

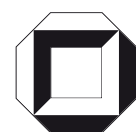
Erik-Oliver Blaß

**Sicherer, aggregierender Datentransport  
in drahtlosen Sensornetzen**



# **Sicherer, aggregierender Datentransport in drahtlosen Sensornetzen**

von  
Erik-Oliver Blaß



---

universitätsverlag karlsruhe

Dissertation, Universität Karlsruhe (TH)  
Fakultät für Informatik, 2007

## **Impressum**

Universitätsverlag Karlsruhe  
c/o Universitätsbibliothek  
Straße am Forum 2  
D-76131 Karlsruhe  
www.uvka.de



Dieses Werk ist unter folgender Creative Commons-Lizenz  
lizenziert: <http://creativecommons.org/licenses/by-nc-nd/2.0/de/>

Universitätsverlag Karlsruhe 2007  
Print on Demand

ISBN: 978-3-86644-142-2





# Sicherer, aggregierender Datentransport in drahtlosen Sensornetzen

zur Erlangung des akademischen Grades eines

DOKTORS DER NATURWISSENSCHAFTEN

der Fakultät für Informatik  
der Universität Fridericiana zu Karlsruhe (TH)

genehmigte

**Dissertation**

von

**Dipl.-Inform. Erik-Oliver Blaß**

aus Wuppertal

Tag der mündlichen Prüfung: 20. April 2007

Erster Gutachter: Prof. Dr. Martina Zitterbart  
Universität Karlsruhe (TH)

Zweiter Gutachter: Prof. Dr. Felix Freiling  
Universität Mannheim





—TEMPUS FUGIT!  
Für Papa



---

# Danksagung

---

Frau Professor Dr. Martina Zitterbart danke ich für die Leitung dieser Arbeit und für zahlreiche Anregungen und Ratschläge im Verlaufe ihrer Durchführung. Herrn Prof. Dr. Felix Freiling danke ich für die Übernahme des Korreferats und für wertvolle Hinweise auch auf formale Aspekte dieser Arbeit.

Danke den Wissenschaftlern Dr. Roland Bless, Dr. Curt Cramer, Dr. Artur Hecker (MCF) und Dipl.-Inform. Bernhard Hurler für zahlreiche Hilfestellungen und Diskussionen.



---

# Inhaltsverzeichnis

---

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Problemstellung . . . . .	2
1.2	Ziel der Arbeit . . . . .	4
1.3	Ergebnisse und Gliederung der Arbeit . . . . .	5
<b>2</b>	<b>Grundlagen und Annahmen</b>	<b>7</b>
2.1	Beispielszenarien . . . . .	7
2.1.1	Betreutes Wohnen . . . . .	8
2.1.2	Überwachen von Kernwaffentests . . . . .	10
2.2	Merkmale drahtloser Sensornetze . . . . .	11
2.2.1	Ressourcenarmut . . . . .	12
2.2.2	Fehlende Infrastrukturen . . . . .	14
2.2.3	Selbstorganisation und Spontaneität . . . . .	15
2.2.4	Kommunikationsfluß: Aggregation . . . . .	16
2.2.5	Dynamisches Netzverhalten . . . . .	22
2.3	Weitere Annahmen . . . . .	23
2.4	Angreifermodell . . . . .	24
2.4.1	Ziele des Angreifers: Angriffe und Bedrohungen . . . . .	24
2.4.2	Charakterisierung des Angreifers . . . . .	26
2.4.3	Anzahl korrumpierter Knoten $\mathcal{B}$ . . . . .	31
2.4.4	Annahmen über Blätter und Senke . . . . .	32
2.4.5	Denial-of-Service . . . . .	33
2.5	Herleitung der Unterprobleme . . . . .	34
2.5.1	Schlüsselaustausch . . . . .	34
2.5.2	Authentischer Datentransport . . . . .	35

2.6	Grundlagen zur Sicherheit . . . . .	36
2.6.1	Kryptographische Schlüssel . . . . .	36
2.6.1.1	Ver- und Entschlüsseln . . . . .	36
2.6.1.2	Symmetrische Verschlüsselung . . . . .	37
2.6.1.3	Asymmetrische Verschlüsselung . . . . .	38
2.6.1.4	Vergleichen von Schlüssellängen . . . . .	38
2.6.1.5	Fazit: Verschlüsselung in Sensornetzen . . . . .	39
2.6.1.6	Annahmen über Verschlüsselung in dieser Arbeit . . . . .	39
2.6.2	Authentizität . . . . .	41
2.6.2.1	Authentizität mit asymmetrische Kryptographie . . . . .	41
2.6.2.2	Authentizität mit symmetrischer Kryptographie . . . . .	41
2.6.2.3	Authentizität in Sensornetzen . . . . .	43
2.6.2.4	Annahmen über Authentizität . . . . .	44
2.6.2.5	Non-Repudiation in dieser Arbeit . . . . .	45
2.6.3	Zerteilen von Geheimnissen . . . . .	46
2.7	Zusammenfassung . . . . .	46
<b>3</b>	<b>Schlüsselaustausch</b>	<b>47</b>
3.1	Motivation . . . . .	47
3.1.1	Neue Herausforderungen . . . . .	48
3.1.1.1	Ressourcenarmut . . . . .	48
3.1.1.2	Fehlende Infrastrukturen . . . . .	48
3.1.1.3	Selbstorganisation und Spontaneität . . . . .	49
3.1.1.4	Kommunikationsflur: Aggregation . . . . .	49
3.1.1.5	Dynamisches Netzverhalten . . . . .	50
3.1.2	Entwurfsziele und erwartete Ergebnisse . . . . .	51
3.2	Stand der Forschung . . . . .	52
3.2.1	Public-Key Varianten . . . . .	52
3.2.2	Einsatz dedizierter Knoten . . . . .	54
3.2.3	Annahmen über sicheres Deployment . . . . .	55
3.2.4	Zufallsverteilte Schlüssellisten . . . . .	57
3.2.5	Deterministisch verteilte Schlüssellisten . . . . .	58
3.2.6	Weitere Arbeiten . . . . .	59

---

3.2.7	Perfect Forward Secrecy . . . . .	61
3.2.8	Zusammenfassung . . . . .	62
3.3	Das Protokoll SKEY . . . . .	63
3.3.1	Protokollidee . . . . .	64
3.3.2	Erläuterungen zum Pseudocode . . . . .	66
3.3.3	Protokollbeschreibung . . . . .	67
3.3.3.1	Initiales Paaren über ein Master Device . . . . .	67
3.3.3.2	Sichere Schlüsselweiterleitung . . . . .	70
3.3.4	SKEY Sicherheit . . . . .	77
3.3.4.1	Sicherheit gegen korrumpierte Knoten . . . . .	78
3.3.4.2	Denial-of-Service . . . . .	79
3.3.4.3	Spoofing . . . . .	79
3.3.5	Erweiterung auf $k$ korrumpierte Knoten . . . . .	79
3.3.5.1	Beschreibung . . . . .	80
3.3.5.2	Bestimmen von $k$ . . . . .	81
3.3.6	Finden mehrerer initialer Zufallsknoten . . . . .	83
3.3.7	Finden der Vorgängerknoten . . . . .	85
3.3.8	Dynamische Aggregation . . . . .	87
3.3.8.1	Auswirkungen durch Änderungen der Aggregation . . . . .	88
3.3.8.2	Dynamisches Anpassen von $k$ . . . . .	89
3.4	Evaluierung . . . . .	89
3.4.1	Speicherverbrauch . . . . .	89
3.4.2	Energieverbrauch . . . . .	90
3.4.3	Simulation . . . . .	91
3.4.3.1	Simulationsumgebung . . . . .	93
3.4.3.2	Simulationsergebnisse – Statische Simulationen . . . . .	95
3.4.3.3	Simulationsergebnisse – Dynamische Simulationen . . . . .	100
3.4.3.4	Simulationsergebnisse – Simulationen von Angreifern . . . . .	102
3.4.4	Ergebnisse im Überblick . . . . .	105
3.5	Zusammenfassung . . . . .	106

<b>4</b>	<b>Authentische Aggregation</b>	<b>109</b>
4.1	Motivation . . . . .	109
4.1.1	Neue Herausforderungen . . . . .	110
4.1.1.1	Kommunikationsflu: Aggregation . . . . .	110
4.1.1.2	Ressourcenarmut . . . . .	111
4.1.1.3	Übrige Anforderungen . . . . .	111
4.1.2	Entwurfsziele und erwartete Ergebnisse . . . . .	111
4.2	Stand der Forschung . . . . .	113
4.2.1	Authentizität durch Homomorphismen . . . . .	113
4.2.2	Einschränkung der Aggregationsfunktion . . . . .	115
4.2.3	Verfahren zur Klassifizierung von Daten . . . . .	116
4.2.4	Weitere Arbeiten . . . . .	117
4.2.5	Zusammenfassung . . . . .	120
4.3	Das Protokoll ESAWN . . . . .	121
4.3.1	Protokollidee . . . . .	124
4.3.2	Erläuterungen zum Pseudocode . . . . .	126
4.3.3	Protokollbeschreibung . . . . .	127
4.3.3.1	Auswahl von $k$ Zeugen . . . . .	131
4.3.3.2	Ablauf der Verifikation . . . . .	132
4.3.3.3	Kenntnis von IP . . . . .	136
4.3.3.4	Probabilistische Verifikation . . . . .	137
4.3.3.5	Verteilung des Seeds . . . . .	137
4.3.4	ESAWNs Sicherheit . . . . .	138
4.3.4.1	Beispiel mit $k=2$ . . . . .	139
4.3.4.2	error-Nachricht . . . . .	140
4.3.5	Auswirkung probabilistischer Überprüfung . . . . .	141
4.3.6	Sicherheitsbetrachtung: Wahl von $k$ und $p$ . . . . .	143
4.3.7	Diskussion über die Vollständigkeit von ESAWN . . . . .	144
4.3.8	Korrektheitsbeweis für ESAWN . . . . .	146
4.4	Evaluierung . . . . .	149
4.4.1	Speicherverbrauch . . . . .	149
4.4.2	Energieverbrauch . . . . .	150



4.4.2.1	Authentische Nicht-Aggregation . . . . .	150
4.4.2.2	Nicht-Authentische Aggregation . . . . .	151
4.4.2.3	Sichere Aggregation mit ESAWN . . . . .	151
4.4.3	Simulation . . . . .	153
4.4.3.1	Energieverbrauch . . . . .	153
4.4.3.2	Sicherheit von ESAWN – WKA . . . . .	158
4.4.3.3	Zum Verlauf der WKA-Kurven . . . . .	164
4.4.4	Wahl von $k$ bei ESAWN und SKEY . . . . .	165
4.4.5	Kombinierter Aufwand von SKEY und ESAWN . . . . .	165
4.4.6	Ergebnisse im Überblick . . . . .	165
4.5	Zusammenfassung . . . . .	166
<b>5</b>	<b>Zusammenfassung und Ausblick</b>	<b>169</b>
5.1	Ergebnisse der Arbeit . . . . .	170
5.2	Weiterführende Arbeiten . . . . .	171
<b>A</b>	<b>Zum Energieverbrauch der MICA2-Knoten</b>	<b>173</b>
<b>B</b>	<b>Analyse zufallsverteilter Schlüssellisten</b>	<b>175</b>
B.1	Funktionsweise . . . . .	175
B.2	Analyse . . . . .	176
B.2.1	Simulation von Angreifern . . . . .	178
B.2.2	Simulation von Dynamik . . . . .	182
B.2.3	Maximaler Speicherverbrauch . . . . .	183
B.2.4	Rücknahme von Schlüsseln . . . . .	185
<b>C</b>	<b>Simulationen zum 802.11 MAC-Verhalten</b>	<b>187</b>
C.1	Simulationen mit 802.11 MAC . . . . .	187
C.2	Simulationsergebnisse . . . . .	188
C.3	Zusammenfassung . . . . .	192
<b>D</b>	<b>Simulationen zu <math>k</math> und <math>p</math></b>	<b>193</b>
<b>E</b>	<b>Symbole</b>	<b>197</b>
	<b>Literaturverzeichnis</b>	<b>199</b>



---

# Abbildungsverzeichnis

---

1.1	Leseflüsse durch die Kapitel . . . . .	6
2.1	Beispiel für ein einfaches Sensornetz, alle roten Punkte sind Sensoren . . . . .	9
2.2	Weltweite Positionen von radionuklidischen Sensorfeldern . . . . .	10
2.3	MICA2-Mote [66], zwei 1,5V AAA Batterien auf der Unterseite . . . . .	13
2.4	Aggregation als baumartiger Kommunikationsfluß . . . . .	17
2.5	Ein Aggregationsbaum $G$ aus zwei Aggregationsteilbäumen $G'_1, G'_2$ . . . . .	21
3.1	Schlüsselverteilung im Aggregationsbaum . . . . .	50
3.2	Beitritt von Knoten $i$ , initiale Zufallsknoten sind $e$ und $d$ . . . . .	64
3.3	Veranschaulichung des Protokollablaufs . . . . .	65
3.4	Teilen und Versenden von $K_{i,f}$ . . . . .	74
3.5	Zurücksenden der Schlüsselteile an $f$ . . . . .	75
3.6	Ein etwas komplizierteres Beispiel . . . . .	76
3.7	SKEY bei $k$ korrumpierten Knoten . . . . .	81
3.8	Theoretischer Verlauf von $k$ in Abhängigkeit von $\beta$ . . . . .	82
3.9	Wahrscheinlichkeiten für $\geq k + 1$ funktionsfähige Knoten . . . . .	84
3.10	Knoten $c$ übernimmt $b$ 's Aggregationsbeziehungen . . . . .	88
3.11	SKEY-Speicherverbrauch, zur rel. Standardabweichung siehe Text . . . . .	96
3.12	Speicherverbrauch, Vergleich zwischen SKEY und [88](=EGLI) . . . . .	98
3.13	Energieverbrauch SKEY mit unterschiedlichen Parametern . . . . .	99
3.14	Energieverbrauch, Vergleich zwischen SKEY und [88] . . . . .	101
3.15	Reorganisation, Mehraufwand von [88] gegenüber SKEY, $\delta = 3$ . . . . .	102
3.16	Anteil gebrochener Assoziationen bei SKEY, Aggregationsgrad $\delta = 3$ . . . . .	103
3.17	Assoziationssicherheit, Vergleich SKEY und [88], $n = 5000$ Knoten . . . . .	104
4.1	Einfache Aggregation . . . . .	110

4.2	Graduelle Authentizität würde variablen Energieverbrauch bedeuten . . . . .	122
4.3	Veranschaulichung des Protokollablaufs . . . . .	124
4.4	Nachfolger von $v$ im Aggregationsbaum: $\mathbb{S}$ aus Algorithmus 12 . . . . .	126
4.5	Idee der Aggregationsüberprüfung durch Zeugen . . . . .	127
4.6	Auswahl von Zeugen in Abhängigkeit von $k$ . . . . .	131
4.7	Auswahl von $k$ Zeugen, mindestens ein Zeuge nicht kompromittiert . . . . .	138
4.8	Theoretischer Verlauf der WKA, $\delta = 4$ . . . . .	142
4.9	Zum Beweis über Teilbäume des gesamten Baums . . . . .	149
4.10	Speicherverbrauch von ESAWN . . . . .	150
4.11	Energiekosten für komplette Aggregation, $\delta = 3$ . . . . .	154
4.12	Relative Energiekosten von ESAWN . . . . .	156
4.13	Relative Energiekosten von ESAWN III . . . . .	157
4.14	Relative Energiekosten von ESAWN IV . . . . .	158
4.15	ESAWN Energieaufwand, $\beta = \{1, 10\}\%$ . . . . .	161
4.16	ESAWN Energieaufwand, $\beta = 20\%$ . . . . .	162
4.17	Verlauf der WKA in Abhängigkeit von $p$ , $\beta = 1\%$ . . . . .	164
B.1	Auswirkungen korrumpierter Knoten bei $n = 1000$ . . . . .	180
B.2	Auswirkungen korrumpierter Knoten bei $n = 3000$ . . . . .	180
B.3	Auswirkungen korrumpierter Knoten bei $n = 5000$ . . . . .	181
B.4	Auswirkungen von Knotenausfall auf gültige Schlüssel, $n = 1000$ . . . . .	183
B.5	Auswirkungen von Knotenausfall auf gültige Schlüssel, $n = 3000$ . . . . .	184
B.6	Auswirkungen von Knotenausfall auf gültige Schlüssel, $n = 5000$ . . . . .	184
B.7	Maximaler Speicherverbrauch pro Knoten . . . . .	185
C.1	ESAWN-Energieaufwand ohne und mit 802.11 MAC, jeweils $p = 100\%$ . . . . .	189
C.2	ESAWN-Energieaufwand ohne und mit 802.11 MAC, jeweils $p = 50\%$ . . . . .	190
C.3	SKEY-Energieaufwand ohne und mit 802.11 MAC . . . . .	191

---

# Tabellenverzeichnis

---

3.1	Stand der Forschung <i>Schlüsselaustausch</i> . . . . .	62
3.2	Übersicht: Parameter für Simulationen . . . . .	95
4.1	Stand der Forschung <i>authentische Aggregation</i> . . . . .	121
4.2	Zum Beispiel mit $k = 2$ , Daten auf den einzelnen Knoten. . . . .	139
B.1	Parameterwahl für Simulationen . . . . .	179
C.1	Auswirkungen von Bit Error Rates auf das Energieverhältnis . . . . .	192
D.1	Energetisch günstigste $k$ und $p$ bei verschiedenen $n$ und $\beta = 1\%$ . . . . .	194
D.2	$\beta = 10\%$ . . . . .	194
D.3	$\beta = 20\%$ . . . . .	195
E.1	Symbole und ihre Bedeutung . . . . .	197



---

# Liste der Algorithmen

---

1	Hinzufügen eines neuen Knotens $i$ ins Sensornetz . . . . .	67
2	$\text{pairNode}(i, k, K_{MD}, \text{MAXNODES})$ . . . . .	68
3	$i.\text{introduceToIRN}()$ . . . . .	70
4	$i.\text{exchangeKeys}()$ . . . . .	71
5	$m.\text{error}$ . . . . .	71
6	$\text{splitKey}(K, s)$ , Idee siehe Abschnitt 2.6.3, S. 46 . . . . .	72
7	$m.\text{forwardShare}(i, K^m, x)$ . . . . .	73
8	$m.\text{sendToNode}(i, K^m, x)$ . . . . .	73
9	$i.\text{getIP}()$ . . . . .	86
10	$m.\text{findIP}(i, \text{purpose})$ . . . . .	87
11	$v.\text{doMeasure}(k, \text{SEEDS}, p, \Pi)$ . . . . .	128
12	$v.\text{doAggregate}(k, \text{SEEDS}, p, \Pi, \mathbb{S})$ . . . . .	129
13	$v.\text{receiveFromNodes}(i, p, \Pi, \mathbb{S})$ . . . . .	130
14	$v.\text{checkAggregates}(\text{AggStore}, \text{AggStore}', j, \text{SEEDS}, \Pi, \mathbb{S})$ . . . . .	130
15	Ein mögliches $v.\text{error}(\Pi, j)$ . . . . .	131
16	$v.\text{computeAggregates}(\text{AggStoreIn}, p, i, \mathbb{S})$ . . . . .	134
17	Pseudocode zum Berechnen von WKA's . . . . .	160

