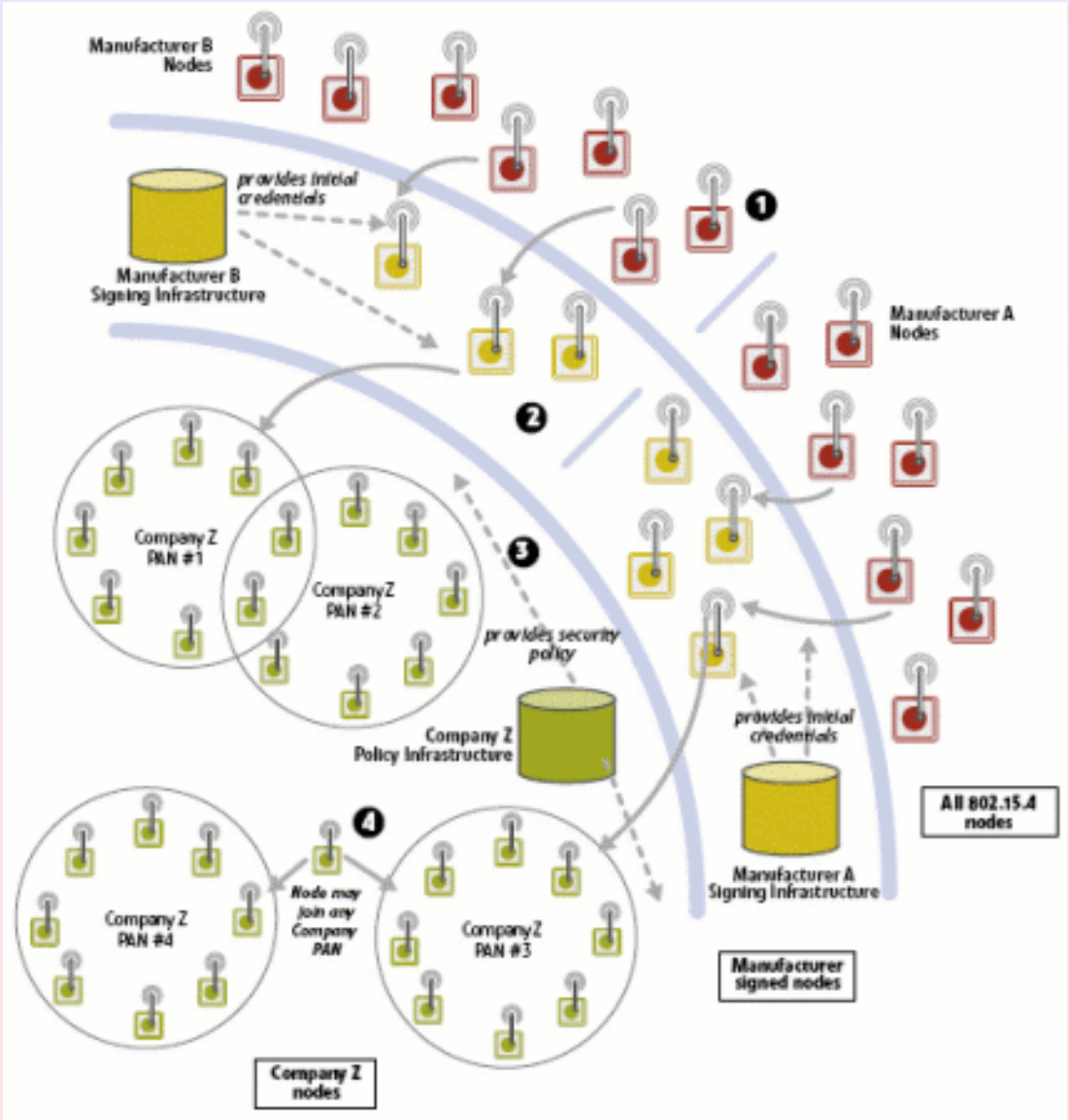
Kabellose Sensornetze: ZigBee, Bluetooth & co.

Marcel Noe

TNG Technology Consulting GmbH

Überblick

Was ist ein Sensornetz?



- Netzwerk aus vielen verteilten Sensorknoten
- Oft ad-hoc vernetzt
- Energieversorgung meist über Batterie

Die ISM Bänder

- 6,765 MHz
- 13,553 MHz
- 26,957 MHz
- 40,66 MHz
- 433 MHz
- 902 MHz
- 2,4 GHz
- 5,7 GHz
- 24 GHz
- 61 GHz
- 122 GHz
- 244 GHz

- In den meisten Ländern für jeden frei verwendbare Frequenzbänder
- Alle kabellosen Consumerprodukte verwenden eines der ISM-Bänder
- Verwendung anderer Frequenzen benötigt spezielle Lizenzen

Eigenschaften verschiedener Frequenzbänder

Grundsätzlich: Je höher die Frequenz, desto höher die Datenübertragungsraten. Aber desto schlechter auch Reichweite ein Eindringtiefe.

900 MHz

- ca. 2,6 fache Reichweite wie 2,4GHz
- Bandbreite: 26 MHz (1/3 wie im 2,4GHz Band)
- Nur in Region 2 (Hauptsächlich Amerika. **nicht** Europa)

2.4 GHz Band

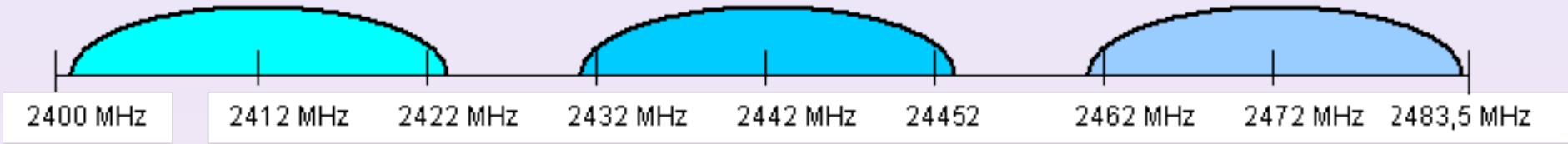
- Reichweite ungerichtet bis ca. 100m
- Maximal zulässige Sendeleistung: 100mW
- Weltweit zulässig
- Bandbreite: 100MHz

5 GHz

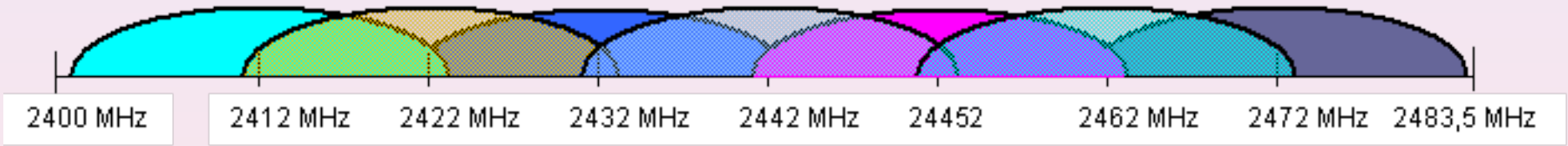
- Maximal zulässige Sendeleistung: 1W, daher theoretisch höhere Reichweite als 2,4GHz
- Weltweit zulässig (Ausgenommen bestimmte Kanäle, z.B. in Japan)
- DFS und TPC zwingend vogeschrieben, um militärische Anwendungen nicht zu stören
- Bandbreite: 150MHz
- Weniger ”Betrieb” als im 2,4GHz Band

Frequenzspreizung: Motivation

IEEE 802.11b-European Regulations - 3 non -overlapping channels possible

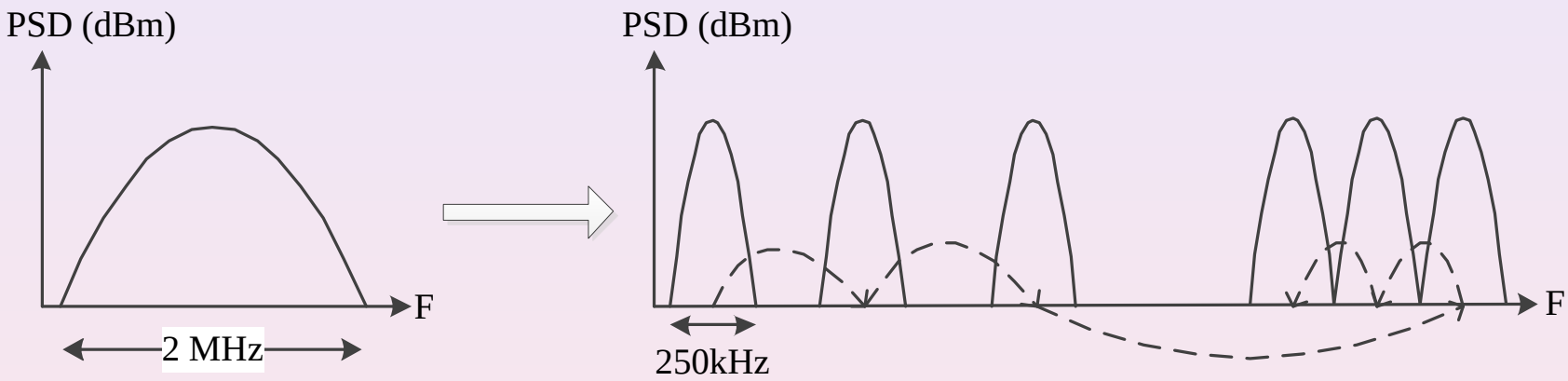


IEEE 802.11b European Regulations – 7 overlapping channels out of 13 shown,
not shown are the Channels with the center frequencies: 2417, 2427, 2437, 2447, 2457 and 2467

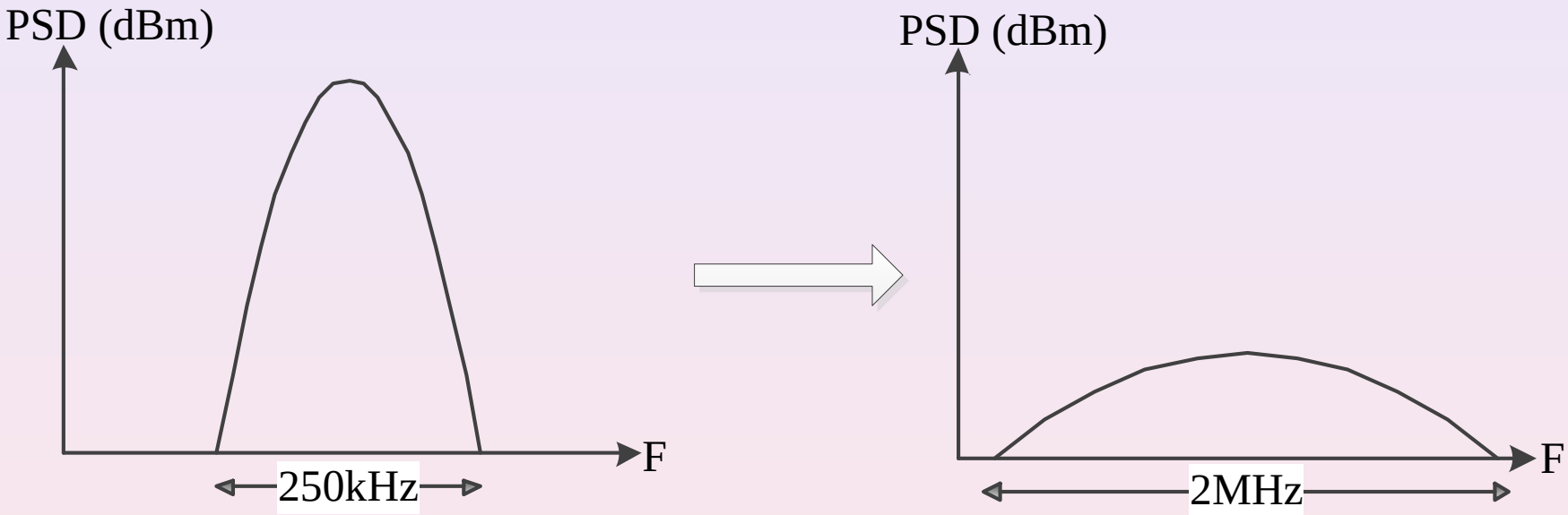


Bluetooth: 79 channels for frequency hopping

FHSS: Frequency Hopping Spread Spectrum



DSSS: Direct Sequence Spread Spectrum



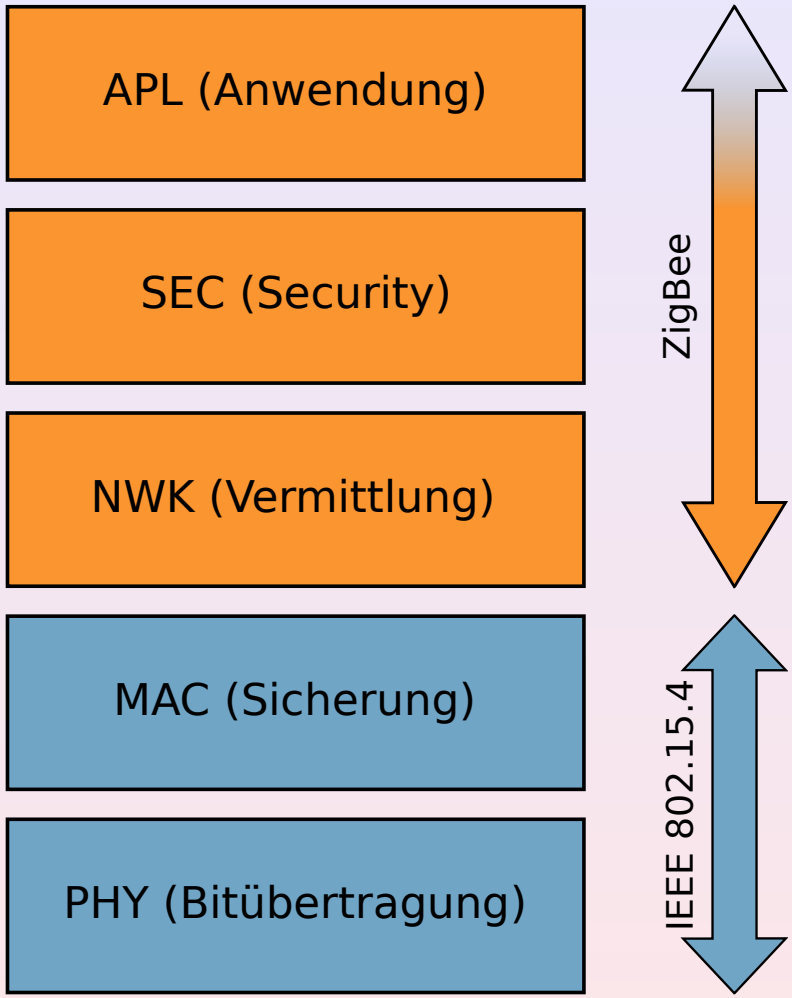
IEEE 802.11: WLAN

- 2,4GHz und 5GHz
- Übertragungsraten bis 150Mbit/sec
- Reichweiten ungerichtet bis ca. 100m, bei Sichtverbindung mit externer Antenne sogar bis 300m
- Richtfunk bis ca. 40km
- Je nach Standard: Verwendung von DSSS, FHSS und OFDM
- Relativ hoher Leistungsbedarf: 100mA zum Empfangen, 190mA zum Senden
- Ad-Hoc Modus möglich

Bluetooth

- 2,4GHz
- Übertragungsraten bis 2,1MBit/sec
- Reichweite bis 10m (Class 3), 50m (Class 2), 100m (Class 3)
- FHSS
- Leistungsbedarf ca. 56,7mW (16,6mA) für ein Class 2 Slave
- Maximal 255 Teilnehmer
- Jedoch nur 7 gleichzeitig aktive Slaves
- 1 Master
- Teilnehmer müssen gepaired werden

ZigBee



- Protokollstack auf Basis von IEEE 802.15.4
- 868MHz (nur Europa), 900MHz (nur Amerika) und 2,4GHz (weltweit)
- 1mW Sendeleistung
- Reichweite bis ca. 100 Meter
- DSSS
- Übertragungsrate: 20kbit/sec (868MHz), 40kbit/sec (900MHz), 250kbit/sec (2,4GHz)
- 19mA im Betrieb, 6μA im Sleep-Modus (Nur auf RFDs)
- FFDs (Full Functional Devices) und RFDs (Reduced Functional Devices)

NI wireless sensor networks

- Programmierbare Ethernet und Wlan Gateways verfügbar
- Knoten mit 4 digitalen und 4 analogen Eingängen
- Anbindung an LabVIEW
- Proprietäres Protokoll auf Basis von IEEE 802.15.4
- Relativ teuer: ca. 500 Euro pro Sensorknoten

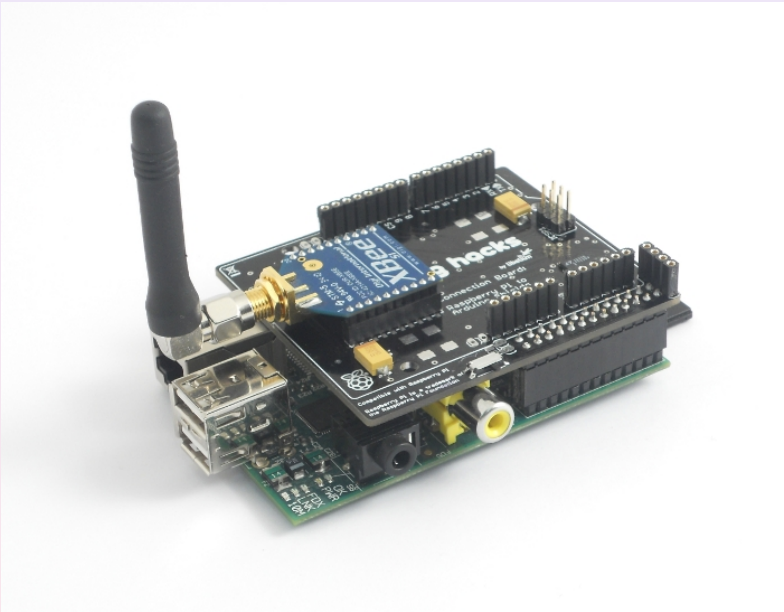
Libelium

- Sensornetzprodukte auf ZigBee Basis
- Sowohl als kostengünstige Entwicklerboards als auch als fertige Komplettlösung verfügbar
- Unabhängige Energieversorgung über Solarzellen
- Multiprotokoll-Gateways mit ZigBee, Wlan und Bluetooth
- Opensource Software
- Lösungen für Smartcities
- Reichweite nach Herstellerangabe zwischen 7 und 14km

Arduino

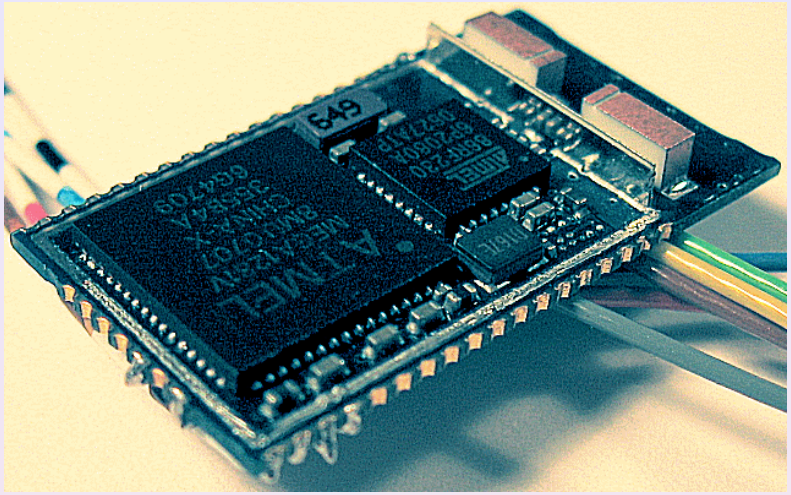
- ZigBee Schild für Arduino
- Sockel für ein Digi International XBee Pro
- Preis für Modul und Schild zusammen unter 40 Euro
- XBee Module sind in verschiedenen Ausführungen erhältlich, die teilweise Pin-kompatibel sind
- Hergestellt von Libelium, Grundlage für die kommerziellen Waspmotes

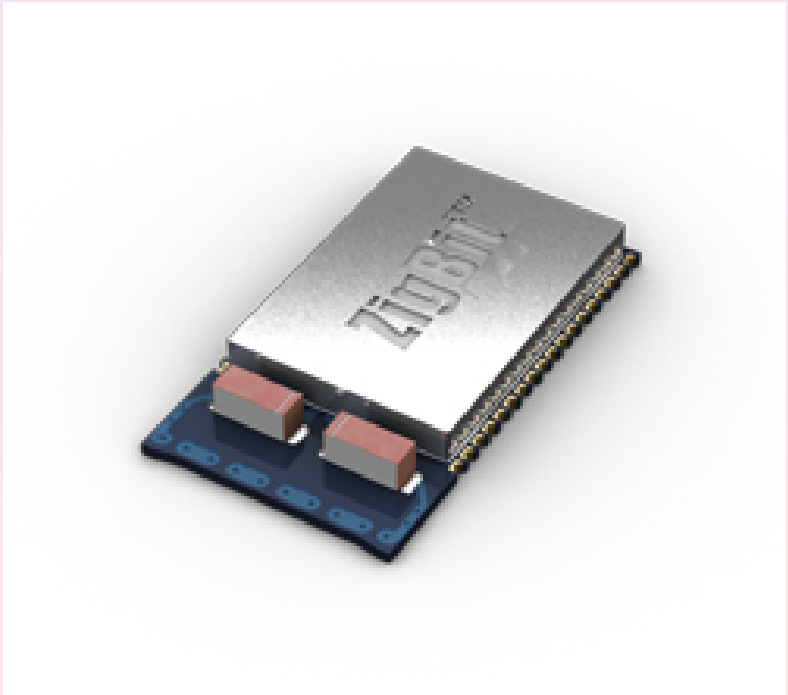
Raspberry Pi



- Verwendung des Arduino ZigBee Schild mit Hilfe der Raspberry Pi to Arduino Shield.
- Preis für den Adapter: 40 Euro

ZigBit



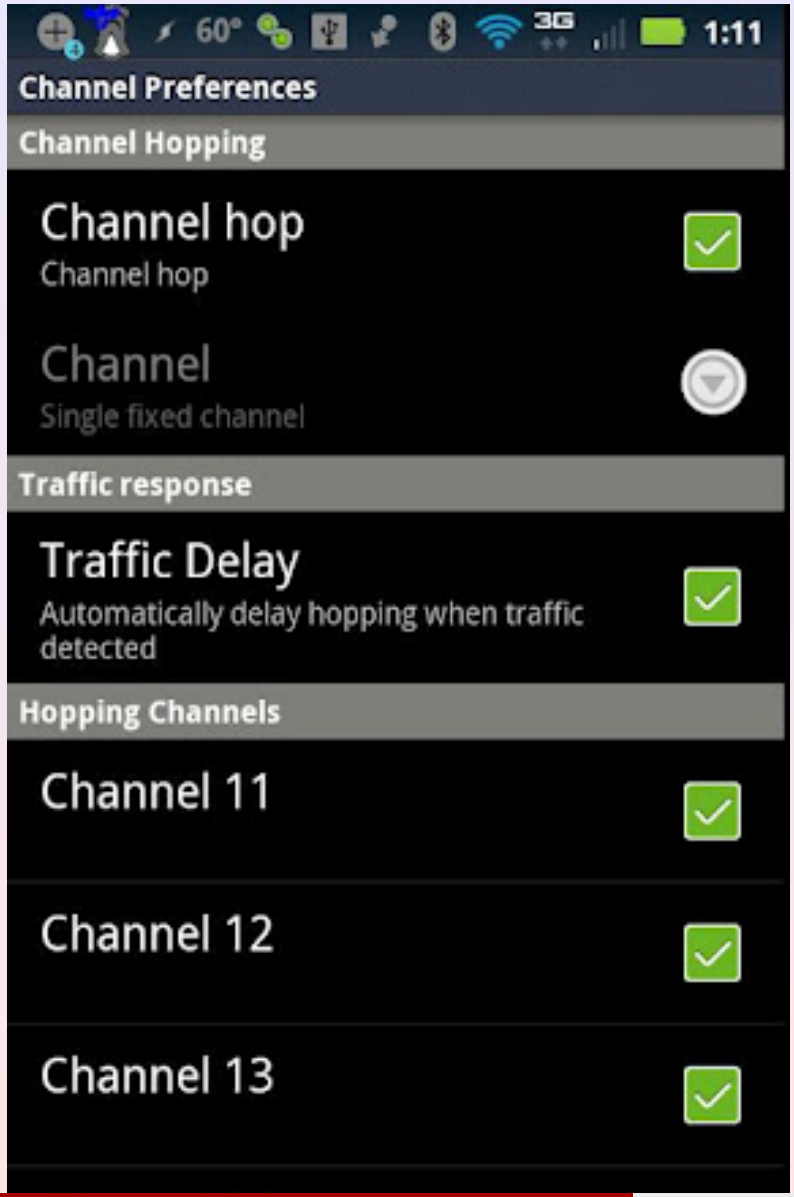


- Kombination aus IEEE.802.15.4 Radios mit einem ATmega1281V Mikrocontroller
- 30 GPIO Leitungen
- UART, USART, I2C, SPI, 1-Wire, 4 ADCs, JTAG
- Stückpreis um die 14 Euro
- Mit etwas Geschick im Löten praktisch schon ein komplettes Starterkit.

ZigBee: WEP Reloaded

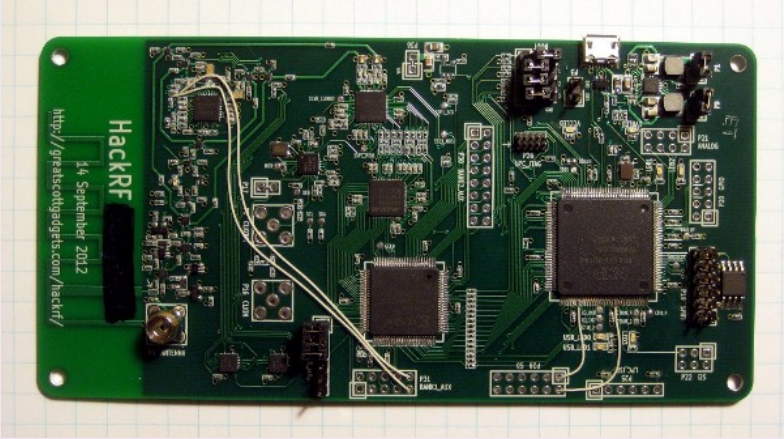
- Theoretisch 128-Bit-AES Verschlüsselung
- Aber oft managelhaftes Key-Management:
- Jedes Device in einem Netzwerk hat den selben PSK
- Keys können mittels JTAG extrahiert werden
- Oft schlecht gewählte Keys
- Kein Schutz gegen Replay Attacken
- Known-Plaintext Attacken möglich
- Besser: Security auf Application Layer. Aber: Auf einem 8-Bit Mikrocontroller...

Kisbee



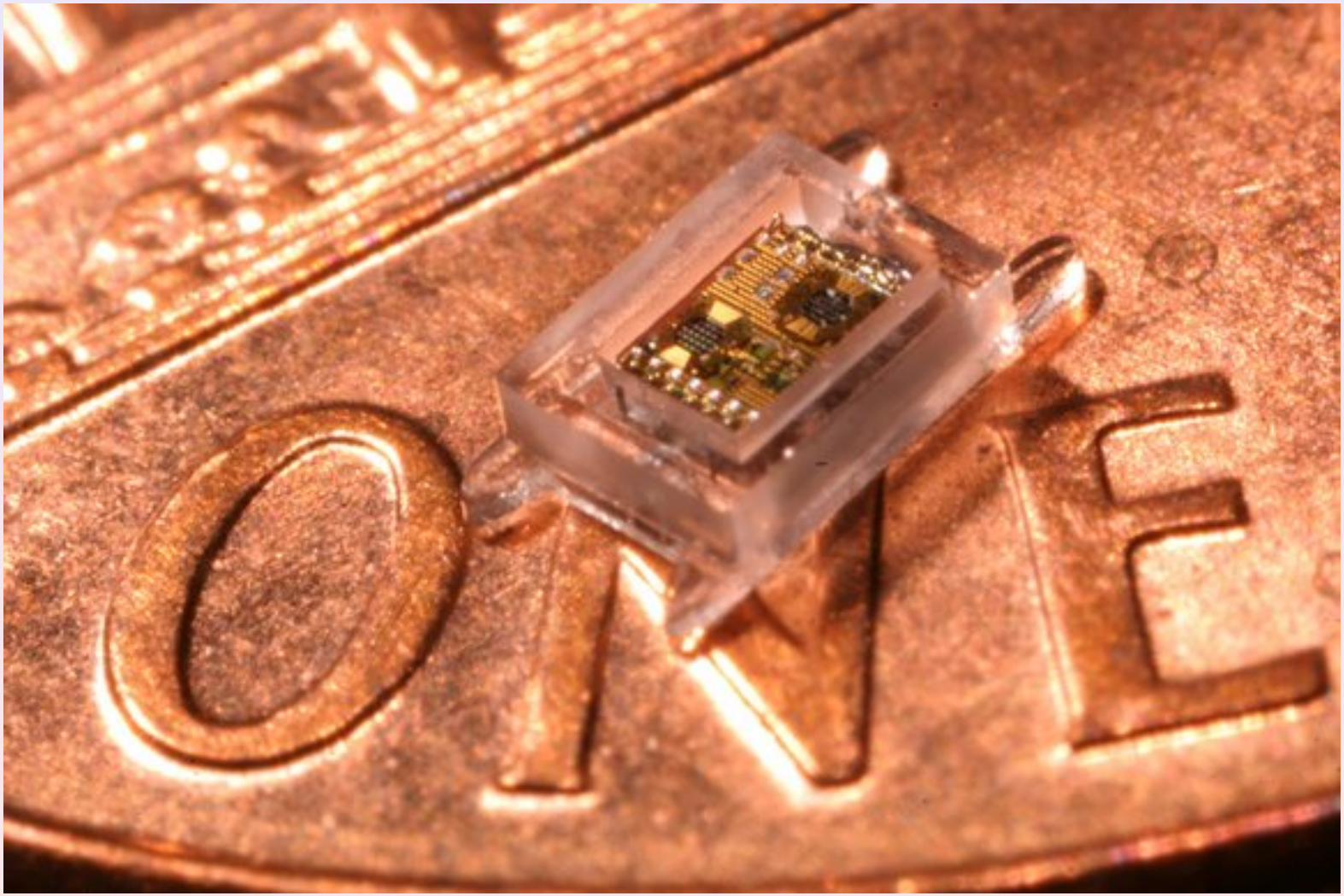
- Projekt von den Kismet Autoren zum Angriff auf ZigBee Netze
- Läuft auf Android
- ZigBee Device kann per Bluetooth oder USB angebunden werden

HackRF



- Idee: Low cost devices, das in der Lage ist, auf praktisch allen verwendeten Frequenzen zu Senden und zu Empfangen
- Damit werden auch Attacken auf Protokolle ausserhalb des ISM-Bandes möglich (z.B. GSM)
- Oder auf NFC, RFID...
- Integration in GNURadio
- Alle Bauteile sind auf kompatibilität mit OpenSourceSoftware sowie Robustheit ausgelegt

Smart dust



Meine Kleidung funkt!

Tracking


Smartphones Detection
Bluetooth
Wifi
SHOP
DEPARTMENT STORE
WI FI

Further Reading

https://dev.noetech.net/svn/diplomarbeit/
User: anonymous
Passwort: anonymous