



UNIVERSITÄT KARLSRUHE (TH) - FORSCHUNGSUNIVERSITÄT  
FAKULTÄT FÜR ELEKTRO- UND INFORMATIONSTECHNIK  
INSTITUT FÜR BIOMEDIZINISCHE TECHNIK

## DIPLOMARBEIT

Entwurf und Implementierung eines kabellosen Sensornetzes  
zur Überwachung von Patienten bei einem  
Massenanfall von Verletzten (MANV)

vorgelegt von	cand. inform. Marcel Noe
Betreuer	Prof. Dr. Armin Bolz Prof. Dr. Rüdiger Dillmann Dr.-Ing. Marc Jäger
Abgabetermin	01.11.2010



**Eidesstattliche Erklärung**

Hiermit erkläre ich an Eides Statt, dass ich die vorliegende Diplomarbeit selbständig und ohne unzulässige fremde Hilfsmittel angefertigt habe. Die verwendeten Literaturquellen sind im Literaturverzeichnis vollständig angegeben. Die Arbeit wurde in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde zur Erlangung eines akademischen Grades vorgelegt.

Karlsruhe, 31.10.2010



# Vorwort

Diese Arbeit entstand am..... in Koopeartion mit... blabla

Noch was zum Titel:

Es ist oft sinnvoll, zunächst einen vorläufigen Arbeitstitel zu formulieren. Mit ihm legen Sie für sich fest, was Sie beschreiben wollen. Der endgültige Titel sollte einerseits so kurz wie möglich sein, andererseits aber auch möglichst viele Informationen über den Gegenstand der Arbeit enthalten. Beachten Sie, daß die meisten Leser der wissenschaftlichen Zeitschrift, in der Sie Ihre Arbeit veröffentlichen wollen, nur deren Titel lesen. Der Titel soll den Leser kurz und präzise über den Inhalt der Arbeit informieren. Abkürzungen sollten vermieden werden. Aus dem Titel muß ersichtlich sein, ob es sich um eine experimentelle oder um eine theoretische Arbeit handelt. Sie sollten viel Mühe darauf verwenden, den treffenden Titel zu wählen. Ich empfehle, zunächst die Wörter aufzuschreiben, die Ihrer Meinung nach in dem Titel unbedingt vorkommen müssen, um den Inhalt zu charakterisieren. Dann sollten Sie diese Wörter geschickt zu einem Titel zusammenfügen. Beachten Sie aber immer, daß der Titel auch nicht zu lang sein darf.



# Danksagung

An dieser Stelle möchte ich den Personen danken, ohne die diese Arbeit so nicht entstanden und auch nicht möglich gewesen wäre. Ein herzliches Dankeschön gilt...

- ...
- ...
- ...
- ...
- ...
- ...

Die Danksagung ist ein wichtiger Teil der Arbeit. Hier sollten Sie sich bei all denen bedanken, die Ihnen bei den beschriebenen Forschungen behilflich waren. Es ist zwingend erforderlich, daß in der Danksagung steht, welche Institutionen Ihnen evtl. Daten kostenlos zur Verfügung gestellt haben und von welchen Institutionen Ihre Arbeit finanziert wurde. Allgemein ist zu sagen, daß man in der Danksagung nicht geizen sollte. Durch das Erwähnen von Hilfen, die man erhalten hat, kann man sich Türen öffnen, die später eventuell von großem Nutzen sein können. Ein weiterer Tip: Schicken Sie jedem/jeder, der/die in der Danksagung erwähnt wird, ein Exemplar Ihrer Arbeit (am besten mit Widmung). Er/sie wird sich freuen.





# Abstract

... Die Zusammenfassung („Abstract“) ist nach dem Titel der zweitwichtigste Bestandteil einer wissenschaftlichen Arbeit. Sie sollten deshalb für die Zusammenfassung, ebenso wie für den Titel, besonders viel Mühe und Zeit verwenden, da die gesamte wissenschaftliche Arbeit nur von sehr wenigen Wissenschaftlern gelesen wird, die Zusammenfassung aber von vielen. Aus der Zusammenfassung muß hervorgehen, wovon die Arbeit handelt, worauf sie aufbaut, und vor allen Dingen, welche neuen Erkenntnisse gewonnen wurden. Die wichtigsten Ergebnisse der Arbeit müssen kurz und präzise aufgezählt werden. Es genügt nicht zu schreiben, daß dies und jenes in der Arbeit behandelt werden. Wichtig ist, daß die „harten Fakten“, welche sich aus den Untersuchungen ergeben haben, aufgelistet sind. Handelt es sich um eine theoretische Arbeit, dann müssen Sie erwähnen, von welchen Gleichungen Sie ausgegangen sind und welche Näherungen Sie verwendet haben; bei einer experimentellen Arbeit müssen Sie erwähnen, welche Experimente Sie durchgeführt haben und eventuell auch, welche Auswertungsmethoden (falls nicht Standardmethoden) Sie verwendet haben. Beachten Sie, daß Ihre Arbeit von Wissenschaftlern unterschiedlicher Herkunft und Ausbildung gelesen wird. Bedenken Sie, daß sich auch Wissenschaftler für Ihre Arbeit interessieren können, die aus benachbarten Disziplinen stammen und nicht mit dem von Ihnen verwendeten wissenschaftlichen „Jargon“ vertraut sind, oder solche, welche die in Ihrem Fach üblichen Abkürzungen nicht kennen. Deshalb soll die Zusammenfassung für alle (natur-)wissenschaftlich gebildeten Leser verständlich sein. Das bedingt, daß eventuell benutzte Abkürzungen erklärt werden müssen, und daß nur solche Begriffe vorkommen dürfen, die ein „normaler“ Wissenschaftler üblicherweise kennt oder die er notfalls in einem Lexikon nachschlagen kann. Die Zusammenfassung sollte keine Literaturhinweise enthalten. Die Zusammenfassung ist ein selbständiger Teil der Arbeit. Das bedeutet, daß die in der Zusammenfassung erklärten Abkürzungen im Hauptteil noch einmal erklärt werden

## VIII

müssen. Einerseits darf die Zusammenfassung nicht zu lang sein (max eine Seite), andererseits muß sie aber auch alle wichtigen Informationen über Ihre Untersuchungen enthalten. Auf präzise Formulierungen ist größten Wert zu legen.

# Inhaltsverzeichnis

Abbildungsverzeichnis	XI
Tabellenverzeichnis	XIII
<b>1 Einleitung</b>	<b>1</b>
1.1 Motivation der Arbeit . . . . .	1
1.2 Aufgaben und Ziele der Arbeit . . . . .	1
1.3 Gliederung und Vorgehensweise der Arbeit . . . . .	1
<b>2 Stand der Technik</b>	<b>3</b>
<b>3 Grundlagen</b>	<b>5</b>
3.1 Kabellose Übertragungsprotokolle . . . . .	5
3.1.1 Einführung . . . . .	5
3.1.2 DECT . . . . .	5
3.1.3 GSM/UMTS . . . . .	6
3.1.4 WLAN . . . . .	6
3.1.5 Übersicht . . . . .	6
3.1.6 WPAN: Wireless Personal Area Networks . . . . .	9
3.1.7 Weitere Protokolle . . . . .	14
3.1.8 Diskussion . . . . .	14
3.2 Der Analog Devices ADuC702X Mikrocontroller . . . . .	14
3.3 Java . . . . .	14
3.4 Corba . . . . .	14
<b>4 Fortschritt der Arbeit</b>	<b>15</b>
<b>5 Praktische Realisierung des Sensornetzes</b>	<b>17</b>
5.1 Entwurf . . . . .	17

5.1.1	Hardware . . . . .	17
5.1.2	Firmware . . . . .	18
5.1.3	Software . . . . .	20
5.2	Implementierung . . . . .	22
5.2.1	Hardware . . . . .	22
5.2.2	Firmware . . . . .	22
5.2.3	Software . . . . .	22
<b>6</b>	<b>Ergebnisse</b>	<b>23</b>
6.1	Baselinewandering . . . . .	23
6.1.1	Messungen unter verschiedenen Bedingungen . . . . .	23
6.1.2	Vergleichende Messung mit Referenzgerät . . . . .	23
6.2	HRV-Variation . . . . .	23
6.2.1	Messungen unter verschiedenen Bedingungen . . . . .	23
6.2.2	Vergleichende Messung mit Referenzgerät . . . . .	23
6.3	QRS-Komplexe . . . . .	24
6.3.1	Messungen unter verschiedenen Bedingungen . . . . .	24
6.3.2	Vergleichende Messung mit Referenzgerät . . . . .	24
6.4	Vergleiche der Verfahren zueinander . . . . .	24
<b>7</b>	<b>Diskussion</b>	<b>25</b>
7.1	Baselinewandering . . . . .	25
7.2	HRV-Variation . . . . .	25
7.3	QRS-Komplexe . . . . .	25
7.4	Vergleich der Verfahren zueinander . . . . .	25
<b>8</b>	<b>Zusammenfassung und Ausblick</b>	<b>27</b>
	<b>Glossar</b>	<b>29</b>
	<b>Literaturverzeichnis</b>	<b>30</b>

# Abbildungsverzeichnis



# Tabellenverzeichnis





# Kapitel 1

## Einleitung

### 1.1 Motivation der Arbeit

...

### 1.2 Aufgaben und Ziele der Arbeit

...

### 1.3 Gliederung und Vorgehensweise der Arbeit

...



# Kapitel 2

## Stand der Technik

Standardverfahren der Atmungsdetektion mit Nachteilen, Problemen etc. aufzeigen...



# Kapitel 3

## Grundlagen

### 3.1 Kabellose Übertragungsprotokolle

#### 3.1.1 Einführung

In diesem Abschnitt werden die gängigsten Funkprotokolle kurz vorgestellt. Insbesondere wird erläutert, inwieweit das entsprechende Protokoll als Grundlage für das zu entwickelnde Sensornetz geeignet ist.

Mit Ausnahme von DECT und GSM bzw. UMTS ist diesen Protokollen gemein, dass sie sich alle im ISM-Band befinden.

#### 3.1.2 DECT

Bei DECT („Digital Enhanced Cordless Telecommunications“) handelt es sich um einen Standard, der vor allem zur Anbindung von Schnurlostelefonen an eine Basisstation gedacht ist<sup>1</sup>.

In Europa wird ein eigenes Frequenzband im Bereich von 1800 bis 1900 MHz verwendet, in dem 10 Kanäle zur Verfügung stehen. Pro Kanal können maximal 32kbit Nutzdaten pro Sekunde übertragen werden. Die maximal zulässige Sendeleistung beträgt 250mW, womit eine Reichweite von ca. 30-50 Metern in Gebäuden und ca. 300m im Freien realisiert werden kann. Jede Basisstation kann bis zu 6 Geräte anbinden.

Beim Einsatz außerhalb Europas muss bedacht werden, dass die Verwendung der Frequenzen von 1800 bis 1900 MHz hier evtl. nicht zulässig ist. In diesem

---

<sup>1</sup>Es gibt jedoch auch weitere Anwendungen wie z.B. Babyfone.

Fall muss auf das ISM-Band ausgewichen werden, welches sich hier mit anderen Anwendungen geteilt werden muss.

DECT bietet eine optionale Verschlüsselung der Nutzdaten, welche jedoch im Jahr 2009 geknackt wurde, so dass DECT mittlerweile als unsicher gelten muss. Aufgrund der geringen Nutzdatenmenge sowie der Einschränkung auf 6 Teilnehmer ist DECT für den Einsatz als Sensornetz-Protokoll nicht geeignet.

### 3.1.3 GSM/UMTS

### 3.1.4 WLAN

### 3.1.5 Übersicht

WLAN oder Wi-Fi bezeichnet den heute gängigen Standard eines Funkprotokolls zum Aufbau von kabellosen lokalen Netzwerken. Es gibt mehrere Versionen des Standards, die verbreitetsten sind IEEE 802.11a, IEEE 802.11b/g und IEEE 802.11n.

Es sind zwei Betriebsmodi möglich:

- Infrastruktur-Modus: Eine zentrale Station („Access-Point“) dient als Basisstation für alle weitere Stationen. Jede Station, die am Netzwerk teilnimmt, muss hierzu die Signale des *Access-Points* empfangen können.
- Ad-hoc-Modus: Dieser Betriebsmodus kommt ohne zentrale Komponente aus. Es wird eine Peer-to-Peer-Verbindung zwischen allen am Netzwerk teilnehmenden Stationen aufgebaut. Hierzu ist es notwendig, dass alle Stationen sich gegenseitig empfangen können.

Der Infrastruktur-Modus bietet gegenüber des Ad-Hoc-Modus' klare Vorteile: Im Gegensatz zum Ad-hoc-Modus ist es nicht notwendig, dass alle Stationen sich gegenseitig empfangen müssen, es reicht aus, wenn der Access-Point empfangen werden kann. Hierdurch ist eine größere Ausbreitung des Netzwerks möglich als im Ad-Hoc-Modus.

Es werden verschiedene Datenübertragungsraten unterstützt. Standardmässig wird immer die größtmögliche Übertragungsrate gewählt, die störungsfrei verwendet werden kann. Je weiter sich die Stationen voneinander entfernen, desto geringer wird die Übertragungsrate, bis schliesslich die niedrigst mögliche Übertragungsrate von 1MBit/sec erreicht wird.

Es gibt eine ganze Menge von Unterstandards, die sich durch zulässige Frequenzen, Übertragungsraten und Sendeleistung unterscheiden. Teilweise ist auch Kanalbündelung vorgesehen. Nicht jeder Standard kann in jedem Land eingesetzt werden, und die meisten Endgeräte unterstützen nur eine Teilmenge dieser Standards. Hier sollen nur die wichtigsten drei Standards erwähnt werden.

### **IEEE 802.11b**

Bei IEEE 802.11b handelt es sich um den ältesten WLAN-Standard, der bereits 1999 spezifiziert wurde. Dieser Standard wird praktisch von jedem WLAN fähigen Endgerät unterstützt. Die Kommunikation findet im ISM-Band im Bereich von 2.4GHz statt. Je nach Land sind 11-14 Kanäle möglich, die sich jedoch teilweise überlappen. Dies führt dazu, dass maximal 3 Netzwerke ohne Störungen gleichzeitig betrieben werden können. Die maximale Sendeleistung beträgt 100mW. Es sind Übertragungsraten von 5,5 bis 11 MBit (brutto) möglich. Die Nettoübertragungsrate beträgt ca. 50% der Bruttorate. Es sind Reichweiten bis 40m (Innen) bzw. 100m (Im Freien) möglich Kumar u. a. (2008).

### **IEEE 802.11g**

Der IEEE 802.11g Standard stellt eine Erweiterung des IEEE 802.11b Standards da. Wesentliche Neuerung ist eine Erhöhung der Bruttodatenrate von 11 auf 54MBit/sec, von denen netto ca. 40% zur Verfügung stehen. Erwähnenswert ist, dass die beiden Standards Interoperabel sind, d.h. ein 802.11b Gerät kann einem 802.11g Netzwerk beitreten und umgekehrt. Dies ist auch der Grund, weshalb dieser Standard momentan am weitesten verbreitet ist.

### **IEEE 802.11a**

Der IEEE 802.11a Standard verwendet Frequenzen im 5GHz Bereich. Er ist daher inkompatibel zum IEEE 802.11b/g Standard. Je nach Frequenzband sind Sendeleistungen zwischen 30 und 1000mW zulässig. Mit dem passenden Frequenzband sind daher höhere Reichweiten als mit dem IEEE 802.11b/g Standard möglich. Die Bruttodatenrate beträgt bis zu 54MBit/sec. Ein Vorteil des IEEE 802.11a Standards ist die Kommunikation im 5GHz Bereich. Aktuell ist dieser Bereich noch wenig genutzt, so dass in diesem Bereich oft ein störungsärmerer Betrieb als im 2,4GHz-Bereich möglich ist. Es ist jedoch zu erwarten, dass sich dies in

Zukunft ändern wird.

### Störsicherheit

?? IEEE 802.11 verwendet den CSMA/CA<sup>2</sup>-Algorithmus zur Störungsbehandlung. Möchte ein Station senden, so muss diese zunächst für einige Zeit lauschen, ob der zu verwendende Kanal auch wirklich frei ist. Ist der Kanal belegt, so wartet sie eine zufällige Zeit, bis sie erneut versucht, auf den Kanal zuzugreifen. Wichtig hierbei ist, dass es bei Funkprotokollen nicht möglich ist, eine Kollision zu erkennen um eine bestehende Übertragung abubrechen, wie es z.B. bei *Ethernet* der Fall ist. Zur Vermeidung von Kollisionen kann bei IEEE 802.11 daher zusätzlich zu CSMA/CA eine Art Token-Passing eingesetzt werden. Hier kommt RTS/CTS zum Einsatz: Möchte eine Station ein großes Datenpaket senden, so sendet diese zuerst ein RTS-Paket<sup>3</sup> an den Empfänger, welcher dies mit einem CTS-Paket<sup>4</sup> quittiert. Erst wenn das CTS-Paket empfangen wurde, wird mit der Übertragung des eigentlichen Datenpakets begonnen. Für alle andere Stationen im Netzwerk ist nun klar, dass sie bis zur abgeschlossenen Übertragung dieses Paketes nicht auf das Netzwerk zugreifen dürfen.

Bei dem Einsatz der in IEEE 802.11i definierten Verschlüsselungsverfahren (WEP<sup>5</sup>, WPA oder WPA2) wird lediglich die Nutzdaten des Paketes verschlüsselt. Die CTS/RTS-Pakete können weiterhin erkannt werden, so dass die Kollisionsverhinderung auch dann funktioniert, wenn die Pakete nicht entschlüsselt werden können (Diese Situation ist z.B. in Mietshäusern oft anzutreffen, wo mehrere unterschiedliche WLANs auf dem selben Kanal senden). Jedoch geht dies mit einer reduzierten Übertragungsrate für die einzelnen Netzwerke einher.

Problematisch ist die Störung durch andere Quellen wie z.B. Mikrowellenherden, DECT Telefonen oder Bluetooth, da diese nicht dem CSMA/CA Verfahren unterliegen und zu beliebiger Zeit senden können. Insbesondere die Störung durch Bluetooth ist problematisch, da Bluetooth und WLAN Geräte oft aufeinander-

---

<sup>2</sup>Carrier Sense Multiple Access with Collision Avoidance. Zu deutsch: Gemeinsamer Mediengriff mit Kollisionsvermeidung

<sup>3</sup>Ready to send

<sup>4</sup>Clear to send

<sup>5</sup>Die Sicherheit von WEP ist bereits seit einigen Jahren kompromittiert. Es sollte nichtmehr verwendet werden



treffen (z.B. weil an einem Notebook Bluetooth-Maus und -Tastatur verwendet werden oder weil ein PDA z.B. Schnittstellen für beide Protokolle besitzt). Wie in Abschnitt ?? genauer erläutert besitzt Bluetooth 79 Kanäle, welche bis zu 1600 mal pro Sekunde gewechselt werden. Problematisch ist nun, dass 22 dieser Kanäle in das IEEE 802.11b/g-Frequenzspektrum fallen. Durch den häufigen Kanalwechsel, die geringeren Übertragungsraten so die Möglichkeit, den Wechsel auf belegte Kanäle zu vermeiden ist diese Störung für Bluetooth deutlich unproblematischer als für WLAN. Je nach Implementierung kann dies zu einer deutlichen Reduktion der Übertragungsrate des WLANs führen; ausserdem kann die Wartezeit für das erfolgreiche Senden von Paketen deutlich ansteigen. Dies hat die IEEE dazu veranlasst, eine eigene Arbeitsgruppe zu gründen, die sich mit dem Problem der gegenseitigen Störung von WLAN und Bluetooth zu beschäftigen. Die Ergebnisse dieser Arbeitsgruppe spiegeln sich im IEEE 802.15.2 Standard wieder.

### Leistungsaufnahme

Der Energiebedarf für WLAN ist relativ hoch. Beispielsweise benötigt der vom Hersteller Broadcom als besonders energiesparend bezeichnete Chip BCM4326 bis zu 100mA zum Empfangen und zwischen 141 und 190mA zum Senden.<sup>6</sup>

### Anzahl Teilnehmer

## 3.1.6 WPAN: Wireless Personal Area Networks

### Übersicht

Als WPANs („Wireless Personal Area Networks“) werden kabellose Kleinnetzwerke bezeichnet, die dazu dienen, wenige Geräte über kurze Entfernungen (mehrere Meter) miteinander zu verbinden. Sie dienen als Ersatz von Kabelverbindungen zur Anbindung von Peripherie an Computergeräte (z.B. zur Verbindung von Headsets mit Mobiltelefonen oder von Tastatur und Maus mit einem PC).

### IEEE 802.15

Der IEEE 802.15-Standard behandelt *Wireless Personal Area Networks*. Er ist in mehrere Unterstandards aufgeteilt:

- IEEE 802.15.1: Bluetooth 1.2

---

<sup>6</sup>BCM4326 Datasheet

- IEEE 802.15.2: Zusammenarbeit zwischen IEEE 802.15 (WPAN) und IEEE 802.11 (WLAN)
- IEEE 802.15.3: WPANs mit hohen Datenübertragungsraten (20MBit/sec und höher)
- IEEE 802.15.4: WPANs mit niedriger Datenübertragungsraten

Für diese Arbeit sind vor allem der Bluetooth und der ZigBee Standard interessant.

### IEEE 802.15.1: Bluetooth

**Überblick** Bluetooth wurde ursprünglich von dem Mobilfunkhersteller Ericsson als Ersatz für RS-232 Verbindungen entwickelt. Die Entwicklung des Bluetooth Standards erfolgt heute unter der Regie der *Bluetooth Special Interest Group* („SIG“). Version 1.1 des Bluetooth Standard wurde von der IEEE als IEEE 802.15.1-2002 übernommen. Nach Veröffentlichen einer weiteren Version IEEE 802.15.1-2005, die dem Bluetooth 1.2 Standard entspricht, wurde von der IEEE jedoch beschlossen, nicht weiter mit der *Bluetooth SIG* zu kooperieren, so dass es keine weiteren Versionen des IEEE 802.15.1 Standards geben wird. Aktuell ist Version 4.0 des Bluetooth Standard, wobei jedoch die meisten Geräte nur geringere Standards (Typischerweise 2.0 oder 2.1) unterstützen. Für den Bluetooth 4.0 Standard existiert zum Zeitpunkt dieser Arbeit keine Implementierung auf dem Markt.

Die wichtigsten Meilensteine der Bluetooth-Entwicklung kann folgendermaßen zusammengefasst werden:

- Bluetooth 1.1: Erste Version von praktischer Relevanz. Entspricht IEEE 802.15.1-2002.
- Bluetooth 1.2: Entspricht IEEE 802.15.2-2005. Bringt einige Verbesserungen gegenüber der Version 1.1 wie z.B. schnelleres Finden von Endgeräten (Discovery), höhere Störsicherheit durch die Verwendung von AFH<sup>7</sup>, Übertragungsraten bis 721kbit/sec.
- Bluetooth 2.0: Einführung des EDR<sup>8</sup>-Modus mit bis zu 3.0 MBit/sec (2.1 MBit/sec netto).

---

<sup>7</sup>Adaptive frequency-hopping spread spectrum

<sup>8</sup>Enhanced Data Rate

- Bluetooth 2.1: Vereinfachung des Pairings (vgl. ??) durch Einführung von SSP<sup>9</sup>, Verbesserung der Sicherheit durch explizite Aushandlung der Verschlüsselung.
- Bluetooth 3.0: Einführung eines Hochgeschwindigkeits-Datenkanals auf Basis von IEEE 802.11 (vgl. 3.1.4) mit bis zu 24MBit/sec., verbessertes Powermanagement, Einführung von Verbindungslosen Datentelegrammen (Uncasts).
- Bluetooth 4.0: Einführung des *Bluetooth Low Energy* Standards (vgl. 3.1.6).

**Pairing** Bei der Entwicklung von Bluetooth wurde ein besonderes Augenmerk auf Datensicherheit gelegt. Dies liegt daran, dass über Bluetooth in vielen Fällen auf sensible Daten (z.B. der Inhalt von Mobiltelefonen, Telefongespräche die über Headsets geführt werden etc.) zugegriffen werden kann. Bluetooth verwendet hierfür das Konzept des Pairings, also der Paarung. Bevor zwei Bluetooth Geräte miteinander kommunizieren können, müssen sie gepaart werden. Um dies durchzuführen muss zunächst die Identität der zu paarenden Geräte bestätigt werden. Hierzu gibt es zwei verschiedene Verfahren:

- Legacy: Bis Bluetooth 2.0 muss an beiden Geräten eine identische PIN eingegeben werden. Die PIN ist beliebig und kann bis zu 16 Byte lang sein.
- Secure Simple Pairing: Bluetooth 2.1 definiert neben der PIN-Eingabe weitere Verfahren zum Paaren von Geräten. z.B. kann bei dem *Just-Works*-Verfahren die PIN komplett ausgelassen werden<sup>10</sup> oder es wird an beiden Geräten eine Nummer angezeigt, deren Gleichheit einfach nur noch bestätigt werden muss.

Ist diese Überprüfung erfolgreich generieren beide Geräte einen kryptographischen Schlüssel und die weitere Kommunikation erfolgt verschlüsselt. Sobald zwei Geräte gepaart wurden können sie miteinander kommunizieren ohne eine erneute Paarung durchführen zu müssen.

---

<sup>9</sup>Secure Simple Pairing

<sup>10</sup>Die Verbindung erfolgt trotzdem verschlüsselt, allerdings sind nun Man-in-the-middle-Angriffe möglich

**Reichweite** Bluetooth definiert drei verschiedene Klassen von Geräten mit jeweils unterschiedlicher Reichweite:

- Klasse 1: maximale Sendeleistung: 100mW, Reichweite ca. 100m
- Klasse 2: maximale Sendeleistung: 2.5mW, Reichweite ca. 10m
- Klasse 3: maximale Sendeleistung: 1mw, Reichweite ca. 1m

Diese Einteilung dient unter anderem der Datensicherheit. Da z.B. ein Headset in der Regel nur die Distanz zwischen Kopf und Tasche des Anwenders überbrücken muss reicht hier die Verwendung eines Klasse 2 Gerätes. Durch die Einschränkung der Sendeleistung wird nicht nur die Akkulaufzeit der Geräte erhöht, sondern auch die Wahrscheinlichkeit, dass ein Angreifer die gesendeten Daten empfangen kann, verringert.

Es bleibt allerdings festzustellen, dass mit Hilfe von geeigneten Antennen die Reichweite von Bluetooth signifikant gesteigert werden kann. So ist es z.B. einer Gruppe von Hackern gelungen, mit Hilfe von Yaggi-Antennen mit Bluetooth eine Distanz von über 800m zu überbrücken.

**Übertragungsrate** Die Übertragungsrate von Bluetooth hängt natürlich von Faktoren wie der Verbindungsqualität und der Entfernung ab. Der Standard definiert folgende maximale Datenübertragungsraten:

- Bluetooth 1.1: 721kbit/sec
- Bluetooth 2.0: 3.0MBit/sec
- Bluetooth 3.0: 24 Mbit/sec (über einen 802.11 Kanal)

**Störsicherheit** Bluetooth verwendet einen Frequenzbereich von 2,402 - 2,480 GHz. Innerhalb dieses Bereiches werden 79 verschiedene Kanäle definiert. Zur Minimierung von Störungen wird sogenanntes *Channel-Hopping* verwendet. Hierbei wird der verwendete Kanal bis zu 1600 mal pro Sekunde gewechselt. Mit dem Bluetooth 1.2 Standard wurde das verbesserte AFH<sup>11</sup>-Verfahren eingeführt, welches gestörte Kanäle erkennt, und eine Verwendung dieser vermeidet.

---

<sup>11</sup>Adaptive frequency-hopping spread spectrum

Insbesondere WLAN-Netzwerke und Bluetooth Netzwerke stören sich gegenseitig. Wie in Abschnitt ?? bereits erläutert wird WLAN deutlich stärker durch Bluetooth gestört als dies umgekehrt der Fall wäre. Tritt eine Störung auf einem Kanal auf, versucht das AFH-Verfahren die Verwendung dieses Kanals zu vermeiden. Hierdurch sinkt zwar die Erreichbare Datenübertragungsrate, allerdings kann eine Kommunikation mit verminderter Übertragungsrate weiterhin stattfinden.

Es ist festzustellen, dass Bluetooth – insbesondere im Vergleich zu WLANs – recht robust gegenüber Störungen ist.

**Anzahl Teilnehmer** Sobald zwei oder mehr Geräte miteinander verbunden sind, formen diese ein sogenanntes *Piconet*. In einem *Piconet* können sich bis zu 255 Geräte befinden, wobei ein Gerät eine der folgenden beiden Rollen hat:

- **Master:** Der Master koordiniert die Kommunikation im Netzwerk. Hierzu gibt er jeweils Zeitslots vor, in denen Daten gesendet werden dürfen. Pro *Piconet* kann es nur einen Master geben.
- **Slaves:** Slaves bekommen vom Master die Erlaubnis, Daten zu senden. Es können immer nur 7 Slaves gleichzeitig aktiv sein. Aktive Slaves müssen permanent empfangsbereit sein, um die Anforderungen des Masters zu empfangen.

Da immer nur 7 Slaves gleichzeitig aktiv sein dürfen, befinden sich alle übrigen Slaves im sogenannten *Parkzustand*. Erst wenn ein Slave vom Master explizit dazu aufgefordert wird, darf er in den aktiven Zustand wechseln.

Um die Anzahl der aktiven Geräte in einem Netzwerk zu erhöhen gibt es die Möglichkeit, ein sogenanntes Scatternet zu bilden. Hierbei handelt es sich um die Verbindung von mehreren *Piconets* mit jeweils maximal 8 Geräten zu einem größeren Verbund. Hierbei leitet jeweils ein Gerät, das in jeweils 2 der *Piconetze* verbunden ist, Pakete vom einen Netz in das andere Netz über. Im Vergleich zu *Piconetzen* kann hiermit eine deutlich höhere Anzahl von Geräten unterstützt werden. Durch die Verkettung der Netzes kann es jedoch vorkommen, dass einzelne Pakete eine relativ hohe Anzahl von *Piconetzen* durchqueren müssen, um ihr Ziel zu erreichen.

## Leistungsaufnahme

### IEEE-802.15.4: ZigBee

Wibree: Bluetooth Low Energy

### 3.1.7 Weitere Protokolle

- WiMAX - Mikrowellen-Richtfunk - Z-Wave - Wireless USB

### 3.1.8 Diskussion

## 3.2 Der Analog Devices ADuC702X Mikrocontroller

## 3.3 Java

## 3.4 Corba

# Kapitel 4

## Fortschritt der Arbeit

So Sachen wie, dass es nicht mehr von der Bewegung am Brustkorb abhängt (indirekt bei QRS), dass die HRV-Methode auch Messungen der Atmung Beispielsweise am Handgelenk zulässt, also weit weg von der Lunge...





# Kapitel 5

## Praktische Realisierung des Sensornetzes

### 5.1 Entwurf

#### 5.1.1 Hardware

##### MANVNode

##### ADuC

Beim MANVNode handelt es sich um ein Prototyp des späteren Erste-Hilfe-Sensor für den MANV-Einsatz. Zwar existiert der Erste-Hilfe-Sensor bereits, allerdings hat dieser noch keinerlei Netzwerkfähigkeit. Der Erste-Hilfe-Sensor basiert auf einem ADuC7019 Microcontroller und ergänzt diesen durch Detektionskomponenten, zur Patientenüberwachung.

Für die Entwicklung der Netzwerkanbindung sind diese Detektionskomponenten nur insofern relevant, dass es zu keiner Gegenseitigen Störung zwischen Detektion- und Netzwerkkomponenten kommen darf. Daher wurde im ersten Schritt alle nicht benötigten Komponenten weggelassen, und lediglich der reine Mikrocontroller verwendet. Später wurden die hierbei entwickelte Netzwerkkomponenten zusammengefasst und in die Hardware des Erste-Hilfe-Sensors integriert.

Die eigentliche Entwicklung fand mit Hilfe eines ADuC7026 Evaluations-Board statt. Dieses Board hat den Vorteil, dass alle Anschlüsse des Mikrocontrollers auf Steckerleisten geführt, und damit leicht zugänglich sind. Ausserdem ist eine JTAG-Schnittstelle vorhanden, die ein einfaches Debuggen des Mikrocontrollers

ermöglicht.

### **ZigBee-Schnittstelle**

Für die Anbindung des Erste-Hilfe-Sensors an das Sensornetz wird ein ZigBit-Modul der Firma Atmel verwendet. Dieses Modul bietet den Vorteil, dass es bereits über einen kompletten ZigBee-Stack verfügt, der einfach über AT-Befehle gesteuert werden kann, die per UART gesendet werden.

Der ZigBee-Stack auf dem ZigBit Modul ist austauschbar und kann durch eine eigene Firmware ersetzt werden. Hierzu wird von der Firma Atmel ein umfangreiches SDK<sup>1</sup> angeboten. Für den Rahmen dieser Diplomarbeit ist die vorgefertigte Serial-Net-Firmware allerdings ausreichend. Einziger Wermutstropfen ist die fehlende Verschlüsselung, welche für den Serieneinsatz natürlich erforderlich wäre.

Die Kommunikation mit dem ZigBit Modul erfolgt grundsätzlich synchron. Jeder AT-Befehl wird entweder mit „OK“, „ERROR“ oder einer Ergebnisszeile quittiert. Der Treiber für das ZigBit-Modul kann also prinzipiell als endlicher Automat mit zwei Zuständen implementiert werden. Zu beachten ist jedoch, dass prinzipiell jederzeit Ereignisse vom Typ „Data Received“ auftreten können. Es ist also notwendig, die Antwort des ZigBit Moduls zu parsen, und zu entscheiden, ob es sich um eine Antwort auf einen zuvor gesendeten Befehl oder aber um ein Data-Ereignis handelt. Wichtig ist, dass diese Ereignisse nicht verloren gehen dürfen, da es sich um Befehle handelt, die von der MANVSuite an den Sensor gesendet wurden, und von diesem abgearbeitet werden müssen.

#### **5.1.2 Firmware**

Die Firmware des Erste-Hilfe-Sensors wurde um einen Treiber für das ZigBit-Modul ergänzt. Die Firmware wurde in der Programmiersprache C geschrieben, und setzt direkt auf die Hardware des ADuC auf. Es wurde lediglich die von Rowley Crossworks angebotene Standardbibliothek verwendet, die einige praktische Funktionen wie Stringmanipulation, einen Interrupthandler und einen fertigen Startup-Code bietet.

Die Entwicklung von Software für einen Microcontroller zeichnet sich durch die Abwesenheit eines Betriebssystems aus. Ein Großteil der Funktionalität, die man

---

<sup>1</sup>Software-Development-Kit: Eine Art Baukasten für Software, die viele benötigte Teile bereits fertig zur Verfügung stellt

von der Entwicklung von Software für einen standard Mikrocomputer gewohnt ist, ist schlichtweg nicht vorhanden. Hier sind insbesondere eine automatische Speicherverwaltung sowie Threads und Prozesse zu erwähnen. Da der Erste-Hilfe-Sensor viele Aufgaben gleichzeitig erfüllen muss, stellt dies eine ernst zu nehmende Herausforderung dar. Das Problem wurde durch ein Interrupt getriebenes Programmiermodell gelöst.

Es werden folgende Interrupts verwendet:

Timer0: Dieser Timer-Interrupt führt die Patientenüberwachung durch. Die einzelnen Sensoren werden abgefragt, und eine Analyse der empfangenen Daten wird durchgeführt.

Timer1: Dieser Interrupt führt einige periodische Aufgaben durch. Zunächst werden die am Sensor vorhandenen Taster abgefragt (Alarm Stummschalten, Alarm manuell auslösen etc.). Danach wird überprüft, in welchem Zustand der Sensor sich aktuell befindet, also z.B. ob ein Alarm aufgetreten ist, oder ob der Patient sich in einem guten Zustand befindet. Abhängig hiervon werden nun LEDs und ein angeschlossener Piezzo-Summer geschaltet, um den Zustand nach aussen zu signalisieren. Zu letzt wird noch überprüft, wann zuletzt eine Übertragung des Zustands des Sensors an die MANVSuite erfolgt ist. Liegt dies länger als einen konfiguriertes Zeitintervall zurück, so wird eine Übertragung des aktuellen Zustands veranlasst.

Ein weiteres Problem sind die sehr beschränkten Ressourcen des Mikrocontrollers. Insbesondere der Speicher ist mit 16kB sehr knapp bemessen.

## UART

Der ADuC verfügt über einen UART Interrupt, welcher eine Statusänderung des UARTs signalisiert. Im Register *COMIEN0* wird konfiguriert, welche Zustände über den Interrupt signalisiert werden sollen. Tritt nun einer dieser Zustände auf, so wird der UART Interrupt ausgelöst. Im Interrupthandler muss nun überprüft werden, welches Ereigniss zum Auslösen des Interrupts geführt hat. Dies ist im Register *COMSTA0* gespeichert. Wichtig ist an dieser Stelle, dass auch mehrere Ereignisse gleichzeitig auftreten können. Dies muss im Interrupthandler berücksichtigt werden, da sonst Ereignisse verloren gehen können.

Das eigentliche Senden und Empfangen erfolgt über die beiden Register *COMRX* und *COMTX*. Zum Senden wird hierzu ein einzelnes Zeichen in *COMTX* gelegt. Nun muss eine gewisse Zeit gewartet werden, bis das Zeichen gesendet wurde,

und das nächste Zeichen in *COMTX* gelegt werden kann. Für das Empfangen wird das Register *COMRX* in analoger Weise verwendet werden. Ob das nächste Zeichen empfangen bzw. gesendet werden kann, kann mit Hilfe der Bits *DR* („Data Ready“ - Daten liegen vor) bzw. *TEMT* („Transmit Buffer empty“ - Daten können gesendet werden) bestimmt werden.

Die einfachste Methode wäre hierbei, in einer Schleife Busy-Waiting zu betreiben, und so lange zu warten, bis sich eins der beiden Bits verändert. Dies wäre jedoch sehr aufwendig und würde den Mikrocontroller unnötig lange blockieren. Statt dessen wird der Zustand der beiden Register nur dann überprüft, wenn ein UART-Interrupt aufgetreten ist.

Zum Senden und Empfangen von Daten werden zwei Ringpuffer verwendet. Möchte ein Unterprogramm Daten senden, so greift es nicht direkt auf die UART-Schnittstelle zu sondern legt diese Daten lediglich in den Sendepuffer. Das eigentliche Senden wird nun vom UART-Interrupthandler durchgeführt; das Unterprogramm kann weiter arbeiten, ohne auf das fertige Senden der Daten warten zu müssen.

Das Empfangen von Daten erfolgt analog. Jedesmal wenn ein Zeichen von der seriellen Schnittstelle empfangen wurde, wird dieses in den Empfangspuffer gelegt. Das Abarbeiten des Empfangspuffer erfolgt nun als Idle-Task: Immer dann, wenn der Mikrocontroller gerade keine anderen Aufgaben erfüllen muss, wird der Empfangspuffer abgearbeitet und eventuell empfangene Befehle werden abgearbeitet. Dies kann natürlich jederzeit durch die Abarbeitung von Interrupts unterbrochen werden.

## MANV-USB-Connector

Der MANV-USB-Connector ist die Schnittstelle zwischen Sensornetz und Computer. Es handelt sich um einen USB-Stick, der einen ZigBit-Modul beinhaltet. Zusätzlich sind zwei weitere Bauteile enthalten, die das ZigBit-Modul mit Strom versorgen, sowie eine Umsetzung der UART-Schnittstelle des ZigBit-Moduls auf USB vornehmen. Für die Stromversorgung ist es notwendig, die 5V der USB-Schnittstelle auf die 3V des ZigBit-Moduls umzusetzen.

### 5.1.3 Software

In dieser Arbeit wurde ein Java-Treiber (MANVConnector) entworfen und implementiert. Dieser Treiber realisiert die die Anbindung an die von Herrn Tepelmann in Tepelmann (2010) entwickelte MANVSuite.

Der MANVConnector hat einerseits die Aufgabe, Daten die von dem MANV-USB-Connector empfangen wurden in Corba-Events umzusetzen, und an den MANVServer weiterzuleiten. Andererseits empfängt sie Corba-Events vom MANVServer, dekodiert diese und sendet diese in Form von Sensornetz Befehlen an die zuständigen MANVNodes weiter.

Bei der Kommunikation mit dem auf dem USB-Stick aufgebrachten ZigBee-Modul stellen sich grundsätzlich die selben Synchronisierungsprobleme wie in der MANVFirmware. Da der MANVConnector jedoch alle Möglichkeiten der Java-Virtual-Machine nutzen kann, lassen sich diese deutlich einfacher und eleganter lösen.

Analog zu den Sende- und Empfangspuffern in der Firmware gibt es im MANV-Connector drei Queues:

- Die Command Queue: In dieser Queue werden alle zu sendenden Befehle gespeichert.
- Die Event Queue: In dieser Queue werden alle empfangenen Ereignisse gespeichert.
- Die Result Queue: In dieser Queue werden alle bereits gesendeten Befehle zusammen mit dem Resultat, das dieser Befehl hatte, gespeichert.

Jedes Element der einzelnen Queues verfügt über eine Priorität; die Queues sorgen dafür, dass der Zugriff nach Priorität sortiert erfolgt. Hierdurch wird sicher gestellt, dass wichtige Ereignisse wie z.B. ein Alarm bevorzugt ausgeliefert werden.

Der MANVConnector ist in drei Threads aufgeteilt:

- SocketWriter: Dieser Thread entnimmt Befehle aus der *CommandQueue* und sendet diese über den MANV-USB-Connector an das Sensornetz. Nun blockiert der Thread so lange, bis das Ergebnis des Befehls zur Verfügung steht. Sobald dies der Fall ist, wird der Befehl zusammen mit dem Ergebnis in die *ResultQueue* eingefügt.
- SocketReader: Dieser Thread empfängt Daten aus dem Sensornetz. Handelt es sich um ein Ergebnis, so wird dies dem *SocketWrite* signalisiert, und das Ergebnis zur Abholung durch den *SocketWriter* zur Verfügung gestellt. Handelt es sich hingegen um einen Ereignis, so wird dieses in die *EventQueue* eingefügt.

- Haupt-Thread: Dieser Thread ist für die Kommunikation mit MANVServer zuständig. Befehle, die vom MANVServer empfangen werden, werden für das Sensornetz aufbereitet und in die CommandQueue eingestellt. Ausserdem werden Ereignisse aus der *EventQueue* entnommen, in Corba-Events übersetzt und an den MANVServer zugestellt.

## 5.2 Implementierung

### 5.2.1 Hardware

### 5.2.2 Firmware

### 5.2.3 Software

# Kapitel 6

## Ergebnisse

### 6.1 Baselinewandering

#### 6.1.1 Messungen unter verschiedenen Bedingungen

... nur die reinen Messergebnisse kommen hier rein mit Erläuterung/Begründung etc... Bilder von den Messungen und Fakten

#### 6.1.2 Vergleichende Messung mit Referenzgerät

... Ebenfalls nur Bilder und Zahlen im Vergleich zu der Referenzmethode (am Besten Bilder, in denen die Atmungskurve von der neuen Methode und der Referenzmethode gleichzeitig zu sehen sind)

### 6.2 HRV-Variation

#### 6.2.1 Messungen unter verschiedenen Bedingungen

... wie oben

#### 6.2.2 Vergleichende Messung mit Referenzgerät

... wie oben

## 6.3 QRS-Komplexe

### 6.3.1 Messungen unter verschiedenen Bedingungen

... wie oben

### 6.3.2 Vergleichende Messung mit Referenzgerät

... wie oben

## 6.4 Vergleiche der Verfahren zueinander

Hier nur Grafiken, Fakten, Zahlen etc. reinmachen, die die verschiedenen Verfahren überlappend zeigen und kurz erläutern, aber nicht bewerten.

Der Ergebnisteil (Ergebnisse, results) sollte die wesentlichen Befunde der aktuellen Arbeit in nachvollziehbarer, durch geeignete Präsentation (Tabellen, Grafiken) unterstützter Weise darbieten. Die Auswahl der dargebotenen Ergebnisse ist nach der Relevanz im Hinblick auf die Fragestellung zu treffen. Dies gilt gleichermaßen für Positivergebnisse, welche die Argumentation der Autoren stützen, wie auch für Negativergebnisse und Probleme bei der Durchführung der Untersuchung, sofern diese einen Einfluss auf das Ergebnis gehabt haben könnten. Die Datenpräsentation sollte einen unverfälschten, aber durch geeignete Aufarbeitung der Daten (Mittelwertbildung, andere zusammenfassende deskriptive Statistik, etc.) fokussierten Überblick geben. Außerdem sollte der Ergebnisteil verschiedene Teilergebnisse nicht isoliert präsentieren, sondern den Leser in einer zusammenhängenden Beschreibung durch die Resultate führen. Dies schließt eine Beschreibung der wichtigsten Befunde aus Tabellen und Grafiken ein. ———



# Kapitel 7

## Diskussion

Bewertung (auch subjektive Meinung) der einzelnen Verfahren. Vor- und Nachteile. Wo gibt es Probleme (z.B. bei HRV nur im unteren Frequenzbereich einsetzbar?? etc.), wie ist die Abweichung zu Referenzmessungen...

### 7.1 Baselinewandering

...

### 7.2 HRV-Variation

...

### 7.3 QRS-Komplexe

...

### 7.4 Vergleich der Verfahren zueinander

In der Diskussion (discussion) stellen die Autoren ihre Schlussfolgerungen aus den Ergebnissen vor. Dabei ist eine Wiederholung der Ergebnisdarstellung zu

vermeiden. Das diskutierte Ergebnis braucht nur noch erwähnt, nicht aber erneut dargestellt zu werden. Inwieweit konnte eine in der Einleitung vorgestellte Hypothese gestützt oder widerlegt werden? Inwiefern sind die Ergebnisse in Übereinstimmung mit bisherigen publizierten Befunden und Hypothesen oder stehen im Gegensatz zu diesen? Neben der Einleitung ist die Diskussion derjenige Teil des Artikels, in dem ein Schwerpunkt darauf liegt, die gerade ausgeführte Studie in die sonstige Fachliteratur einzuordnen.

# Kapitel 8

## Zusammenfassung und Ausblick

\*\*\*Beispiel wie ein Zitat auf Armins (?) Buch funktioniert\*\*\*



# Glossar



# Literaturverzeichnis

- [Kumar u. a. 2008] KUMAR, Anurag ; D. MANJUNATH, D. ; KURI, Joy: *Wireless networking*. Amsterdam : Morgan Kaufmann / Elsevier, 2008 (The Morgan Kaufmann series in networking). – ISBN 978–0–12–374254–4 ; 0–12–374254–4
- [Tepelmann 2010] TEPELMANN, Jan: *Entwicklung und Implementierung einer graphischen Benutzeroberfläche zur Überwachung von Patienten in einem Sensornetz in einem MANV-Szenario (Arbeitstitel)*. Karlsruhe : Karlsruher Institut für Technologie (KIT), 2010