ZACHODNIOPOMORSKI UNIWERSYTET
TECHNOLOGICZNY W SZCZECINIE

Wydział
Informatyki

PRACA DYPLOMOWA

Communication algorithms and principles for a prototype of a wireless mesh network

Autor:
Sergiusz Urbaniak

Opiekun pracy:
dr inż. Remigiusz Olejnik

Szczecin, 2011

Oświadczenie

Oświadczam, że przedkładaną prac magisterską/inżynierską kończącą studia napisałem samodzielnie. Oznacza to, że przy pisaniu pracy poza niezbędnymi konsultacjami, nie korzystałem z pomocy innych osób, a w szczególności nie zlecałem opracowania rozprawy lub jej części innym osobom, ani nie odpisywałem rozprawy lub jej części od innych osób. Potwierdzam też zgodność wersji papierowej i elektronicznej złożonej pracy. Mam świadomość, że poświadczenie nieprawdy będzie w tym przypadku skutkowało cofnięciem decyzji o wydaniu dyplomu.

Sergiusz Urbaniak

Contents

List of Figures

List of Tables

Chapter 1

Introduction

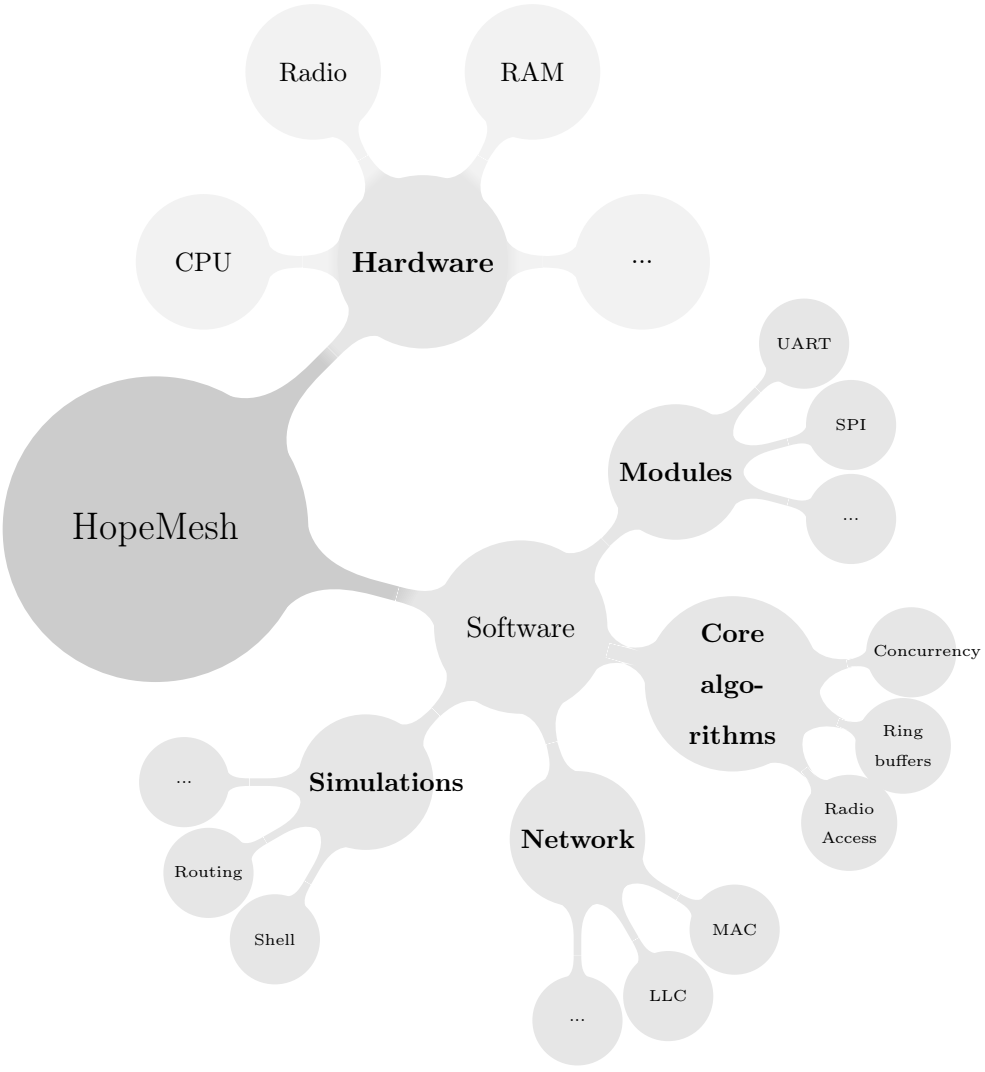


Figure 1.1. HopeMesh project mind map

This thesis has the goal to implement an advanced and refined version of the predecessor implementation [2] for a fail-safe mesh network prototype using embedded technologies. The project name "HopeMesh" reflects the major goal to implement a mesh routing algorithm based on cheap HOPERF radio modules. This goal can be split in the following aspects according to the mind map as seen in figure 1.1:

- **Hardware:** The goal is to explore alternative, enhanced and reusable hardware solutions for an embedded implementation.
- **Modules:** The goal is to find the necessary software modules from an abstract architectural point of view.
- **Algorithms:** The goal is to explore and elaborate on concrete algorithms and data structures for the implementation of the software modules.
- **Network:** The goal is to implement a network stack which not only provides a mesh routing based on the B.A.T.M.A.N. algorithm but also provides lower network layers.
- **Simulation :** The goal is to provide the basis for a simulation environment for the provided algorithms that can execute on regular PCs.

The author wants to prove that an implementation of a robust and scalable mesh network using embedded devices despite its hardware constraints is quite possible. He wants to explore algorithms and software architectures usually hidden behind the curtain of operating systems. The desired end result is not only to have a working mesh network prototype but also an algorithmic framework for further development. Therefore the author also wanted to provide a framework which allows to try and research future algorithms on a regular PC. Finally the author wanted to provide a reproducible hardware design in order to able to equip a complete laboratory of mesh nodes for further research and investigation.

1.1. Thesis overview

The thesis is structured in the same order as the above mentioned goals. The first part analyzes the existing prototype hardware. An enhanced version is proposed by providing an alternative CPU and the connection of external RAM. Level shifters are introduced for the connection of the RFM12B radio module and the existing UART connection is being enhanced by an USB interface. Finally connectors for an external keyboard and an external LCD module are introduced.

The second part elaborates on the envisioned software architecture. It identifies the necessary software modules which have to be implemented in order to provide a robust design. It defines modules for the human interaction and for the internal state control. The network stack module and the RFM12B driver module are identified for the mesh network access.

The third part explores the algorithmic foundations and data structures which are being used for the implementation. Different concurrency models are being analyzed and a threading framework for the software modules is proposed. An algorithm for the seamless integration of the UART module is being proposed and finally the complex concurrency behavior of the RFM12B driver module analyzed. The fourth part is solely dedicated to the network stack. The implemented network layers and packet structures are described as well the used transmission encoding (Hamming).

The last part elaborates on the implemented simulations in order to verify the modeled algorithms, data structures and network stacks on a regular PC.

Chapter 2

Hardware Design

2.1. Introduction

The predecessor implementation uses an Atmel Atmega16 RISC microprocessor. The author decided to analyze whether this CPU is still adequate for the new implementation. The decision about a microprocessor to be used in an embedded application depends very much on the requirements. Not only that many vendors are available on the market but also each vendor has a very rich product portfolio of different microprocessors to choose from.

The author set up the following requirements for the new hardware architecture:

- **GCC tool chain:** The author wanted to use an open source development environment. The existing GCC toolchain is known to most programmers and the compiler can be used cross-platform on Windows, the MacOS and Linux operating systems.

- **USB connectivity:** Instead of using the rather old and nowadays even mostly not available RS-232 connection the author wanted to migrate to an USB based connection type in order to use a regular PC as a terminal.

- **RAM:** In order to store many routing entries additional RAM is necessary as the predecessor thesis already pointed out. An address size of 16 bit theoretically allows addressing 65,536 nodes. If we wanted to store just every single address

in a routing table we already need more than 130kB of RAM if only the target address had to be stored. Realistically the author wanted to store at least 1000 nodes in a routing table.

Type	Name	Size (Byte)
Address	Gateway	2

-

2.2. Hardware Modules

2.2.1. RAM

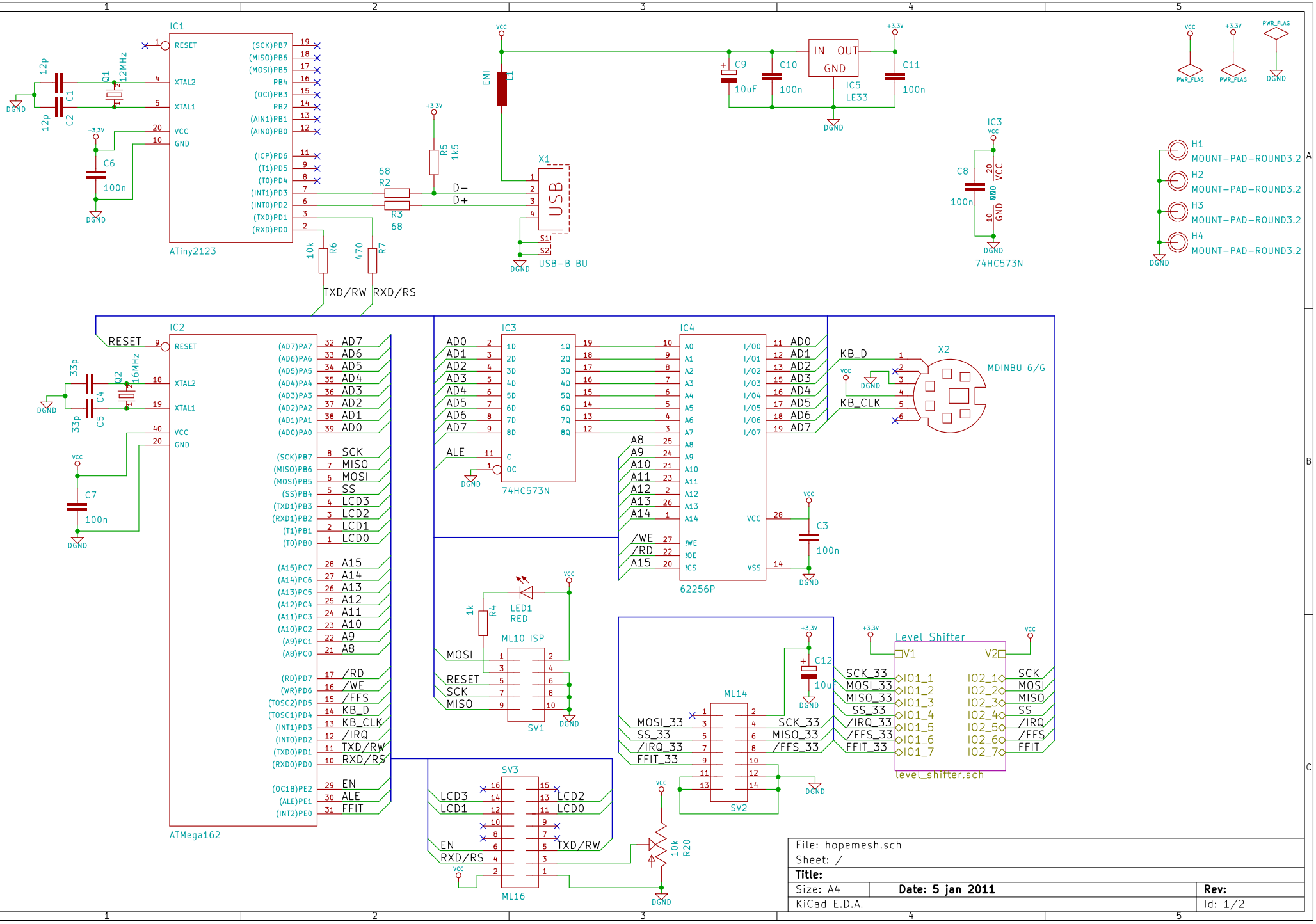
- Harvard architecture
- RAM bus
- Latch

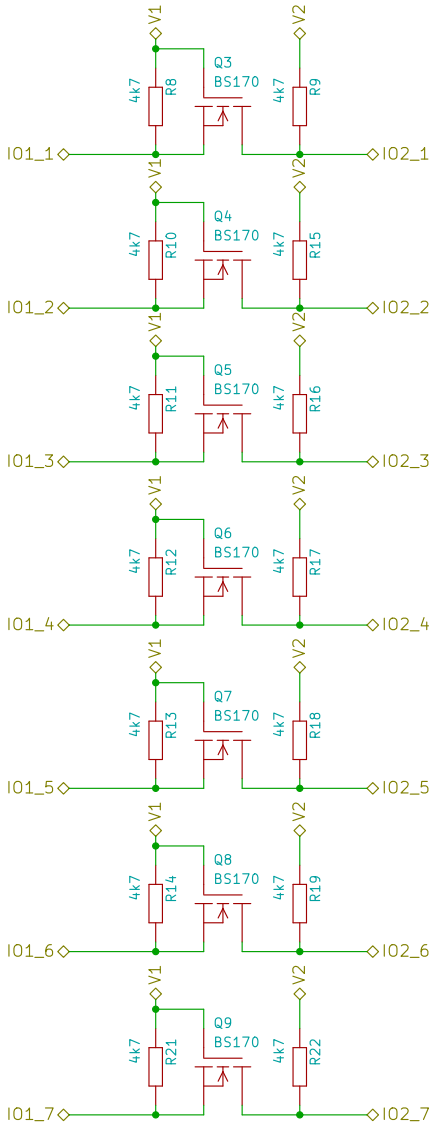
2.2.2. USB Serial Device

2.2.3. RFM12B Radio

2.2.4. Keyboard

2.3. Schematic


IC1
ATiny2123
IC2
ATMega162
IC3
74HC573N
IC4
62256P
IC5
LE33
IC3
74HC573N
X1
USB
USB-B BU
X2
MDINBU 6/G
ML10 ISP
SV1
SV2
SV3
ML14
ML16
Level Shifter
level_shifter.sch
H1
MOUNT-PAD-ROUND3.2
H2
MOUNT-PAD-ROUND3.2
H3
MOUNT-PAD-ROUND3.2
H4
MOUNT-PAD-ROUND3.2
TXD/RW
RXD/RS
File: hopemesh.sch
Sheet: /
Title:
Size: A4
Date: 5 jan 2011
Rev:
KiCad E.D.A.
Id: 1/2



File: level_shifter.sch		
Sheet: /Level Shifter/		
Title:		
Size: A4	**Date: 5 jan 2011**	**Rev:**
KiCad E.D.A.		Id: 2/2

2.4. Printed Circuit Board

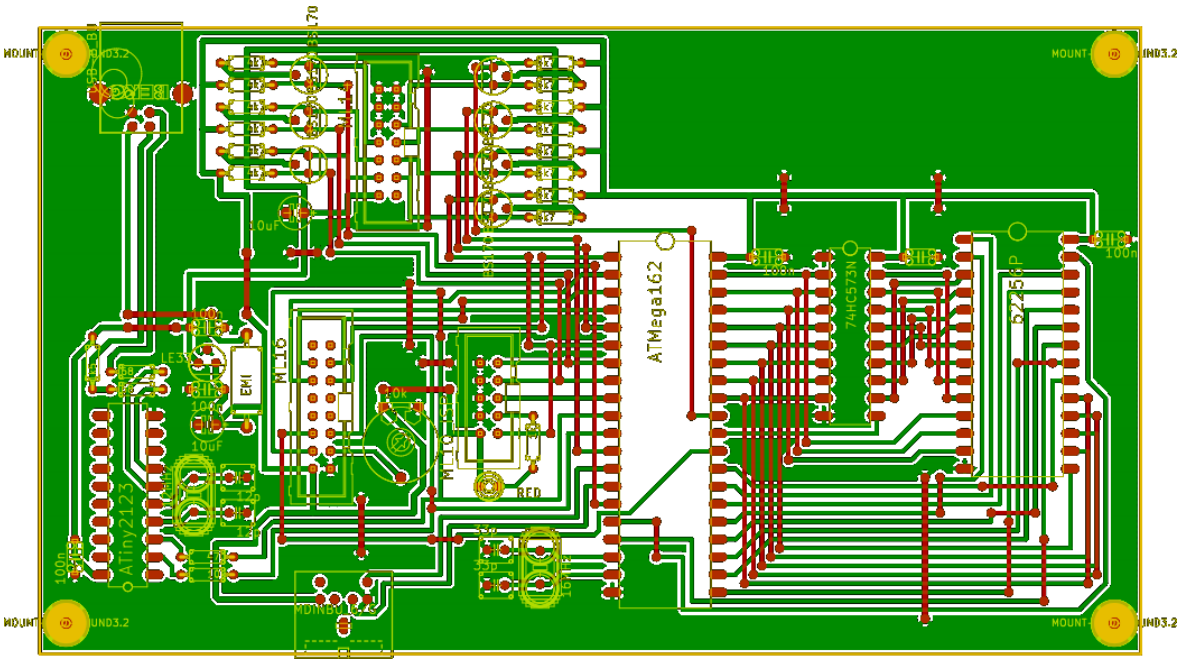


Figure 2.3. 2nd revision PCB layout

In order to able to set up future mesh nodes a reproducable hardware design had to designed. The goal was to be able to produce many mesh nodes and to be able to equip a whole laboratory. One possibility is to manually wire each mesh node. Due to the complexity of the schematic this solution was not acceptable. The author decided to design a printed circuit board (PCB) in order to be able to produce new mesh nodes quickly. The following design requirements were established by the author:

- **One sided PCB:** The PCB was aimed to be manufactured in an uncomplicated environment. Two-sided PCBs allow minimizing the physical size of the device but for research this is not an important requirement. On the other hand two-sided PCBs require additional effort. Through-holes have to be manufactured and eventually the upper side of the PCB has to be laminated in order to prevent shorts.

- **Non-SMD parts:** The author explicitly avoided SMD parts. The goal was to be able to solder the parts manually with commonly available electronic parts.

The actual design of the PCB (Printed Circuit Board) was performed in three iterative phases:

- **Manually wired prototype :** In order to have a proof of concept a first working prototype was constructed by the author manually. This board was not used for the final realization but was used in order to test the external RAM as well as the UART-USB connection.
- **1st revision PCB :** A first revision of the PCB was designed and manufactured. Despite a function node a few design improvements were identified. The trace count and surface mounting the existing resistors were identified as a further improvement.
- **2nd revision PCB :** The final revision of the PCB was designed in smaller dimensions and the design flaws from the first revision were corrected.

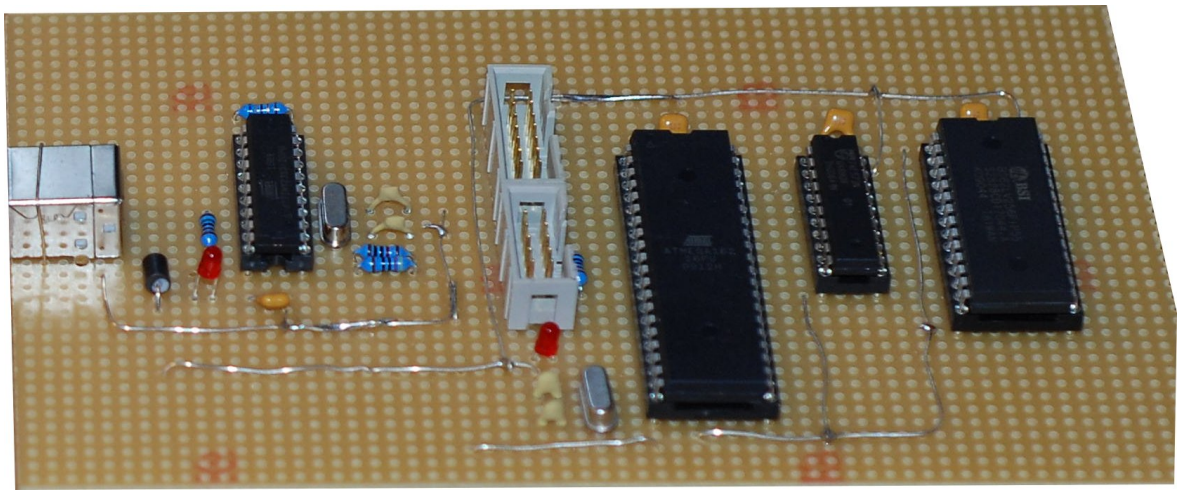


Figure 2.4. Manually wired prototype board

The final version of the PCB was carefully designed to have a logical and effective layout of components. Figure 2.5 shows the zones which include the different hardware modules. The following zones were designed:

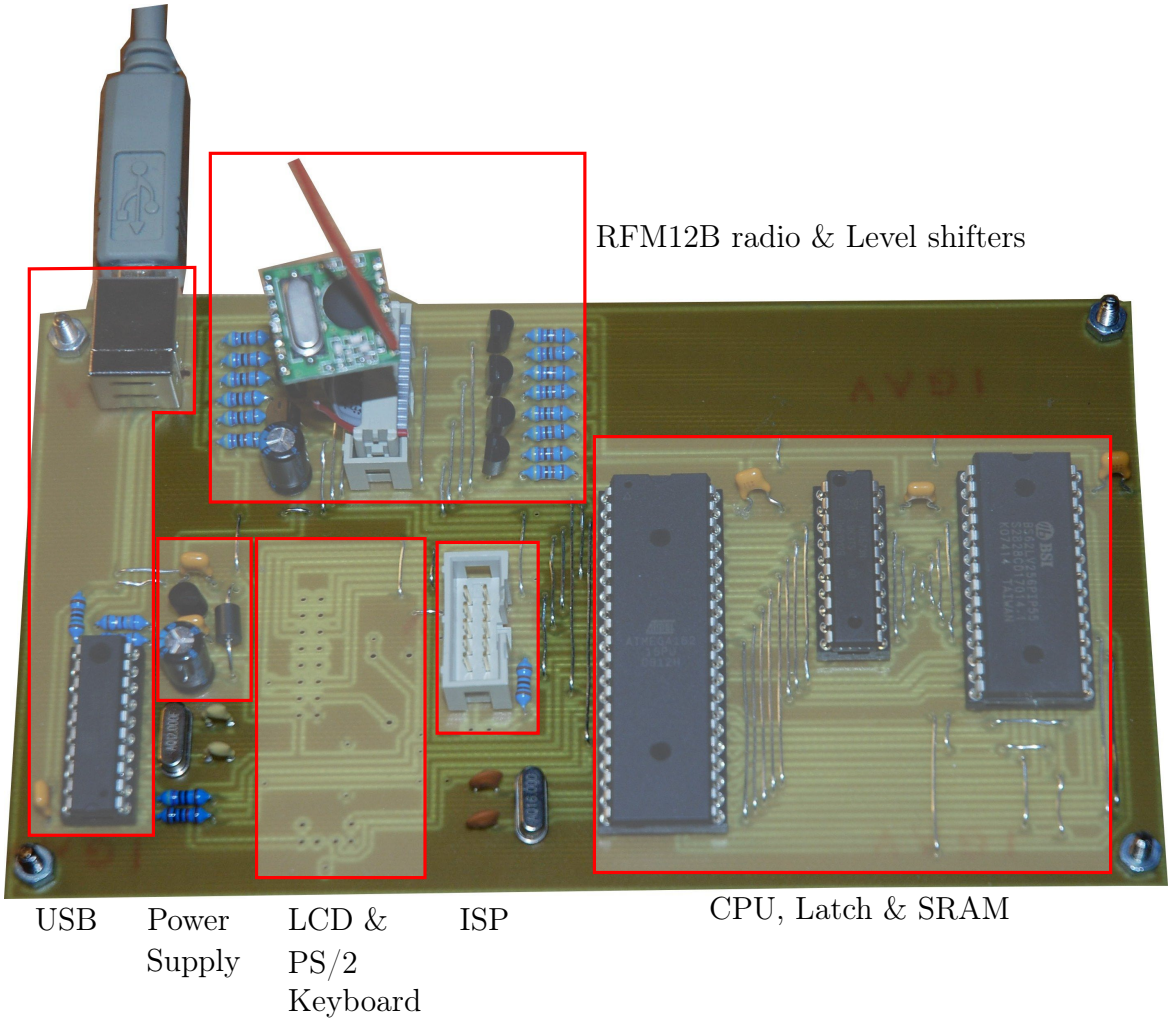


Figure 2.5. 2nd revision PCB areas

- **USB:** The relevant parts and connectors for the USB connection are being placed here. In order to have a comfortable connection to the cable the USB connector was placed in the left upper corner.
- **Power supply:** Right next to the USB zone the PSU parts are placed.
- **RFM12B:** The radio modules as well as the level shifters were placed next to each other.
- **ISP:** The In-System-Programmer connector was placed next to the CPU in order to reduce scattering effects.
- **CPU, Latch & SRAM:** These chips were placed next to each other in order

to reduce the bus trace lengths as much as possible.

Chapter 3

Software Modules

3.1. UART

3.2. SPI

3.3. Watchdog

3.4. Timer

3.5. Shell

3.6. Network Stack

3.7. RFM12 Driver

Chapter 4

Software Algorithms

4.1. Module orchestration

Designing a software system that executes on embedded micro-controllers implies a lot of challenges when many software modules are involved and complexity grows. The conceptually defined modules must be somehow implemented. If the micro-controller lacks an operating system then there is no possibility of using provided abstractions and APIs for module orchestration and execution. Another challenge are limited hardware resources which prevent the deployment of many existing operating system kernels. Basically there are two types of execution models which can be implemented in micro-controllers:

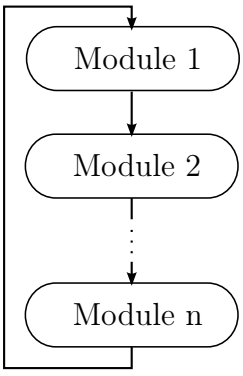


Figure 4.1. Sequential execution model

1. **Sequential execution model:** This type sequentially executes all modules

inside an infinite main loop starting from the first module until the last one. Once the last module ends the execution starts again from the first module.

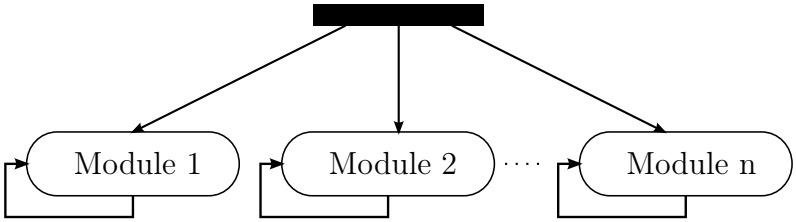


Figure 4.2. Concurrent execution model

2. **Concurrent execution model:** This type executes modules concurrently. Instead of having an infinite main loop that iterates sequentially over all modules the main function only initializes and launches concurrent modules.

4.1.1. Sequential execution

This model does not necessarily needs operating system support or frameworks. It can be simply implemented as a sequence of function calls inside an infinite loop as shown in algorithm 1.

Algorithm 1 Sequential model algorithm

```
while true do
    module_1
    module_2
    ...
    module_n
end while
```

There is one challenge that comes with this type of execution model. That is that only one module can execute at a time due to its sequential nature. If a module i.e. waits for an external resource to provide data it must not block the execution of the main loop until the external resources becomes ready. This would prevent the execution of the other modules. The classic solution to this problem is the introduction of states in modules. Module states can be implemented as classical Finite State Machines [3].

If we take the example from above about waiting for external resources a finite state machine for modules can be modeled as shown in figure 4.3.

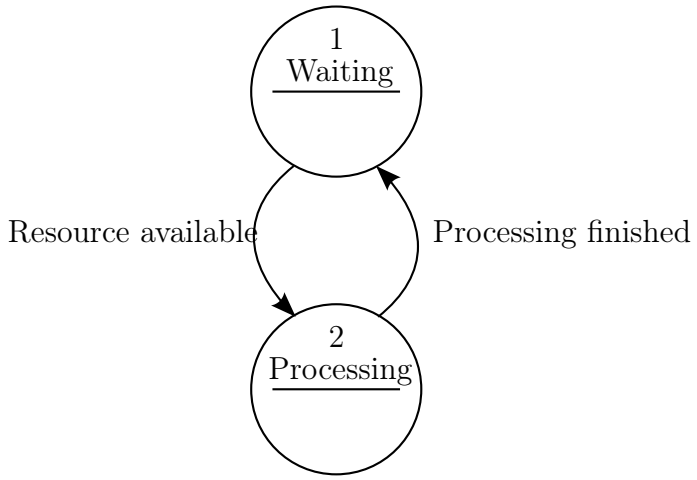


Figure 4.3. State Machine for a module

State machine models can be implemented using `if` or `case` statements which is shown in algorithm 2. The nice side effect of a state machine based implementation is the non-blocking nature of the module execution. Take for instance the execution of state 1 "Waiting" as shown in figure 4.3. The CPU only needs to execute as many instructions as are necessary to check if the awaited resource is available. If the resource is not available the execution returns to the main loop and the next module (together with its state machine) is being executed.

Algorithm 2 State machine algorithm

```
if state is WAITING then
    if resource is available then
        set state to PROCESSING
    else
        exit module
    end if
else if state is PROCESSING then
    process data
    set state to WAITING
end if
```

This implementation emulates a concurrent execution of modules. The context switch between module executions is being done by the modules themselves (using self-interruption) and no external scheduler is involved. This form of concurrent behavior can therefore be described as a non-preemptive or cooperative multi-tasking between modules. The predecessor thesis [2] implementation heavily used the described state machine algorithm although the model theory behind the implementation was not being mentioned in the thesis. Listing 4.1 shows the main function of the predecessor implementation.

Listing 4.1. main loop routine [2]

```
382 while(0x01)
383 {
384         if(uartInterrupt == ON) // got a character from RS232
385 +---- 44 lines:
429
430
431         // --- RECEIVE A DATAGRAM ---
432
433         else if((datagramReceived = datagramReceive(...))
                        && netState > 0)
434 +----182 lines:
616
617
618         else if(helloTime) // prepare periodic Hello message
619 +---- 19 lines:
638
639
640
641         // --- SEND A DATAGRAM ---
642
```

```
643          if(datagramReady && netState > 0)
644 +----  8 lines:
652
653 }
```

A couple of problems arise from the existing implementation. First of all listing 4.1 reveals the following modules:

- UART Module
- Datagram Receiver Module
- Hello Message Sender Module
- Datagram Sender Module

Which module is being executed depends on the state of the main module being represented by the main function. The state of the main module on the other hand depends directly from the state of the submodules. The main module therefore acts more like a controller of the submodules and takes away the responsibility of the submodule's state management. Furthermore the main function is very long and complex (271 lines of code). Therefore the following goals were defined by the author:

- Clear separation of responsibilities between the main loop and the concurrently running modules.
- Simplification of the main loop implementation.

Listing 4.2 shows the new implementation of the main loop. The new implementation makes it very clear which modules are being executed sequentially. Furthermore the main function does not act as a controller but rather leaves the state management in the module's responsibility.

Listing 4.2. main function implementation

```
95 while (true) {
```

```
 96    shell();
 97    batman_thread();
 98    rx_thread();
 99    uart_tx_thread();
100    watchdog();
101    timer_thread();
102 }
```

The next question was how to implement the actual concurrently running modules. One possibility was to reuse the predecessor's methodology and use state machine based implementations. There is a problem though in state machine based implementations and that is the rapidly growing complexity. This problem is called "state explosion problem" and has even a exponential behavior as shown in [4]. The equation 4.1 shows that the number of states is dependent on the number of program locations, the number of used variables and their dimensions.

$$\#states = |\#locations| \cdot \prod_{variable\ x} |dom(x)| \tag{4.1}$$

This equation shows that for instance a program having 10 locations and only 3 boolean variables already has 80 different states. Although this equation might not apply exactly to state machine based implementations it underlines the practical experience of big state-machine based implementations. The alternative to state-machine based applications are thread or process based implementations using the concurrent execution model as shown below.

4.1.2. Concurrent execution

This model requires support from an existing operating system. An existing framework or API provides the necessary abstraction to create new concurrent modules. Each module runs in isolation and can have its own main loop or terminate immediately. In terms of operating systems two abstractions are widely used for concurrently running software modules:

- **Processes**: Processes are usually considered as separately concurrently running programs. Usually each process owns its own memory context and communication with other processes happens through abstractions like pipes or shared memory.

- **Threads**: Threads are concurrently running code parts from the same program. The initial program is considered to run in its own "main thread". Other threads can be started from the main thread. Threads also do run in isolation to each other. Each thread has its own stack. Communication with other threads happens through shared memory provided by static data or the heap.

Processes as well as threads are widely known concepts in classical desktop operating systems. In the area of embedded micro-controllers these concepts also are implemented in many different embedded operating systems:

1. FreeRTOS (http://www.freertos.org)
2. TinyOS (http://www.tinyos.net)
3. Atomthreads (http://http://atomthreads.com)
4. Nut/OS (http://www.ethernut.de/en/firmware/nutos.html)
5. BeRTOS (http://www.bertos.org)

The above solutions have chosen different names for threads or processes (some call them "tasks") but essentially they all share the same concept of the concurrent execution model and will be referred to as concurrent modules from now on. Algorithm 3 shows the pseudo-code that initializes concurrent modules. One can see that in contrast to the sequential execution model the main loop actually does nothing.

Algorithm 3 Concurrent model initialization

start $module_1$

start $module_2$

...

start $module_n$

while true **do**

// no operation

end while

But how does a context switch happen between concurrent modules? Two methodologies exist:

- **Cooperative**: The concurrent modules by themselves return the control to a scheduler which then delegates the control to a different module. Which concurrent module gets control is often based on priorities which are controlled by the scheduler.
- **Preemptive**: Here the concurrent modules do not have control about how and when they get interrupted. It can happen anytime during the execution. Again the context switch between concurrent modules is often handled using priorities in the scheduler.

Nearly all existing solutions have one feature in common. That is that every thread has its own separate stack memory space. This is necessary in order to be able to run the same block of code (for instance a function) in multiple thread instances. On the other hand threads are being executed in the same memory context so sharing data between threads is possible by using the heap or static memory. All of the above mentioned frameworks provide common abstractions which are needed in thread based implementations:

- Semaphores
- Mutexes

- Yielding

In contrast to state machine based or sequential based concurrency thread based implementation can be expressed in very linear algorithms using the above mentioned abstractions. Take for instance the state-machine based algorithm 2. This could be translated into a linear thread-based algorithm as shown in 4.

Algorithm 4 Thread based algorithm

while true **do**

wait for resource mutex

process data

release resource mutex

end while

One can easily see that the thread-based algorithm 4 is much more expressive than the state-machine based algorithm 2.

Together with the necessity of having a scheduler these solutions can be considered as heavy-weight. The scheduler consumes additional CPU cycles and the separate stack memory space per thread consumes additional memory which is very scarce in embedded micro-controller systems.

Although usually a concurrent execution model must be provided in form of an API or an existing kernel there is one exception in the context embedded micro-controllers and that are ISRs (Interrupt Service Routines). Interrupt service routines behave like *preemptive* concurrent modules with highest priority.

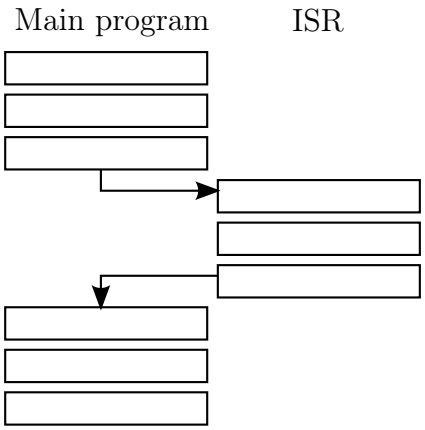


Figure 4.4. Illustration of an Interrupt Service Routine

The ISR interrupts the main program at any time when an external resource triggers an event and executes the service routine. The scheduler in this case is the CPU itself. There is one caveat with ISRs. When one ISR is being executed no other ISR can be triggered. Therefore it is being considered best practice not to perform intense and long running operations in ISRs.

4.1.3. Conclusion

For the implementation of this thesis the following conclusions were drawn:

- Existing solutions supporting the concurrent execution model were considered too heavy-weight for this type of application. Although 32KB of RAM are available the purpose is the support of route storage and network support.
- A sequential execution model was favored instead of the concurrent execution model. On the other hand thread-like linear algorithms are definitely favored instead of state machine based implementations which could lead to a state explosion.

One framework exists which implements the sequential execution model but providing a linear thread-like API being called Protothreads as described in [5]. It is implemented using C macros and expands to switch statements (or to goto statements if the GCC compiler is being used). Instead of consuming a complete stack per thread

the protothread implementation uses only two bytes per (proto)thread. Protothreads actually are stackless and variables initialized on the stack of a protothread function will stay initialized only during the very first call of the protothread.

Algorithm 5 Simple linear algorithm

while true **do**

wait until timer expired

process data

end while

Algorithm 5 shows a very simple linear use case where it waits for an external resource. In this case it waits for the expiration of an external timer by merely watching the timer's state. Since this is a read-only operation no explicit mutual exclusion is needed. This algorithm expressed as a protothread implementation is shown in listing 4.3.

Listing 4.3. linear protothread implementation

```
19 PT_THREAD(test(void))
20 {
21   PT_BEGIN(&pt);
22   PT_WAIT_UNTIL(&pt, timer_ready());
23   process_data();
24   PT_END(&pt);
25 }
```

The implementation of the algorithm is self-describing and corresponds to the APIs known from the concurrent execution model. The expanded version of the listing after the preprocessor stage is seen in 4.4.

Listing 4.4. expanded linear protothread implementation

```
char
test(void)
{
```

```
  // PT_BEGIN
  switch((&pt)->lc) {
    case 0:

      // PT_WAIT_UNTIL
      do {
        (&pt)->lc = 22;
    case 22:
        if(!(timer_ready())) {
          return 0;
        }
      } while(0);

      process_data();
  // PT_END
  };
  (&pt)->lc = 0;
  return 3;
}
```

The expanded version after the preprocessor stage of the implementation looks much more like a state machine based implementation from the sequential execution model. It uses a clever trick called loop unrolling [6] which breaks ups the while statement using the switch statement. This technique is also known as Duff's device as described in [7]. Unfortunately this implementation has one drawback. One cannot (obviously) use switch statements in protothreads. A slightly more efficient implementation using GCC labels circumvents this. Since the context switch is managed by the concurrent modules themselves the behavior can be classified as *cooperative* multitasking.

Due to the lightweight nature of protothreads and the possibility to express algorithms in a linear thread-like fashion this framework was chosen by the author for the

Listing 4.5. Sender route for the UART module [2]

```
void rsSend(uint8_t data)
{
  while( !(UCSRA & (1<<UDRE)));
  UDR = data;
}
```

implementation.

4.2. Ring Buffers

The predecessor thesis [2] used the UART interface in order to communicate with the user and to inform about incoming packets, changes to routes, etc.. As already analyzed in the previous chapter a state machine based sequential concurrent model was used to implement the UART module. There exists one problem with the current implementation.

Listing 4.5 shows that the algorithm examines the UCSRA (USART Control and Status Register A) and blocks infinitely until the UDRE (USART Data Register Empty) bit becomes zero. The execution of all other concurrent modules and the main loop will be blocked until the UART becomes ready to accept data. In this time period no data can be received from the radio. The above mentioned implementation uses the same function for sending strings via the UART interface. For sending the string "hello" via the UART with a speed of 19.2kbps the main loop will be physically blocked for 2.5 milliseconds. In order to improve the implementation the author wanted to accomplish the following goals:

- Refactoring to a non-blocking operation.
- Migration to a concurrent execution model using protothreads.

The Atmega162 micro-processor offers the following ISRs for receiving and sending data via the UART [8]:

- **SIG_USART_RECV**: Is being invoked, when the UDR register contains a new byte received from the UART.

- **SIG_USART_DATA**: Is being invoked, when the UDR register is ready to be filled with a byte to be transmitted via the UART.

So we have the possibility to send or receive data asynchronously from the main loop in the context of a concurrent execution model by using ISRs. Filling the UDR or reading the UDR in the main loop (and thus blocking it) is actually not necessary at all. The main loop can communicate with the ISRs through a receiving and transmitting queue buffer where it writes data to the transmitting queue and reads data from the receiving queue.

Using this sort of communication is known as the "producer-consumer problem". It can be implemented using a FIFO buffer. The Linux kernel ([9] chapter 5.7.1) as well as (embedded) DSP micro-controllers [10] use a very elegant FIFO-algorithm by providing a lock-free buffer being called "circular buffer" or "ring buffer".

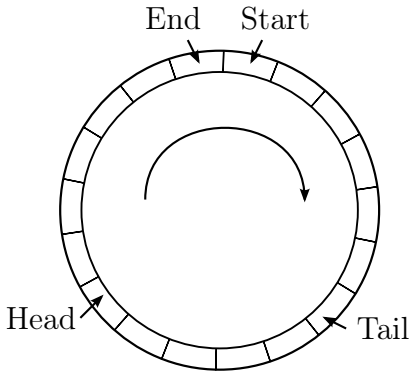


Figure 4.5. Illustration of a ring buffer

Figure 4.5 shows the basic principle of the algorithm. A circular buffer is defined by the following four pointers:

- **Start:** This pointer defines the beginning of the buffer in memory. This pointer is static.
- **End:** This pointer defines the end of the buffer in memory. It can also be expressed as the maximum length of the buffer. This pointer is static.
- **Head:** The head pointer is being changed dynamically by the producer. Whenever the producer wants to write data in the buffer the head pointer is increased

and the corresponding memory filled. If the head points to the same address as the tail pointer the buffer is full or empty.

- **Tail:** The tail pointer is being changed dynamically by the consumer. Whenever the consumer wants to read data from the buffer the tail pointer is increased and the corresponding memory cleared. If the tail points to the same address as the head pointer the buffer is full or empty.

In order to distinguish whether the buffer is full or empty an additional size variable was implemented. The biggest advantage of the presented algorithm is the possibility to write and read data in a lock-free fashion. A consumer thread does not need to wait for a mutual exclusion on the buffer since the consumer thread is the only instance manipulating the tail pointer. The same applies for the producer being the only instance manipulating the head pointer.

The complete listing of the ring-buffer implementation can be seen in appendix A in the file `src/ringbuf.c`. There are two functions provided:

- **ringbuf_add:** This function is being called by the producer. The function immediately returns `true` if a byte could be written to the the buffer or `false` if the buffer is full.

- **ringbuf_remove:** This function is being called by the consumer. The function immediately returns `true` if a byte could read from the buffer or `false` if the buffer is empty.

The important nature of the above mentioned functions is that they are non-blocking because they return immediately. These functions could therefore be called from protothreads. A producer protothread running in the context of the main loop can write data like presented in listing 4.6. The consumer of this data is the SIG_USART_DATA ISR as presented in listing 4.7.

Listing 4.6. Producer writing data

```
PT_THREAD(producer(uint8_t data))
```

```
{
    PT_BEGIN(&pt);
    PT_WAIT_UNTIL(&pt, ringbuf_add(buf, data));
    PT_END(&pt);
}
```

Listing 4.7. Consumer reading data

```
ISR(SIG_USART_DATA)
{
  uint8_t c;
  if (ringbuf_remove(buf, &c)) {
    UDR = c;
  }
}
```

Instead of *physically* blocking the algorithm expressed in listing 4.6 only *logically* blocks the protothread. If the buffer is full a context-switch back to the main loop is performed. The main loop sequentially executes all other concurrent modules and returns to the protothread which then again tries to add data into the ring buffer.

4.3. Half-Duplex Radio Access (Petri Net)

The predecessor implementation used an identical (physically) blocking implementation in order to send or receive data via the RFM12B hardware module. Listing 4.8 shows the algorithm used for sending data.

Listing 4.8. Sender routine for the RFM12B hardware module [2]

```
void rfTx(uint8_t data)
{
        while(WAIT_NIRQ_LOW());
        rfCmd(0xB800 + data);
}
```

This implementation physically blocks the main loop the same way as the UART algorithm shown in listing 4.5. In this case the algorithm does not wait for the status of an internal register to send data but rather waits for the external nIRQ pin from the RFM12B hardware module to go low. The official "RF12B programming guide" [11] also proposes a physically blocking algorithm.

The author wanted to improve the algorithm in a similar fashion as the UART algorithm. The nIRQ pin of the RFM12B was connected to the INT0 pin of the ATMega162 micro-processor allowing to execute the SIG_INTERRUPT0 interrupt service routine asynchronously. But it turned out that the implementation could not be reused at all. The RFM12B radio hardware imposes the following algorithmic challenges for the driver implementation:

- **Single interrupt request for multiple events:** The RFM12 radio module uses only one nIRQ pin in order to generate an interrupt for the following events [12]:
  - The TX register is ready to receive the next byte (RGIT)
  - The RX FIFO has received the preprogrammed amount of bits (FFIT)

  The state management has to be implemented in software otherwise the current state of operation (sending or receiving) is undefined.

- **Half-Duplex operation:** The RFM12 radio module only allows either to receive or to send data at a time but not simultaneously.

The author abstracted the operation of the RFM12B driver algorithm as a (proto)thread. Interestingly enough the thread has a state modeled as a state machine depending whether it receives or sends data. The following states are valid:

- **RX:** This is the receiving state. The thread (logically) blocks until a complete packet has been received. Whether a packet is complete or not depends on the upper network stack layers.

- **TX:** This is the sending state. The thread (logically) blocks until a complete packet has been sent. Again the upper network stack layers decide whether the transmission is complete or not.

The abstract algorithm is shown in 6. The question is who sets the actual state of the radio driver. Receiving data is *non-deterministic*. A packet can arrive at any time and thus the invocation of the SIG_INTERRUPT0 interrupt service routine. Therefore the algorithm sets the RX state as the *default* state for the radio thread.

Sending data on the other hand is *deterministic*. When a user hits the Enter key via the UART module a packet can be constructed. A 3rd party thread has to request the control over the radio module and occupy it until the packet has been fully transmitted. The author realized that this is a concurrency problem between two threads and a single resource:

- **Sender Thread:** The sender thread wants to acquire the control over the radio module until the transmission of a packet is complete.
- **Radio Thread:** The radio thread also wants to acquire the control over the radio module until the packet reception is complete.
- **Single resource:** The external resource in this case is the radio module. Only the receiving radio driver thread or the transmitting sender thread can own the radio hardware resource at a time.

Algorithm 6 RFM12B driver thread algorithm

```
while true do
  if state is RX then
    receive data
  else if state is TX then
    send data
  end if
  set state to RX
end while
```

In classical multi-threaded algorithms this problem can be solved using mutual exclusion. Modeling such an algorithm can be done using petri nets as shown in figure 4.6.

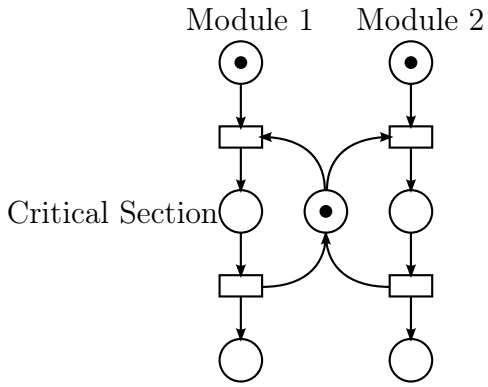


Figure 4.6. Mutual exclusion model using a petri net

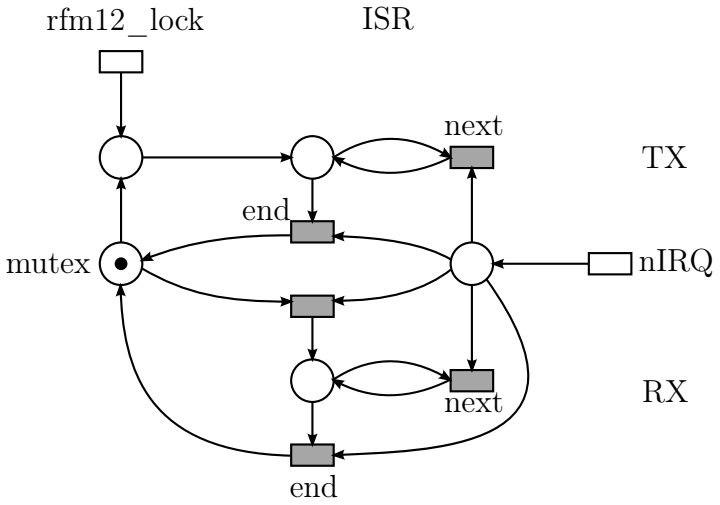


Figure 4.7. Half duplex algorithm modeled as a petri net

Chapter 5

Network Stack

5.1. Reference model

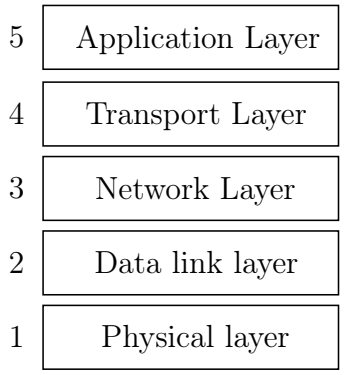


Figure 5.1. Tannenbaum hybrid reference model [1]

Notes:

- Explain why the tannenbaum model was choosen as the reference model.

- Explain each layer and its purposes.

- Explain the division of the data link layer into the two sublayers MAC and LLC.

5.2. Reference implementation

Notes:

- The implementation was heavily inspired by a project available at [13].

Drawbacks:

- Unfortunately the project is only partly finished. Only the PHY and MAC layers are working.
- It is based on a sequential execution model using state machines.

Pros:

- Division of each network layer in a separate source file.
- Communication between the layers through callbacks.

5.3. Layer 1: Physical

The physical layer is implemented using a wireless technology by using the capabilities of the RFM12B low cost ISM band transceiver. This transceiver offers frequency modulation (FSK). Unfortunately it does not offer additional modulations like amplitude modulation (AM) or phase modulation (PSK) so advanced modulation techniques like QPSK or QAM are note possible.

The transceiver operates in one of the three following frequencies:

- **433MHz:** This frequency range is called the "ISM-Band Region 1". According to ITU "Region 1" includes Europe so operation on this band is permitted. But this frequency range is also occupied by amateur radio stations which have primary status on these frequencies. ISM based applications only have a secondary status on this band so this operation frequency was avoided by the author.

- **868MHz:** This frequency range is called the "SRD-Band Europe" and does not collide with amateur radio. Furthermore this band is reserved for low powered devices so collisions in near field applications (<1km) are reduced. The author therefore decided to use transceivers for this frequency range.

- **915MHz:** This frequency range is called the "ISM-Band Region 2" and according

to ITU can only be used in Americas and Greenland. Operation on this frequency in Europe is not allowed.

The typical output power according to the data sheet is 4dBm which according to formula 5.2 equals approx. 2.5mW.

$$P[mW] = 10^{(L_{dBm}/10)} \tag{5.1}$$

The maximum effective radiated power (ERP) is regulated specifically in each country but commonly on the 868MHz SRD band the maximum allowed ERP must not exceed 25mW ERP.

$$ERP[mW] = 10^{((g-2.15)/10)} \times P \times 1000 \tag{5.2}$$

By using a simple quarter wavelength wire (which approximately resembles a dipole antenna having a gain of 2.15 dBi) the ERP power also equals 2.5mW which has a safe margin to the limit.

Furthermore this transceiver can only operate in half-duplex mode. Special care therefore has to be taken when writing device drivers for this module. The algorithmic solution to this problem was already presented in chapter 4.3..

5.4. Layer 2a: MAC Layer

The MAC layer for the thesis implementation follows the Tannenbaum [1] model for dynamic channel allocation with the following key assumptions and exceptions:

- **Station Model:** The independent stations are represented by single mesh nodes in the network.
- **Single Channel Assumption:** The single channel is represented by the common frequency on which the mesh nodes transmit and receive data.
- **Collision Assumption:** This assumption unfortunately does not fully apply to the used RFM12B modules. Although collisions can happen the module does not

provide any facility to detect frame collisions on the carrier since it operates in half-duplex mode only. Therefore Tannenbaum's requirement to resend collided frames could not implemented.

- **Continuous Time:** The frame transmission can indeed begin at any time so this assumption is fulfilled.

- **Carrier Sense:** Using the RSSI (Radio Signal Strength Indicator) command being provided by the RFM12B module the MAC layer can detect whether the carrier is free or occupied. The requirement not to send any data until the carrier is free was implemented by the author as shown in algorithm 7.

Algorithm 7 Implemented MAC carrier sense protocol

```
wait until rfm12 is locked
if carrier sense is configured then
    wait until carrier is free
end if
enable transceiver
enable interrupts
```

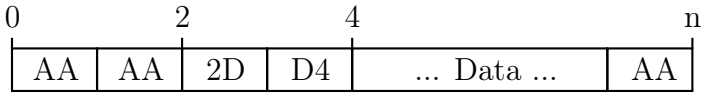


Figure 5.2. MAC frame format

The actual MAC frame format can be seen in figure 5.2. The frame consists of the following four parts:

- **Preamble:** Two bytes containing the value 0xAA are being sent. The reason for this pattern is the bit representation which consists only of alternating 0 and 1 values. This helps the receiving PLL circuit to lock in to the correct frequency in order to minimize bit errors for the sync pattern recognition.

- **Sync pattern:** The sync pattern 0x2DD4 is programmed into the hardware of the RFM12B module. Only after the module recognizes this pattern it will fill its internal receiver FIFO with further data.

- **Data:** The data carries the actual payload for transmission. Since this is a frame based transmission (no length field is specified) the data must not contain data with 0xAA values. An appropriate code has to be chosen by the upper network layers.

- **Postamble:** The end of the frame is marked by the single byte value 0xAA. This is the reason why the data part must not contain this value.

One can see that the implemented MAC frame format does not include any error checking. The algorithm will simply stream bytes to or from the upper network layers until the postamble byte 0xAA is being detected. Only then the MAC layer assumes that the frame reception or transmission is complete.

5.5. Layer 2b: Logical Link Control

The logical link control layer provides the virtual data path for the upper network layers. The implementation in this thesis follows Tannenbaum's [1] category of an unacknowledged connectionless service. According to Tannenbaum's data link layer design principles the following functions were implemented in the LLC layer:

- **Service interface for the network layer:** In contrast to the stream-oriented interface between the LLC layer and the MAC layer the interface between the LLC and upper network layers is packet-oriented. However in this implementation no additional algorithmic efforts were done in order to split up packets in separate frames. For simplicity each packet is transmitted in one frame.

- **Transmission error handling:** The transmission error handling was implemented using an error correction code (Hamming) and an error detecting code (CRC-16).

- **Data flow:** No flow control algorithms were implemented due to its complexity and the different focus in this thesis which is the routing algorithm. Therefore dropped frames (in this case packets) will not be discovered and retransmitted.

5.5.1. Error correction and detection

Due to the nature of a wireless connection which is a highly unreliable channel an error correcting as well as an error detecting code were introduced:

1. *Hamming code:* This error correcting code was used to provide data to the MAC frame. This decision was inherited from the reference implementation [13]. The advantage is that the hamming code produces data which conforms to the requirements set up in the MAC layer by not providing any 0xAA byte values.

2. *CRC-16 checksum:* After decoding or encoding the hamming byte stream an additional CRC-16 based error detecting checksum was implemented for the payload provided by the upper network layers.

Error correction

The implemented error correction code is an extended 8,4 hamming code. A 4 bit data nibble is redundantly encoded into an 8 bit code byte which nicely fit into a byte stream required by the MAC layer. The classical hamming code introduces parity bits p_i at the 2^ith position of the final code word. According to formula 5.3 by having $k = 3$ parity bits we can encode an $n = 4$ bits long data nibble into an $N = k + n = 4 + 3 = 7$ bits long code word.

$$n = 2^k - k - 1 \tag{5.3}$$

where

$$n = \text{data size in bits}$$

$$k = \text{amount of parity bits}$$

Since a 7 bit long code word does not fit nicely into an 8 bit long byte we could either fill the remaining bit with random data or use it as an additional final parity bit p_f which calculates the parity of the previous 7 bits. The following variables are now available for the code word:

$$\text{data word} = d_3, d_2, d_1, d_0$$
$$\text{hamming parity bits} = p_2, p_1, p_0$$
$$\text{final parity bit} = p_f$$

The data word has the following format:

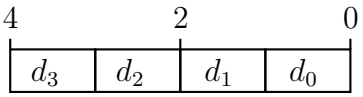
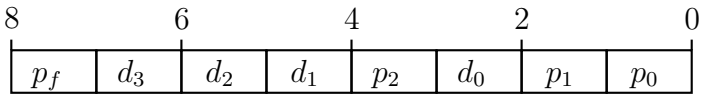


Figure 5.3. Input data word format

The final code word according to the "classical" hamming algorithm has the following format:



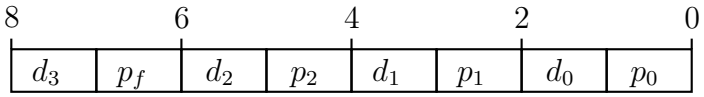
where

$$p_f = p_0 \oplus d_3 \oplus d_2 \oplus d_1 \oplus p_2 \oplus d_0 \oplus p_1 \oplus p_0$$
$$p_2 = d_3 \oplus d_2 \oplus d_1$$
$$p_1 = d_3 \oplus d_2 \oplus d_0$$
$$p_0 = d_3 \oplus d_1 \oplus d_0$$

Figure 5.4. Classical Hamming 8,4 code word format

One could finish further investigation here and just use the classical 8,4 hamming

coding. In comparison the 7,4 hamming code the hamming distance is increased from 3 to 4 and two error bits can be detected and corrected if one data byte is encoded as two separate 4 bit long nibbles resulting as a two byte hamming stream. The author decided to use another hamming encoding discovered in [13] which is also used and standardized in the transmission of teletext for television. The European Telecommunication Standard (ETS) specifies the following hamming encoding in the context of the teletext specification [14]:



where

$$p_f = 1 \oplus p_0 \oplus d_3 \oplus d_2 \oplus d_1 \oplus p_2 \oplus d_0 \oplus p_1 \oplus p_0$$

$$p_2 = 1 \oplus d_2 \oplus d_1 \oplus d_0$$

$$p_1 = 1 \oplus d_3 \oplus d_1 \oplus d_0$$

$$p_0 = 1 \oplus d_3 \oplus d_2 \oplus d_0$$

Figure 5.5. ETS specified 8,4 hamming coding word

The major difference between the two codes is when encoding 0xA and 0xF values as shown in table 5.1. The ETS code ensures that the final code sent via the physical device does not produce continuous streams of 1 or 0 bits. The consequence for radio transmission is better stability for the receiver's PLL which minimizes errors during reception. The author therefore decided to reuse the ETS hamming code for the implementation.

Data	Classical code	ETS code
0000	00000000	00010101
1111	11111111	11101010

Table 5.1. Difference between the classical and ETS hamming code

Error detection

5.5.2. Packet format

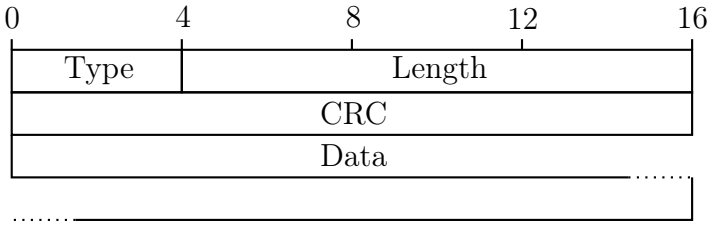


Figure 5.6. LLC packet format

5.6. Layer 3: Batman Routing

Notes:

- elaborate on tannenbaum <-> my implementation

- elobarote which packet formats are necessary and why

5.6.1. OGM packet format

Notes:

- explain fields

- explain when ogms are being rebroadcasted

- explain when an entry to the routing table is added

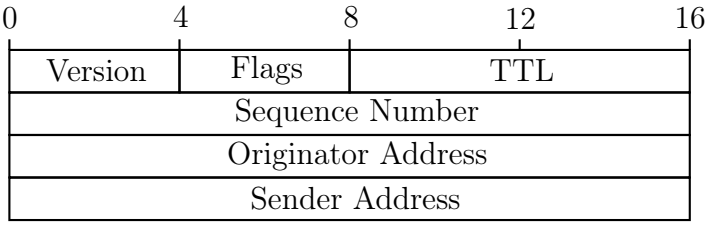


Figure 5.7. OGM packet format

5.6.2. Unicast packet format

Notes:

- explain fields

- explain when unicasts are being rebroadcasted

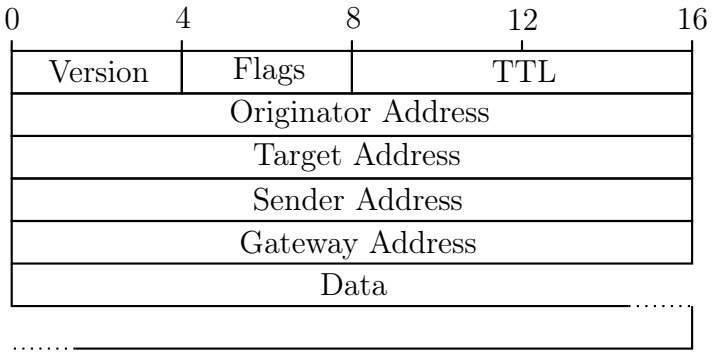


Figure 5.8. Unicast packet format

5.6.3. Routing

Notes:

- explain routing table format

- show how many nodes can be stored in the routing table with the available RAM - eloborate when routing entries are added based on OGM messages - elaborate when routing entries are deleted based on the purging timeout

5.7. Layer 4: Transport

Notes:

- explain the transport frame format

- explain why this layer was essentially ignored.

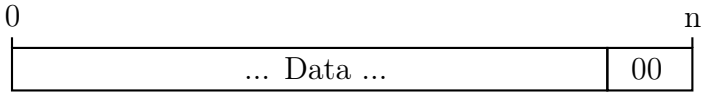


Figure 5.9. Transport frame format

5.8. Layer 5: Application

Notes:

Expose the shell and the rx thread as the application part.

Chapter 6

Research

6.1. Simulations

6.1.1. Shell

6.1.2. Routing

6.1.3. Radio Transmission

6.2. Mesh evaluation

6.3. Results

Chapter 7

Conclusion

7.1. Open issues

Notes:

- Sequence numbers are ignored in the batman routing algorithm

- The transport layer is incomplete

- The MAC multiple access protocol can be much further improved

- The LLC layer does not split packets into frames and does not provide any means of flow control

Appendix A

CD content

1. **src** — The source files for the hopemesh implementation

    - **ringbuf.c** — The ringbuffer implementation

Bibliography

[1] Andrew S. Tanenbaum. *Computer Networks*. Prentice Hall, 2003.

[2] Marek Korniowski. *Projekt odpornej na awarie sieci komputerowej z transmisją danych w pasmach nielicencjonowanych*. 2009.

[3] Taylor L. Booth. *Sequential Machines and Automata Theory (1st ed.)*. John Wiley & Sons Inc, 1967.

[4] Joost-Pieter Katoen. The state explosion problem, 2008. `http://www-i2.informatik.rwth-aachen.de/i2/fileadmin/user_upload/documents/MC08/mc_lec5a.pdf`.

[5] Adam Dunkels, Oliver Schmidt, Thiemo Voigt, and Muneeb Ali. Protothreads: Simplifying event-driven programming of memory-constrained embedded systems. 2006.

[6] Michael Abrash. *Graphics Programming Black Book*. 1997.

[7] Tom Duff. Tom duff on duff's device, 1988. `http://www.lysator.liu.se/c/duffs-device.html`.

[8] Atmel. *Datasheet: ATmega 162*. Atmel, 2009.

[9] Jonathan Corbet, Greg Kroah-Hartman, and Alessandro Rubini. *Linux Device Drivers, 3rd Edition*. O'Reilly, 2005.

[10] Randy Restle. Circular buffer in second generation dsps. 1992.

[11] *RF12B programming guide*. HOPERF, 2011.

[12] Silicon Labs. *Datasheet: Si4421 Universal ISM Band FSK Transceiver*. Silicon Labs, 2008.

[13] Manuel Stahl. Rfm12 protokoll stack, 2008. `http://www.mikrocontroller.net/articles/RFM12_Protokoll_Stack`.

[14] ETSI. *Enhanced Teletext specification*. European Telecommunications Standards Institute, 1997.