and-fun.com/gps-pet-tracking.html, [2009, April 25]

[7] (2009). *LT3652: Power Tracking 2A Battery Charger for Solar Power Datasheet*. Linear Technology.

[8] (2009). Satellite tracking.
Available at: http://www.seaturtle.org/tracking/faq.shtml, [2009, March 21]

[9] (year unknown). Aerial telemetry.
Available at: http://www.skymasters.ca/index.php, [2009, March 12]

[10] (year unknown). Rf link budget calculator.
Available at: http://www.afar.net/rf-link-budget-calculator/ , [2009, March 7]

[11] Blake, R. (2001). *Wireless Communication Technology*. Delmar Thomson Learning.

[12] Chakeres, I.D. and Klein-Berndt, L. (). Aodvjr, aodv simplified. *Mobile Computing and Communications Review*, vol. 6, pp. 100–101.

[13] Coude, R. (1997). Radio mobile.
Available at: http://www.cplus.org/rmw/english1.html, [2009, February 15]

[14] Dobos, M. (2007 June). The osi model.
Available at: http://www.tutorial5.com/content/view/26/79/, [2010, November 8]

[15] Foster, R., Ghassemi, M. and Cota, A. (2010). *Solar energy - renewable energy and the environment*. CRC Press.

[16] Fullmer, C.L. and Garcia-Luna-Aceves, J. (1997). Complete single-channel solutions to hidden terminal problems in wireless lans. *IEEE*.

[17] Irvine, J. and Harle, D. (2002). *Data communications and Networks: an Engineering Approach*. John Wiley and Sons, LTD.

[18] Magna Design Net, I. (2010 September). Review of digital modulation.
Available at: `http://www.magnadesignnet.com/en/booth/technote/ofdm/page2.php, [2010, December 10]`

[19] Markham, A. (2008). *On a Wildlife Tracking and Telemetry System: A Wireless Network Approach*. Ph.D. thesis, University of Cape Town.

[20] Martins, Q. (2010). Why the leopard.
Available at: `http://www.capeleopard.org.za/, [2010, October 24]`

[21] Murthy, C.S.R. and Manoj, B. (2004). *Ad Hoc Wireless Networks: Architectures and Protocols*. Prentice hall.

[22] of Science, M.U. and Technology (2008). Microstrip impedance calculator.
Available at: `http://emclab.mst.edu/pcbtlc2/microstrip.html, [2010, March 13]`

[23] Ott, H.W. (2001). Partitioning and layout of a mixed signal pcb. *Printed Circuit Design*, vol. June.

[24] Paramananthan, S. (1997 November). Error performance of bim transceiver with rs232 interface. Tech. Rep..
Available at: `http://www.radiometrix.co.uk/apps/apnt101.htm`

[25] Sande, E. (2010). Kenya: Gsm radio tracking canopies the wildlife. *News from Africa*.

[26] Sheng, J. (2008). *Performance modeling of IEEE 802.11 ad hoc networks under time-varying channel*. Ph.D. thesis, Rensselaer Polytechnic Institute, United States – New York.

[27] Tanenbaum, A.S. (2003). *Computer Networks:*. Pearson Education International.

[28] Warren, H.S. (2003). *Hacker's delight*. Addison-Wesley.

[29] Wikipedia, t.f.e. (2009 December). Differential manchester encoding.
Available at: `http://en.wikipedia.org/wiki/Differential_Manchester_encoding, [2010, June 7]`

[30] Wikipedia, t.f.e. (2010 November). Throughput.
Available at: `http://en.wikipedia.org/wiki/Throughput, [2010, December 8]`

[31] Zyren, J. and Petrick, A. (1998 June). Tutorial on basic link budget analysis. Application Note 9804.