

Inhaltsverzeichnis

Abkürzungsverzeichnis	XIII
1 Einleitung	1
2 Einführung in drahtlose Sensor-/Aktor-Netzwerke	5
3 Grundlagen Übertragungstechnik	7
3.1 Signalausbreitung	7
3.2 Theoretische Reichweiten	8
3.3 Pfadverlust (Path Loss) und Reichweite	10
3.4 Antennenlänge	11
3.5 Antennen	12
3.5.1 $\lambda/2$ -Dipolantennen	13
3.5.2 $\lambda/4$ -Monopolantennen	14
3.5.3 Chip- bzw. Keramikantennen	15
3.6 Gesetzliche Richtlinien	17
3.6.1 Europäische Richtlinien	17
3.6.2 Internationale Richtlinien	18
4 Sicherheit und Zuverlässigkeit in WSN	19
4.1 Gefahren für die Sicherheit (Security) und die Zuverlässigkeit (Reliability) der Daten und der Datenübertragung in einem WSN . . .	20
4.2 Sicherheitsmechanismen in IEEE 802.15.4- und ZigBee-Netzen . . .	22
4.2.1 Überprüfung der Datenintegrität in IEEE 802.15.4- und ZigBee-Netzen	23
4.2.2 Verschlüsselung der Daten in IEEE 802.15.4- und ZigBee-Netzen	23
4.2.3 Zuverlässigkeit in IEEE 802.15.4- und ZigBee-Netzen	24
4.2.4 Authentifizierung in ZigBee-Netzwerken	25
4.3 Single Point of Failure	25

5	Hardware für ZigBee Komponenten	27
5.1	Verfügbare ZigBee-Hardware	28
5.2	Schnittstellen und Bussysteme von Mikrocontrollern	29
5.3	Sensoren und Aktoren	31
5.4	IEEE 802.15.4/ZigBee und Reichweite	32
5.5	Erhöhung der Reichweite	33
6	Aufbau von programmierbaren Sensor-Funkmodulen	37
6.1	Auswahl des ZigBit-Moduls	38
6.2	Grundschaltung eines Funkmoduls mit dem Atmel ZigBit Chip ATZB-24-A2	40
6.3	Programmierinterfaces	42
6.3.1	Programmierinterface JTAGICE3	43
6.3.2	Programmierinterface AVRISPMkII	43
6.4	Fotowiderstand an einen ADC-Eingang des Zigbit Moduls anschließen	44
6.5	3 LEDs an die universellen digitale Ein-/Ausgänge (GPIOs) des Zigbit-Moduls anschließen	48
6.6	I ² C-Schnittstelle	49
6.6.1	Beispiel einer Kommunikation mit einem Temperatursensor LM73	51
6.7	Verbindung eines Funkmoduls mit dem PC über eine UART-USB Schnittstelle	52
6.7.1	UART-USB Schnittstelle mit dem CP2102EK Evaluation Kit	53
6.7.2	UART-USB-Schnittstelle mit dem FTDI FT232-Chip	54
6.8	Energiebedarf der ZigBit-Module	56
7	AVR Studio, WinAVR, BitCloud, WSNDemo	65
7.1	Installation AVR Studio, WinAVR, BitCloud	66
7.2	WSNDemo	67
7.3	Kompilieren der Anwendung WSNDemo	72
7.4	Übertragen der erstellten Images auf die Funkmodule	73
7.5	Inbetriebnahme der Beispielanwendung WSNMonitor	76
7.6	Hinzufügen weiterer Funkmodule zum Netzwerk	77
7.7	Fuse- und Lockbits von Mikrocontrollern	77
7.7.1	Die Fusebits des Atmega 1281	78
7.7.2	Die Lockbits des Atmega 1281	81
8	IEEE 802.15.4	83
8.1	Einleitung	83
8.2	Komponenten und Netzwerktopologien	85
8.3	Grundstruktur	86

9	IEEE 802.15.4 PHY-Schicht	91
9.1	Konstanten und Variablen der PHY-Schicht (PHY-PIB)	91
9.2	Servicedienste und zugehörige Primitiven der PHY-Schicht	93
9.2.1	PHY Data Service	93
9.2.2	Physical Layer Management Entity (PLME)	93
9.3	Modulation und Frequenzen	96
9.3.1	Digitale Phasenmodulation	97
9.3.2	Binary Phase-Shift Keying (BPSK)	97
9.3.3	Offset Quadrature Phase-Shift Keying (O-QPSK)	99
9.3.4	Symboldauer	100
9.3.5	Frequenz- und Modulationswahl	102
9.4	PHY-Frame	104
10	IEEE 802.15.4 MAC-Schicht	107
10.1	Konstanten und Variablen der MAC-Schicht (MAC-PIB)	107
10.2	Funktionsweise von IEEE 802.15.4 Netzen	111
10.2.1	Adressierung	111
10.2.2	Die Bildung eines IEEE 802.15.4 Netzes	111
10.3	Zugriffssteuerung auf den Funkkanal	112
10.3.1	CSMA-CA	112
10.3.2	ALOHA	113
10.3.3	Superframes	114
10.3.4	Steuerung von garantierten Zeitslots (GTS)	117
10.3.5	Zeitabstand zwischen zwei Frames	117
10.4	Datenübertragung	118
10.4.1	Datenübertragung ohne Superframesunterstützung	118
10.4.2	Datenübertragung mit Superframesunterstützung	118
10.5	Servicedienste und zugehörige Primitiven der MAC-Schicht	119
10.5.1	MAC-Datendienst (MCPS)	119
10.5.2	MAC-Managementdienst (MLME)	121
10.6	MAC-Frame	131
10.6.1	Allgemeine MAC-Framestruktur	131
10.6.2	Datenframe	136
10.6.3	Kommandoframe	136
10.6.4	Beaconframe	141
10.6.5	ACK-Frame	144
10.7	Sicherheit	144
10.7.1	Sicherheitsstufen	145
10.7.2	Authentifizierung mittels CBC-MAC	146
10.7.3	Verschlüsselung durch das CTR-Verfahren	146
10.7.4	Anwendung des CCM*-Verfahren im IEEE 802.15.4 Standard	149
10.7.5	AES-Algorithmus	152

10.7.6	Der Schlüssel	154
10.7.7	Das MAC-Frame mit aktivierten Sicherheitsfunktionen	156
10.7.8	Sicherheitsrelevante MAC-Variablen	158
10.7.9	Beispielrechnung für das CCM*-Verfahren	158
11	Atmel IEEE 802.15.4 MAC-Stack	167
11.1	Aufbau des Atmel IEEE 802.15.4 MAC-Stack	167
11.2	Installation und Verzeichnisstruktur des Atmel MAC-Stack	170
11.3	Anpassen des MAC-Stacks an ein eigenes Board	171
11.4	Beispielanwendung eines einfachen Netzwerks	175
11.5	Beispielanwendung zum Sniffen von Datenverkehr	178
11.6	Taskverarbeitung und Callback-Funktionen	180
11.7	Anwendung einer blinkenden LED	182
11.8	Textausgabe über die UART-Schnittstelle	188
11.9	Beitritt in ein PAN	191
11.10	Senden von Daten	195
11.11	Aufbau eines PANs und Empfang von Daten durch den PAN-Koordinator	198
11.12	Ansteuern des Analog-Digital-Wandler (ADC) und Ermittlung der Batteriespannung	204
12	IEEE-802.15.4-Sniffer mit <code>pracoli</code> und Wireshark	209
12.1	Installation von Python und dem Modul <code>pySerial</code>	209
12.2	Installation von Wireshark	210
12.3	Die <code>pracoli</code> -Sniffersoftware	210
12.4	Wireshark	211
13	ZigBee	215
13.1	Einleitung	215
13.2	ZigBee-Architektur	219
13.3	Komponenten und Netzwerktopologien	220
14	ZigBee-Netzwerkschicht	223
14.1	Konstanten und Variablen der Netzwerkschicht (NIB)	223
14.2	Netzaufbau	227
14.3	Adressierung	229
14.3.1	Verfahren zur verteilten Adresszuweisung	229
14.3.2	Zufälliges Adressvergabeverfahren	232
14.4	Routing	233
14.4.1	Pfadkosten	233
14.4.2	Routing entlang des Assoziationsbaums	234
14.4.3	Routing mittels Routingtabellen	236
14.4.4	Broadcastnachrichten	240

14.4.5	Routing zu Gruppen (Multicast Routing)	241
14.4.6	Many-To-One- und Senderrouting	242
14.5	Periodische Beacons (Superframestruktur)	243
14.6	Die Servicedienste und Primitiven der Netzwerkschicht	245
14.6.1	Network Layer Data Entity (NLDE)	248
14.6.2	Network Layer Management Entity (NLME)	248
14.7	NWK-Frame	262
14.7.1	Allgemeine NWK-Framestruktur	262
14.7.2	NWK-Datenframe	266
14.7.3	NWK-Kommandoframe	266
14.7.4	Beispiel NWK-Frame	273
15	ZigBee-Anwendungsschicht	279
15.1	Anwendungsunterstützungsschicht (APS)	279
15.1.1	Konstanten und Variablen der APS-Schicht (AIB)	280
15.1.2	Adressierung mittels Endpunkten	282
15.1.3	Adressierung von Gruppen	282
15.1.4	Binding	283
15.1.5	Zuverlässige Datenübertragung	285
15.1.6	Fragmentierung	286
15.1.7	Servicedienste und zugehörige Primitiven der APS-Schicht	290
15.1.8	APS-Frame	295
15.2	Cluster und Profile	299
15.2.1	Cluster	300
15.2.2	Profile	307
15.3	ZigBee Device Objekt (ZDO)	309
15.3.1	Deskriptoren	310
15.3.2	ZigBee Device Profil (ZDP)	311
15.3.3	Knotenmanagement	314
15.3.4	Ermittlung von Geräten und Diensten (Discovery)	319
15.3.5	Bindingmanagement	326
16	ZigBee-Sicherheit	333
16.1	Sicherheitsstufen	334
16.2	Framestruktur mit aktivierter Sicherheit	335
16.3	Schlüssel	336
16.4	Trustcenter	338
16.5	Sicherheitsdienste der APS-Schicht	338
16.5.1	Schlüsselanfrage (APSME-REQUEST-KEY)	339
16.5.2	Schlüsseltransport (APSME-TRANSPORT-KEY)	340
16.5.3	Wechsel des aktiven Netzwerkschlüssels (APSME-SWITCH-KEY)	342

16.5.4	Generieren eines Linkschlüssels für eine End-zu-End-Verbindung (APSME-ESTABLISH-KEY)	343
16.5.5	Trustcenter über den Status der Funkmodule informieren (APSME-UPDATE-DEVICE)	346
16.5.6	Funkmodul aus dem Netzwerk entfernen (APSME-REMOVE-DEVICE)	347
16.5.7	Gegenseitige Authentifizierung zweier Funkmodule (APSME-AUTHENTICATE)	348
16.5.8	Tunneln von APS-Kommandoframes des Trustcenters	351
16.5.9	Festlegen von Berechtigungen zum Ausführen von Diensten	351
16.6	Hashing	352
16.6.1	Hashfunktion Matyas-Meyer-Oseas	353
16.6.2	HMAC	355
17	Atmel BitCloud	357
17.1	Aufbau des BitCloud-Stack	357
17.2	BitCloud Taskmanager	359
17.3	Anwendung einer blinkenden LED	361
17.4	Portierung an ein eigenes Funkmodul	364
17.5	Blink-Anwendung als Zustandsautomat	370
17.6	Ausgabe über die UART-Schnittstelle	373
17.7	Ein UART-Manager bei größeren Ausgabenmengen	376
17.8	Datenempfang über die UART-Schnittstelle	380
17.9	Programmierung eines ZigBee-Funknetzwerks	383
17.9.1	Der Aufbau eines Netzwerks und die Einstellung der Parameter	383
17.10	Datenübertragung	388
17.11	I ² C-Bus und Temperatursensor LM73	395
17.12	Ein Fotowiderstand an einem A/D-Wandler	400
	Übersetzungswörterbuch Deutsch-Englisch	403
	Definition und Kurzerklärungen von Begriffen	407
	Literatur	411
	Sachverzeichnis	415