

Inhaltsverzeichnis

Abbildungsverzeichnis	xvii
Tabellenverzeichnis	xxi
Abkürzungsverzeichnis	xxiii
1 Einleitung	1
1.1 Motivation und Ziele	1
1.2 Aufbau der Arbeit	3
1.3 Neue Erkenntnisse dieser Arbeit	5
2 Grundlagen und Forschungsübersicht	7
2.1 Begriffe	7
2.1.1 Mobiles Ad-hoc-Netz	7
2.1.2 Automobiles Ad-hoc-Netz	8
2.1.3 Mehrseitige Sicherheit	10
2.1.4 Effizienz	11
2.2 Forschungsübersicht	13
2.2.1 Förderprogramme und Konsortien	13
2.2.2 Projekte	16
3 Schutzziele, Anwendungen und Angreifermodelle	19
3.1 Schutzziele	19
3.1.1 Vertraulichkeit	20
3.1.2 Integrität	24
3.1.3 Verfügbarkeit	28
3.2 Anwendungen	30
3.2.1 Bestehende Kategorisierungen	31
3.2.2 Telematik-Nachrichten	32
3.2.3 Anwendungskategorie 1: Beacons (A1)	34
3.2.4 Anwendungskategorie 2: Warnungen (A2)	36

3.2.5	Anwendungskategorie 3: Alarmsignale und Anweisungen (A3)	41
3.2.6	Anwendungskategorie 4: Komfort-Dienste (A4)	44
3.3	Angreifermodelle	47
3.3.1	Mögliche Ausprägungen eines Angreifers	47
3.3.2	Konkrete Angreifermodelle	50
3.3.3	Beispiele für Angriffe	53
4	Vorüberlegungen und Annahmen	55
4.1	Architektur-Überblick	55
4.2	VANET-Identität	57
4.2.1	Fahrzeugbezogene Identität	57
4.2.2	Personenbezogene Identität	58
4.2.3	Gemischte Identität	60
4.2.4	Fazit	60
4.3	Manipulationssichere Hardware	61
4.3.1	Notwendigkeit	61
4.3.2	Sicherheit	62
4.3.3	Fazit	63
4.4	Public-Key-Infrastruktur	63
4.4.1	Komponenten	64
4.4.2	Zertifikate und ihr Management	66
4.5	Trusted Third Party	67
4.5.1	Auswahlkriterien	68
4.5.2	Automobilhersteller	69
4.5.3	Unabhängige Organisationen	70
4.5.4	Staatliche Stellen	71
4.5.5	Fazit	72
4.6	Datenübertragungsstandards für mobile Anwendungen	73
4.6.1	Anforderungen	73
4.6.2	Protokolle	75
4.6.3	Fazit	77
4.7	Routing	77
4.7.1	Topologiebasiert	78
4.7.2	Positionsbasiert	79
4.7.3	Fazit	80
4.8	Intrusion Detection und Anreizsysteme	81
4.8.1	Reaktionsmöglichkeiten	81
4.8.2	Erkennung von Fehlverhalten und Reputationssysteme	83
4.8.3	Anreizsysteme	89
4.8.4	Fazit	90
4.9	Annahmen	91

5	Bausteine	95
5.1	Zertifikatsrückruf-Systeme	95
5.1.1	Auswahlkriterien und Vorauswahl	96
5.1.2	Certificate Revocation Status nach KARGL	98
5.1.3	2-3 CRT	102
5.1.4	Rückrufe nach RAYA et al.	104
5.1.5	ADOPT	106
5.1.6	MANET Certificate Revocation Lists	107
5.1.7	MANET Revocation Scheme nach ARBOIT et al.	108
5.1.8	Kurzzeit-Zertifikate	109
5.1.9	Fazit	109
5.2	Positions- und Zeitbestimmung	110
5.2.1	Möglichkeiten und Vorauswahl	110
5.2.2	Auswahlkriterien	114
5.2.3	Positionsbestimmung mit versteckten und mobilen Basisstationen	115
5.2.4	HiRLoc	117
5.2.5	Verifiable Multilateration bzw. SPINE	119
5.2.6	ROPE	124
5.2.7	SecNav	125
5.2.8	Galileo	127
5.2.9	Fazit	130
5.3	Performance kryptographischer Verfahren	131
5.3.1	Sicherheitslevel	131
5.3.2	Messmethodik und Testaufbau	134
5.3.3	Ergebnisse	136
6	VANET-Sicherheitsinfrastrukturen	139
6.1	Anforderungen	139
6.1.1	Integrität	139
6.1.2	Vertraulichkeit	141
6.1.3	Performance	141
6.1.4	Wirtschaftlichkeit und Akzeptanz	142
6.1.5	Hinweise zu den Bewertungen	142
6.2	Ansätze aus dem MANET-Umfeld	144
6.2.1	Verteilte CA	144
6.2.2	Identitätsbasierte Kryptosysteme	149
6.2.3	Web of Trust – Ad-Hoc	151
6.2.4	Neighborhood Key Method	154
6.2.5	Pairwise Keys	156
6.2.6	Kaman	157
6.2.7	SAM	160
6.2.8	Zusammenfassung	165

6.3	Ansätze für VANETs	165
6.3.1	Verfahren von CHOI, JAKOBSSON und WETZEL	165
6.3.2	Identitätsbasiertes System nach KAMAT et al.	170
6.3.3	Ansatz von HUBAUX et al.	172
6.3.4	IEEE Standard 1609.2	177
6.3.5	Efficient Secure Aggregation nach RAYA	178
6.3.6	Verfahren nach CALANDRIELLO et al.	181
6.3.7	PKI+	185
6.3.8	Zusammenfassung	187
6.4	Ansätze zum Schutz der Privatsphäre in VANETs	188
6.4.1	Mix-Contexts nach GERLACH	188
6.4.2	Spatial und Temporal Cloaking nach GRUTESER und GRUNWALD	191
6.4.3	Mix-Zones nach FREUDIGER et al.	194
6.4.4	AMOEBA	196
6.4.5	Zusammenfassung	205
7	Mehrseitig sichere VANET-Sicherheitsinfrastruktur	207
7.1	Initialisierung	208
7.1.1	Überblick	208
7.1.2	Genauer Ablauf	208
7.2	Alltäglicher Einsatz	211
7.2.1	Warnungen	212
7.2.2	Alarmmeldungen und Anweisungen	213
7.2.3	Anmeldung am symmetrischen Teil	215
7.2.4	Absicherung mit symmetrischer Kryptographie	219
7.3	Verkettbarkeit von Beacons	222
7.3.1	Sendehäufigkeit	223
7.3.2	Unverkettbarkeit durch Mix-Zonen	230
7.3.3	Alternativen für fest zugeteilte Pseudonyme	238
7.4	Konkrete Ausgestaltungsvorschläge	242
7.4.1	Kryptographische Algorithmen und Schlüssellängen	242
7.4.2	Schlüsselwechselintervall	244
7.4.3	Verteilung der Mix-Zonen	248
7.4.4	Verwendung von Pseudozufallszahlen	251
7.5	Bewertung und Vergleich	254
7.5.1	Asymmetrisch gesicherter Teil	254
7.5.2	Symmetrisch gesicherter Teil	256
7.5.3	Erweiterung <i>PRAND</i>	258
7.5.4	Erweiterung Mix-Zonen	259
7.5.5	Vergleich	259

8 Fazit	265
8.1 Ergebnisse der Arbeit	265
8.2 Ausblick	267
Literaturverzeichnis	269