

Projekt Programmierung (PP)

Aufgabenstellungen TI

Betreuer

Michael Reyer reyer@ti.rwth-aachen.de

Florian Schröder schroeder@ti.rwth-aachen.de

Forschungsgebiete am Lehrstuhl TI

Funknetzplanung und
-optimierung

Informationstheorie

Kryptographie

Modellierung und Analyse
von MIMO-Systemen

Kapazitätsbestimmung
von Vektorkanälen

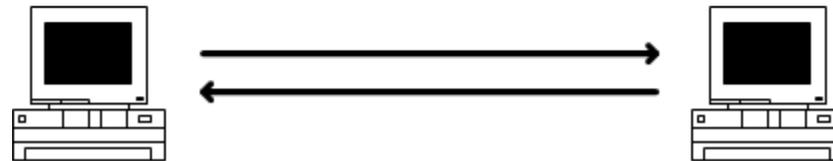
Elliptische Kurven

Ressourcenallokation in
OFDM-Systemen

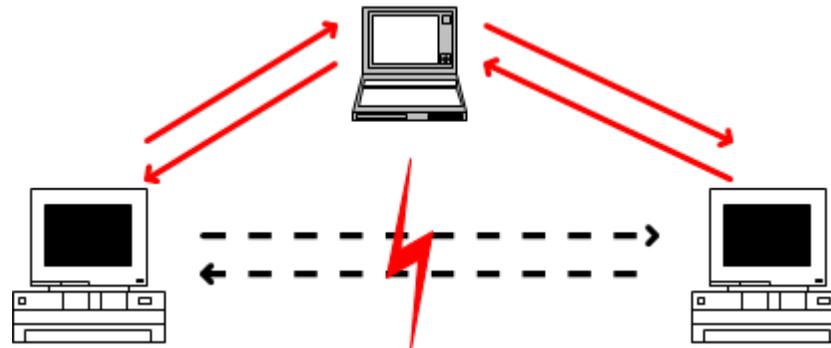
Signalverarbeitung in
Ad-hoc Netzwerken

Paarungsbasierte
Kryptographie

➡ PP am TI: Objektorientierte Umsetzung von Algorithmen



Kommunikation in Netzwerken

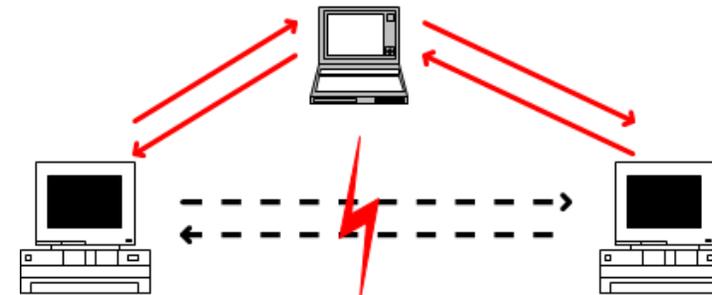


Kommunikation in Netzwerken kann mitgelesen werden!

Kommunikation in Netzwerken kann mitgelesen werden:

- Routing über unbekannte Rechner
- Böswillige Umleitung der Daten
- Man-in-the-middle-Attacken

No.	Time	Source	Destination	Protocol	Info
27	0.110507	134.130.35.81	217.10.10.194	Jabber	Request:
30	0.152295	217.10.10.194	134.130.35.81	TCP	xmpp-client > 4794 [ACK] Seq=0 Ack=1 Win=811 Len=0 TSv=
329	4.289833	134.130.35.81	217.10.10.194	Jabber	Request: <message id='aadfa' to='tobias000@jabber.ccc
329	4.319155	217.10.10.194	134.130.35.81	TCP	xmpp-client > 4794 [ACK] Seq=0 Ack=119 Win=811 Len=0 T!
716	19.153077	134.130.35.81	217.10.10.194	Jabber	Request: <message type='chat' id='aadfa' to='tobias000
718	19.181812	217.10.10.194	134.130.35.81	TCP	xmpp-client > 4794 [ACK] Seq=0 Ack=333 Win=828 Len=0 T!
785	23.214737	134.130.35.81	217.10.10.194	Jabber	Request: <message id='aadfa' to='tobias000@jabber.ccc
785	23.243414	217.10.10.194	134.130.35.81	TCP	xmpp-client > 4794 [ACK] Seq=0 Ack=451 Win=828 Len=0 T!
957	30.442404	217.10.10.194	134.130.35.81	Jabber	Response: <message from='tobias000@jabber.ccc.de/Psi'
958	30.442519	134.130.35.81	217.10.10.194	TCP	4794 > xmpp-client [ACK] Seq=451 Ack=146 Win=3308 Len=
1016	32.744863	217.10.10.194	134.130.35.81	Jabber	Response: <message from='tobias000@jabber.ccc.de/Psi'
1017	32.744888	134.130.35.81	217.10.10.194	TCP	4794 > xmpp-client [ACK] Seq=451 Ack=314 Win=3308 Len=
1022	32.827983	134.130.35.81	217.10.10.194	Jabber	Request: <message type='chat' id='aae1a' to='tobias000
1023	32.857904	217.10.10.194	134.130.35.81	TCP	xmpp-client > 4794 [ACK] Seq=314 Ack=641 Win=845 Len=0
1031	34.027020	134.130.35.81	217.10.10.194	Jabber	Request: <message id='aae2a' to='tobias000@jabber.ccc
1032	34.055127	217.10.10.194	134.130.35.81	TCP	xmpp-client > 4794 [ACK] Seq=314 Ack=756 Win=845 Len=0
1227	41.275484	134.130.35.81	217.10.10.194	Jabber	Request: <message type='chat' id='aae3a' to='tobias000
1228	41.304379	217.10.10.194	134.130.35.81	TCP	xmpp-client > 4794 [ACK] Seq=314 Ack=936 Win=861 Len=0
1235	41.703953	217.10.10.194	134.130.35.81	Jabber	Response: <message from='tobias000@jabber.ccc.de/Psi'
1236	41.703936	134.130.35.81	217.10.10.194	TCP	4794 > xmpp-client [ACK] Seq=936 Ack=460 Win=3308 Len=
1278	42.485070	217.10.10.194	134.130.35.81	Jabber	Response: <message from='tobias000@jabber.ccc.de/Psi'
1279	42.485083	134.130.35.81	217.10.10.194	TCP	4794 > xmpp-client [ACK] Seq=936 Ack=629 Win=3308 Len=



➡ Wie kann man in unsicheren Netzen sicher kommunizieren?

Aufgabe

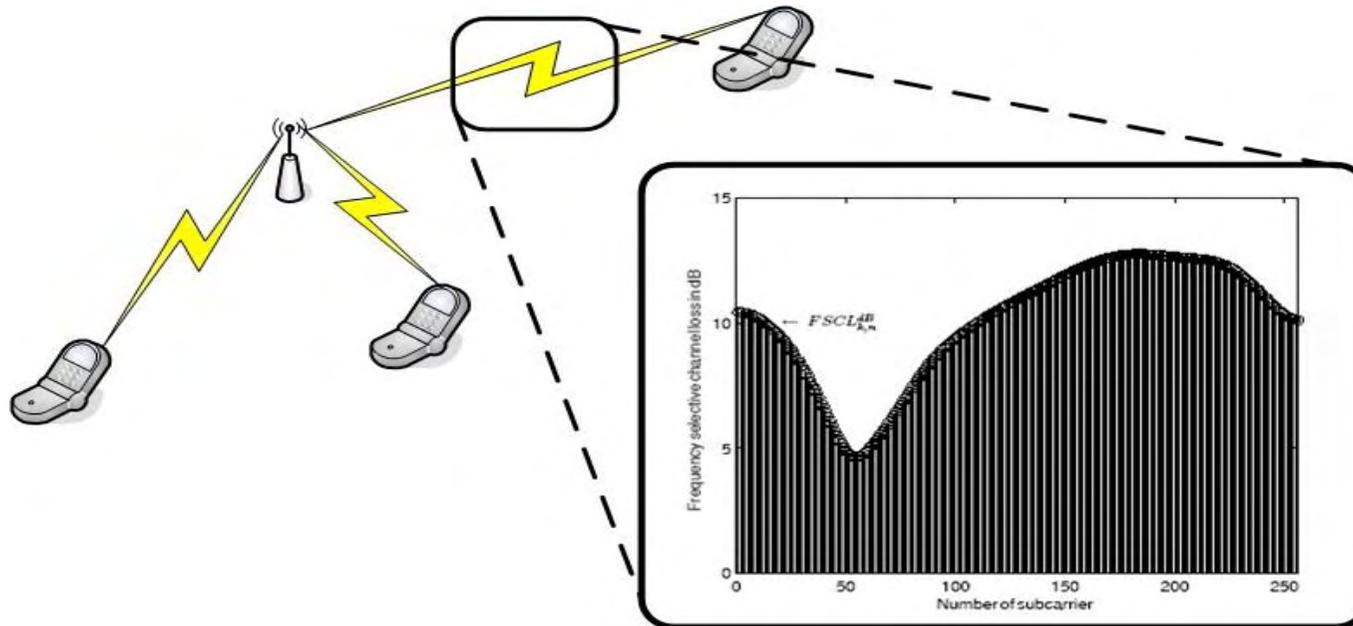
Implementierung eines kryptographisch gesicherten Chatclients

Aspekte des Projekts:

- Diffie-Hellman-Schlüsselaustauschprotokoll
- Symmetrische Verschlüsselungsverfahren (XOR, DES, AES,...)
- Angriffe (Sniffing, Man-in-the-middle)
- GUI (Chat-Programm)
- Kommunikation (TCP/IP)



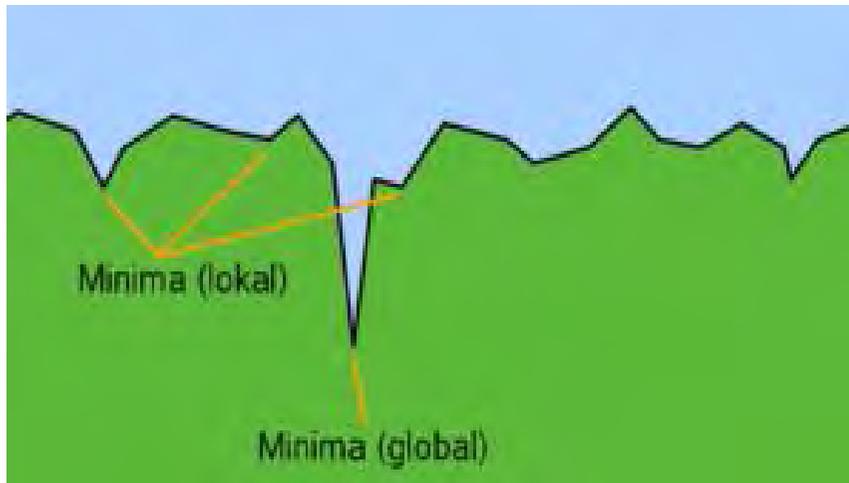
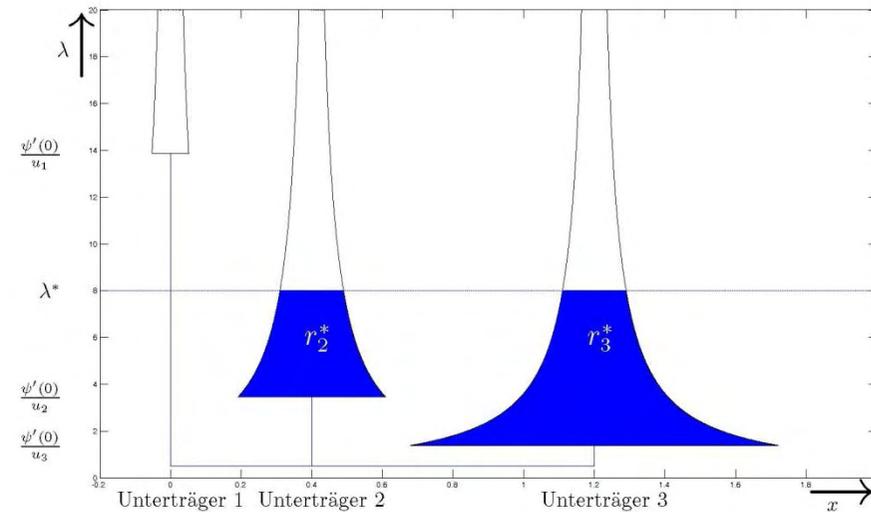
Mobilfunk mit hohen Datenraten



Ein breitbandiger Kanal ist frequenzselektiv

- Leistungszuweisung verbessert die Effizienz
- Geschickte Unterträgerzuweisung erhöht die Kapazität

Leistungszuweisung mittels Water-Filling



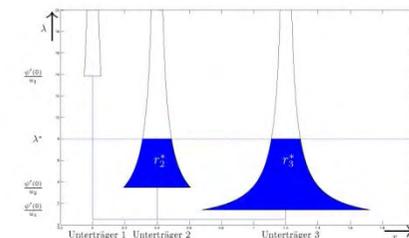
Unterträgerzuweisung mittels Simulated Annealing

Aufgabe

Ressourcenallokation in OFDM-Systemen mittels Simulated Annealing

Aspekte des Projekts:

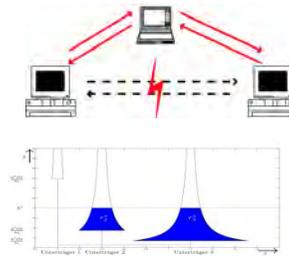
- Leistungszuweisung (Water-Filling, ...)
- Unterträgerzuweisung (Simulated Annealing, Heuristiken, ...)
- Vergleich der Verfahren
- GUI



- Programmiersprache
C++
- Bibliotheken
STL, BOOST und *QT*
- Gemeinsame Projektverwaltung
Subversion
- Dokumentation
Doxygen

Projekte:

- **Crypto-Chat**
- **OFDM mit SA**



Wenn ihr noch Fragen habt, wendet euch an

Michael Reyer reyer@ti.rwth-aachen.de

Florian Schröder schroeder@ti.rwth-aachen.de