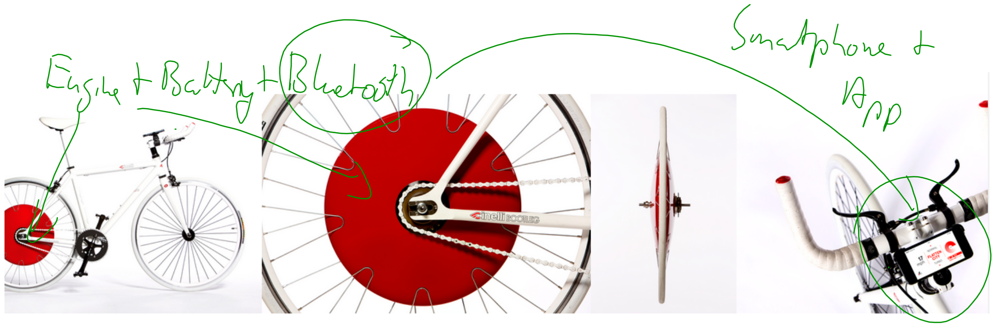
Short-range communication → Bluetooth, ANT+ Wireless HART, ...

Contactless communication → NFC, RFID

Security in NFC

Short range communication

- Bluetooth



Drivers for evolution

- Mobile communication from 2G → 3G

IS95 (CDMA) $\xrightarrow{\text{easy}}$ CDMA 2000

(no SIM)

GSM TDMA → UMTS WCDMA → 90% of market

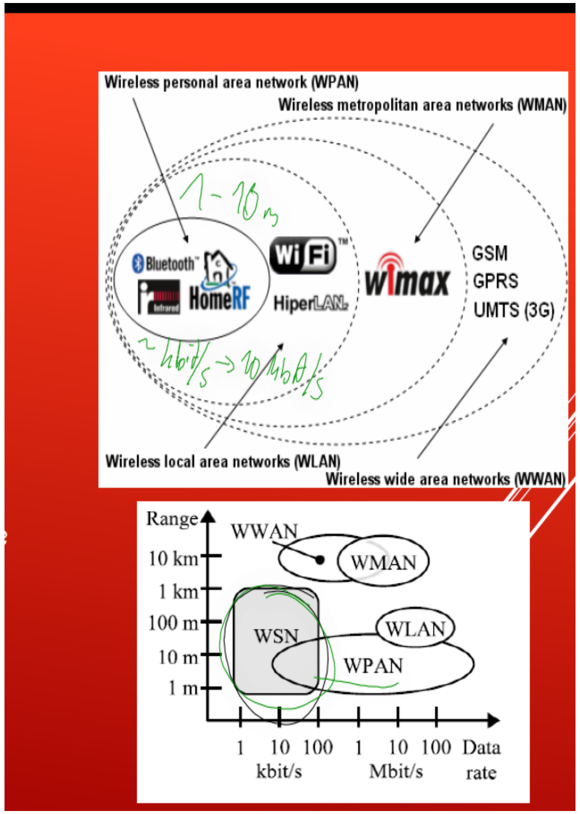
SIM →

ANT, ZigBee Sensor communication

Bluetooth LE (3-4 years late) in the mobile ← dominates

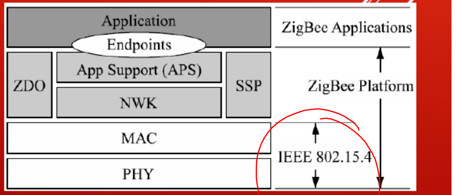
- medical
- assessoires

Bluetooth, ANT+ presentation by
Thomas Aasebø



ZIGBEE - INTRODUCTION

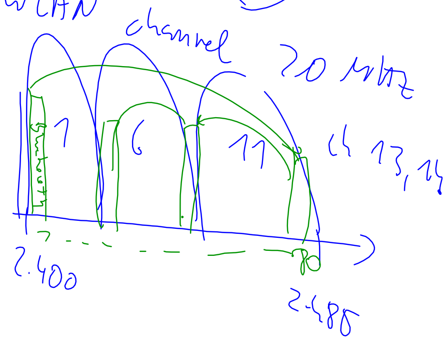
- What is **ZigBee**?
- Who **created** it? Who **owns** the technology?
- Why the strange **name**?
- What is it primarily **used** for?



2.4 GHz ISM

2.4 – 2.485 MHz

WLAN



Interference Bluetooth... WLAN

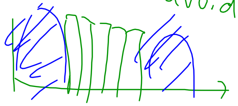
high datarate

Bluetooth

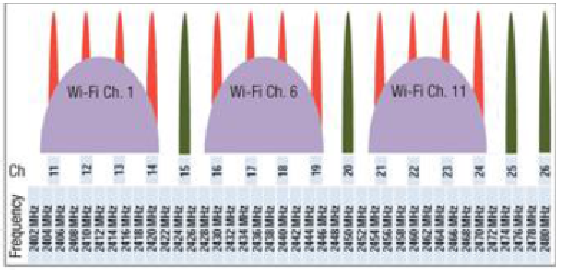
B = 1 MHz

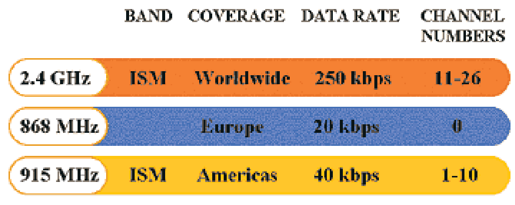
80 × 1 MHz

- Fast frequency hopping
- Bluetooth 3.0 WLAN avoidance



CHARACTERISTICS





	BAND	COVERAGE	DATA RATE	CHANNEL NUMBERS
2.4 GHz	ISM	Worldwide	250 kbps	11-26
868 MHz		Europe	20 kbps	0
915 MHz	ISM	Americas	40 kbps	1-10

- To provide flexibility, **three** unlicensed **bands** are used depending on location – 2.4 GHz, 915 MHz and 868 MHz.
- **Sixteen channels** are allocated in the 2.4 GHz band, each channel being **2 MHz wide** and requiring **5 MHz of spacing**.
- The 2.4 GHz band provides up to **250 kbit/s**, 915 MHz provides up to **40 kbit/s** and 868 MHz provides a data rate up to 20 **kbit/s**.
  - **Throughput** is expected to be around **10 to 115.2 kbit/s.**
- **Direct-sequence spread spectrum**(DSSS) **coding** is utilized.
  - In the 868 and 915 MHz bands, **binary phase-shift keying** (BPSK) is used.
  - **Offset quadrature phase-shift keying** (OQPSK) that transmits two bits per symbol is used in the 2.4 GHz band.

Communications

Antenna Gain
G_T, G_R

Transmit power
P_T

Path loss $\left(\frac{\lambda}{4\pi r}\right)^2$

interference

free space loss

$P_R >$
P Receiver Sensitivity

$SNR = f(\text{interference}, P_R / P_{\text{Sensitivity}})$

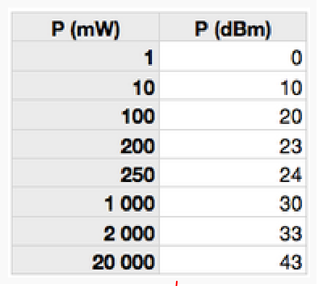
Signal to noise ratio

$P_{\text{Sensitivity}}$ = − 95 dBm (WLAN)
= − 85 dBm bad Bluetooth
= − 104 dB GSM

Capacity
/per channel

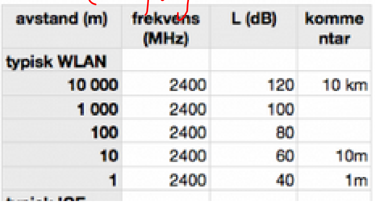
higher bitrate
- increase bandwidth
  bundle channels
- multiple radio channels
  MIMO

Bluetooth class	output power P_{out}
0 dBm	1 mW
4 dBm	
20 dBm	100 mW = WLAN



P (mW)	P (dBm)
1	0
10	10
100	20
200	23
250	24
1 000	30
2 000	33
20 000	43

distance freq L



avstand (m)	frekvens (MHz)	L (dB)	kommentar
typisk WLAN			
10 000	2400	120	10 km
1 000	2400	100	
100	2400	80	
10	2400	60	10m
1	2400	40	1m

$P_R = -40\ dBm$

$P_{sen} = -85\ dBm$

$SNR = 45\ dB$

- interference
- real path loss

Bluetooth

$P_{sens} = -85\ dBm$

$L = 40\ dB\ (1m\ 2.4\ GHz)$

$P_T = 0\ dBm$

$P_R = P_T + G_T + G_R - L$

$\quad\ \ 0 \quad 0 \quad 0 \quad -40$

$P_R = -40\ dBm$

Standby power 2 μW

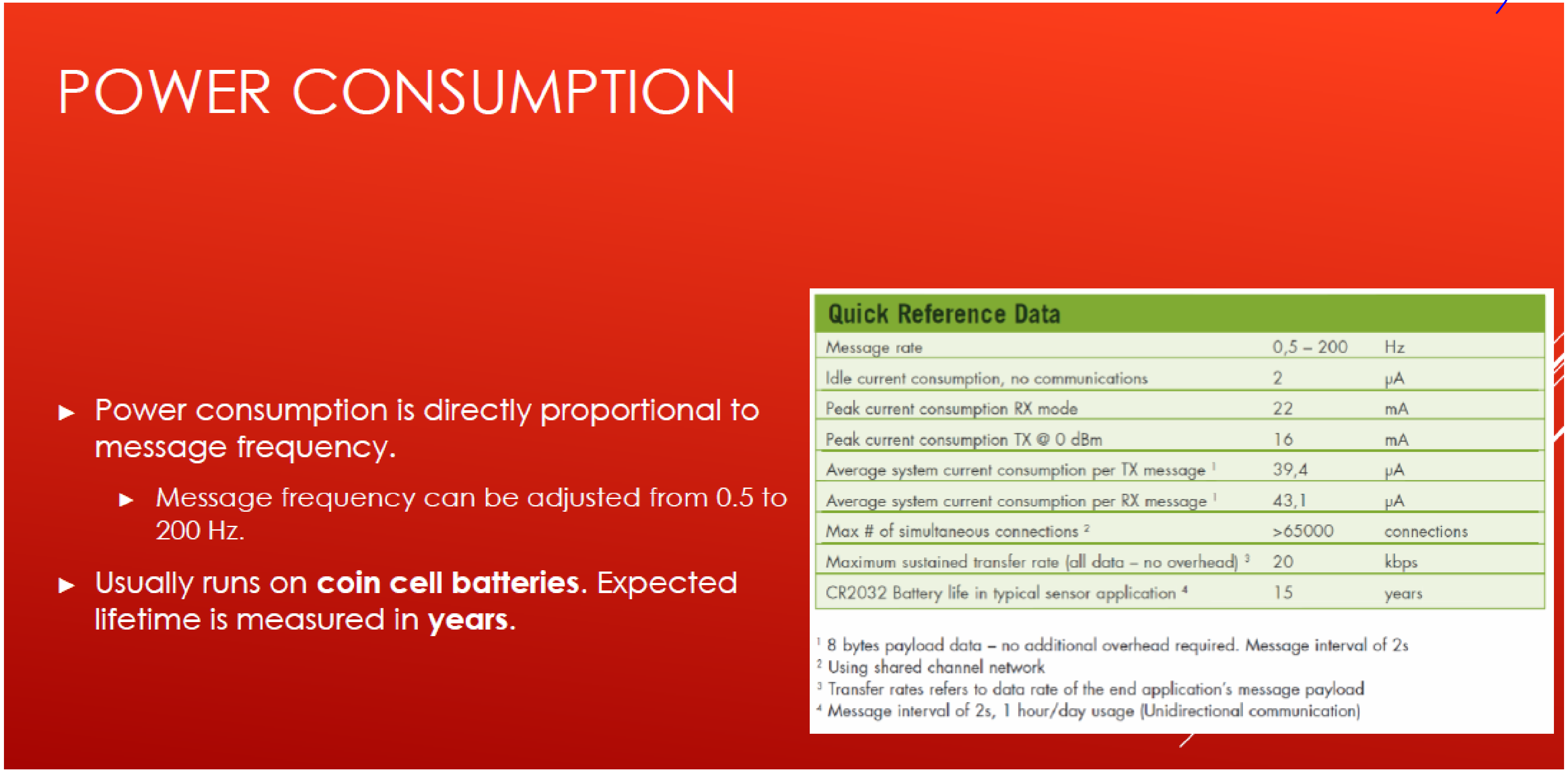
Receive operation 22 mW

Communication 10.000 increase in power

Transmit operation 18 mW (0 dBm) – 150 mW (20 dBm)

1 mW

100 mW



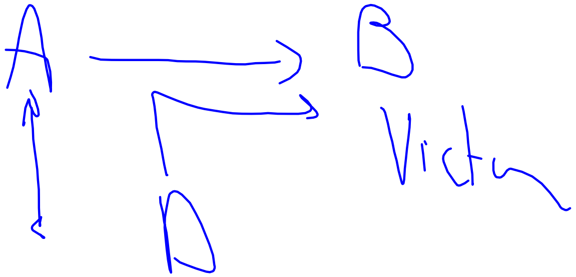
POWER CONSUMPTION

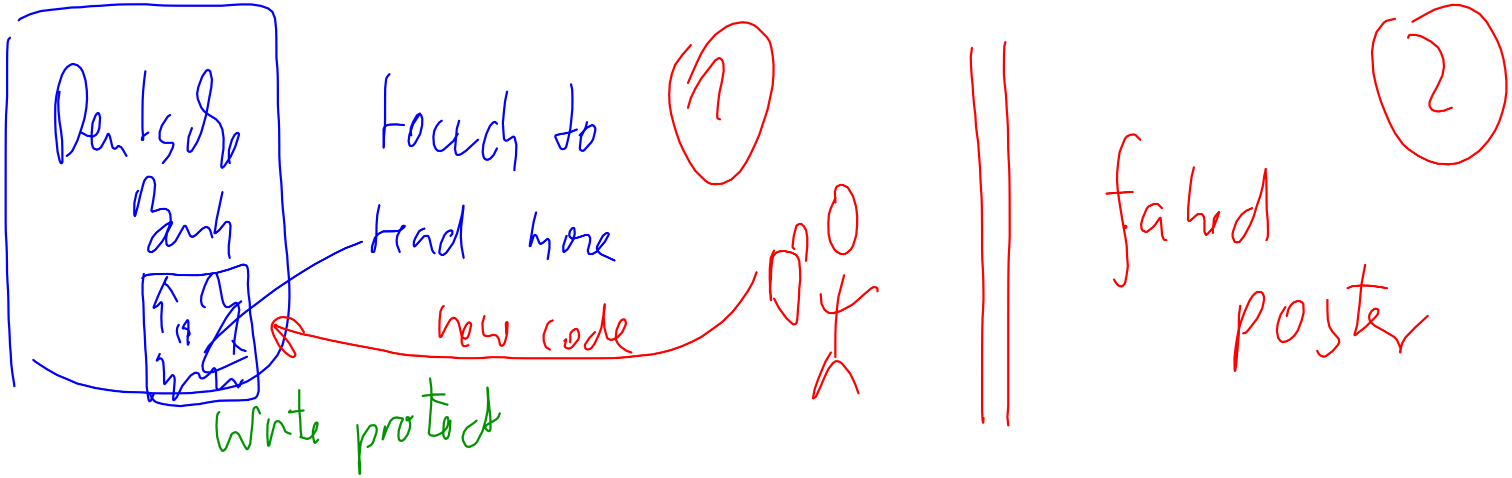
- Power consumption is directly proportional to message frequency.
  - Message frequency can be adjusted from 0.5 to 200 Hz.
- Usually runs on **coin cell batteries**. Expected lifetime is measured in **years**.

Quick Reference Data		
Message rate	0,5 – 200	Hz
Idle current consumption, no communications	2	μA
Peak current consumption RX mode	22	mA
Peak current consumption TX @ 0 dBm	16	mA
Average system current consumption per TX message [1]	39,4	μA
Average system current consumption per RX message [1]	43,1	μA
Max # of simultaneous connections [2]	>65000	connections
Maximum sustained transfer rate (all data – no overhead) [3]	20	kbps
CR2032 Battery life in typical sensor application [4]	15	years

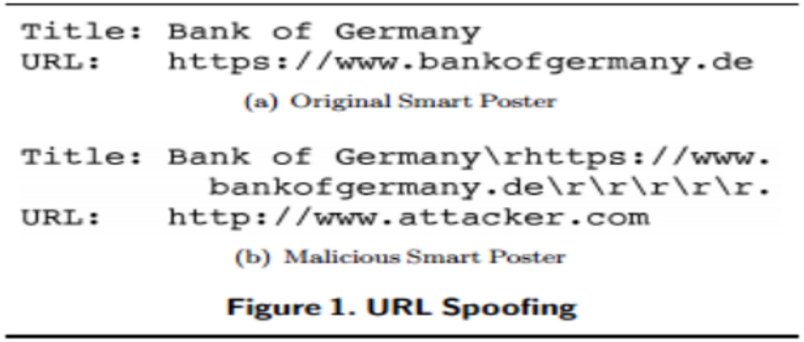
[1] 8 bytes payload data – no additional overhead required. Message interval of 2s
[2] Using shared channel network
[3] Transfer rates refers to data rate of the end application's message payload
[4] Message interval of 2s, 1 hour/day usage (Unidirectional communication)

- In data corruption transmit valid frequency of data spectrum at correct time.
- corruption power is bigger than sender power => detectable.
- In data insertion: only, inserted data transmitted before the original device starts with the answer
- data streams overlap => data corruption





Smart poster URL spoofing



```
Title: Bank of Germany
URL:   https://www.bankofgermany.de
```

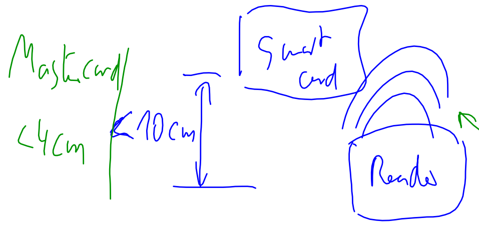
(a) Original Smart Poster

```
Title: Bank of Germany\rhttps://www.
         bankofgermany.de\r\r\r\r\r.
URL:   http://www.attacker.com
```

(b) Malicious Smart Poster

Figure 1. URL Spoofing

- Possible countermeasure: mark the URL in special way



1.) handshake mode of communication
card mode / p2p /

static field sends out $\frac{1}{r^4}$

RF signal eavesdropping

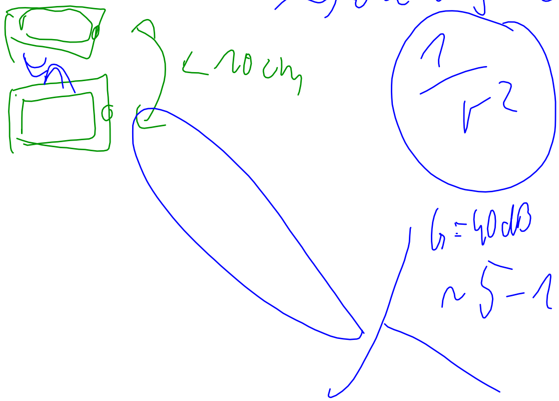
special tools

- RF Signal eavesdropping:
- How close an attacker need to be, based on many things: RF characteristics of sender device, attacker antenna, attack receiver, attacker signal RF decoder, power send by NFC device, attacker location.
- In general, sending device in active mode => 10m, when it in passive mode => 1 m.
- Possible countermeasure: establish a secure channel.

?

bullshit

Active mode



~) electromagnetic field

$\frac{1}{r^2}$

$G = 40\,\mathrm{dB}$ $P_{sens} \approx -120\,\mathrm{dBm}$

~5-10m

What is NFC

a ↔ p

- NFC operational mode :
  - ➢ Read/write mode: active device links up with another device to read information (smart mobile - NFC tag)
  - ➢ Peer-to-peer mode: both devices switch between active (sending data), and passive (receiving data).
  - ➢ Card emulation: using NFC device as credit card.

NFC mode

a/p ↔ a/p

⇒ ISO .....

> Card emulation: access card mode

↳ ISO.....

duplication of cards

Philips Mifare ~~light~~

↳ Tram/busses in NL

Countermeas.

Difference between

$$\text{Gain} = \overset{\overset{=}{\frown}}{\text{dB} , \text{dBi}}$$

reference value

isotropic antenna