Theoritical Limits of ISO/IEC 14443 type A Eavesdropping Attacks

Florian Pfeiffer (perisens)
Klaus Finkenzeller (Giesecke & Devrient)
Erwin Biebl (Fachgebiet Höchstfrequenztechnik – TUM)
12.06.2012

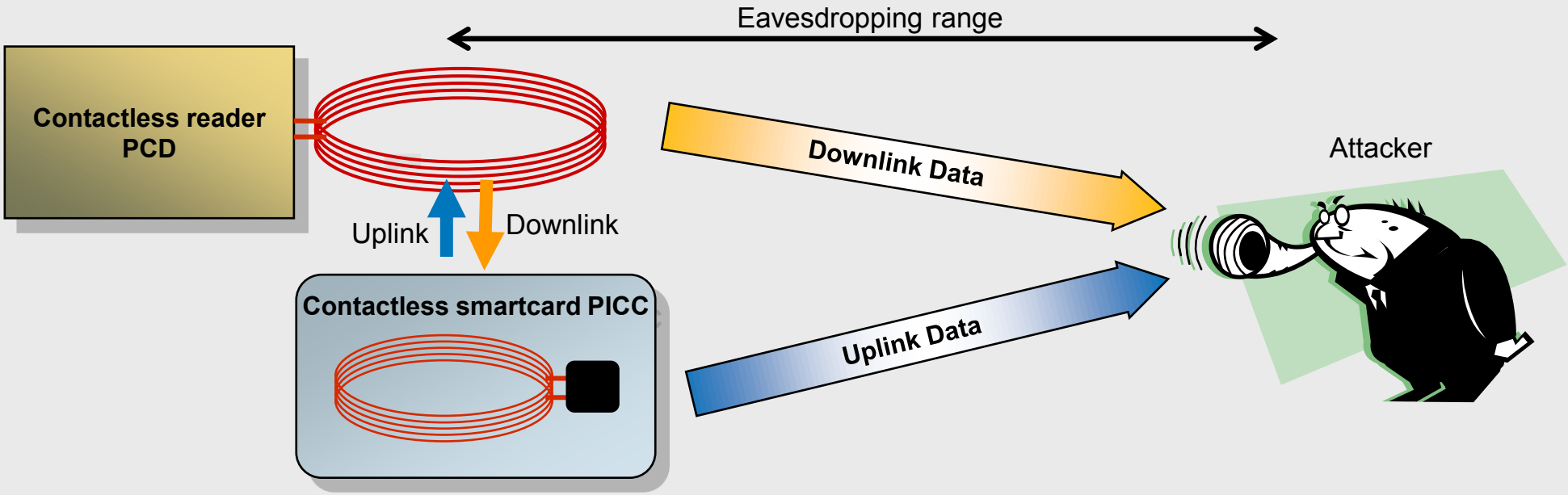
Technische Universität München
perisens GmbH
Giesecke & Devrient
Creating Confidence.

Outline

- Motivation
- Theoretical approach
- Characterization of an exemplary transponder
- Uplink & Downlink results
- Conclusion

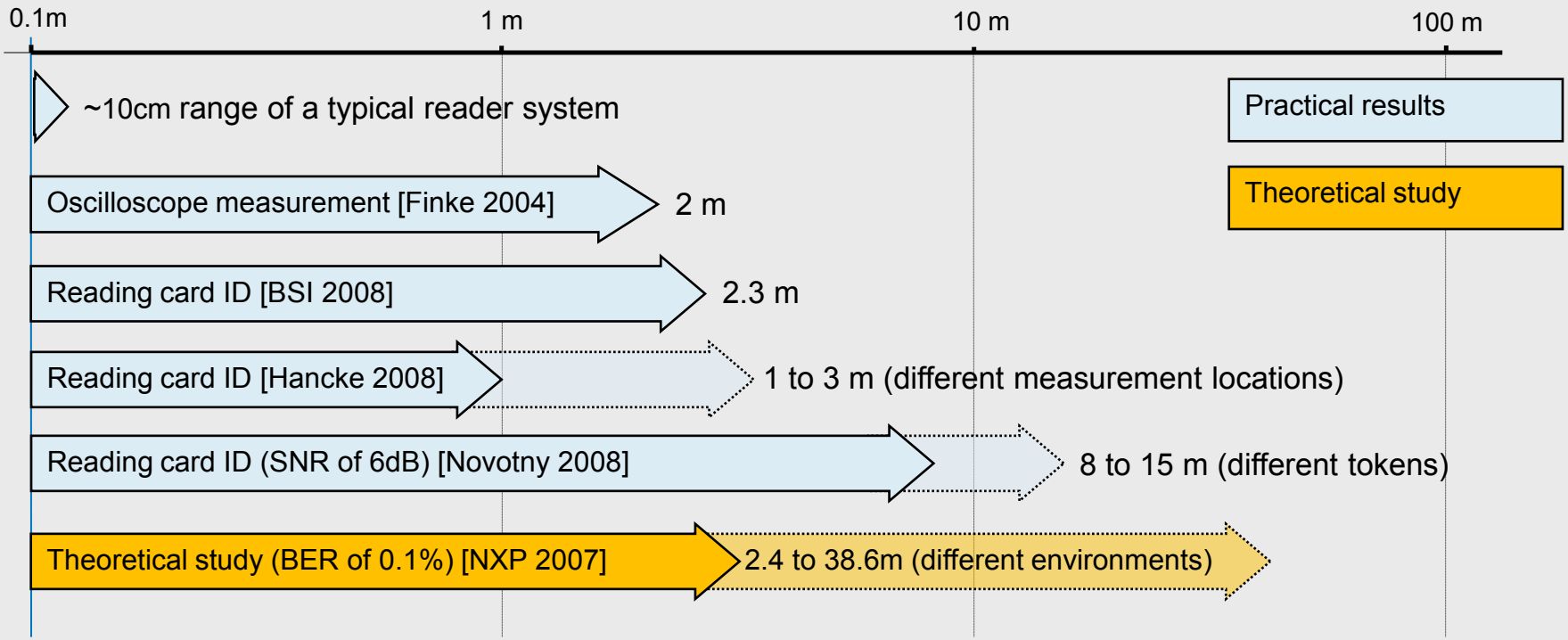
Principle of Eavesdropping I

Eavesdropping is an unauthorized detection of the bidirectional data communication between reader and tag



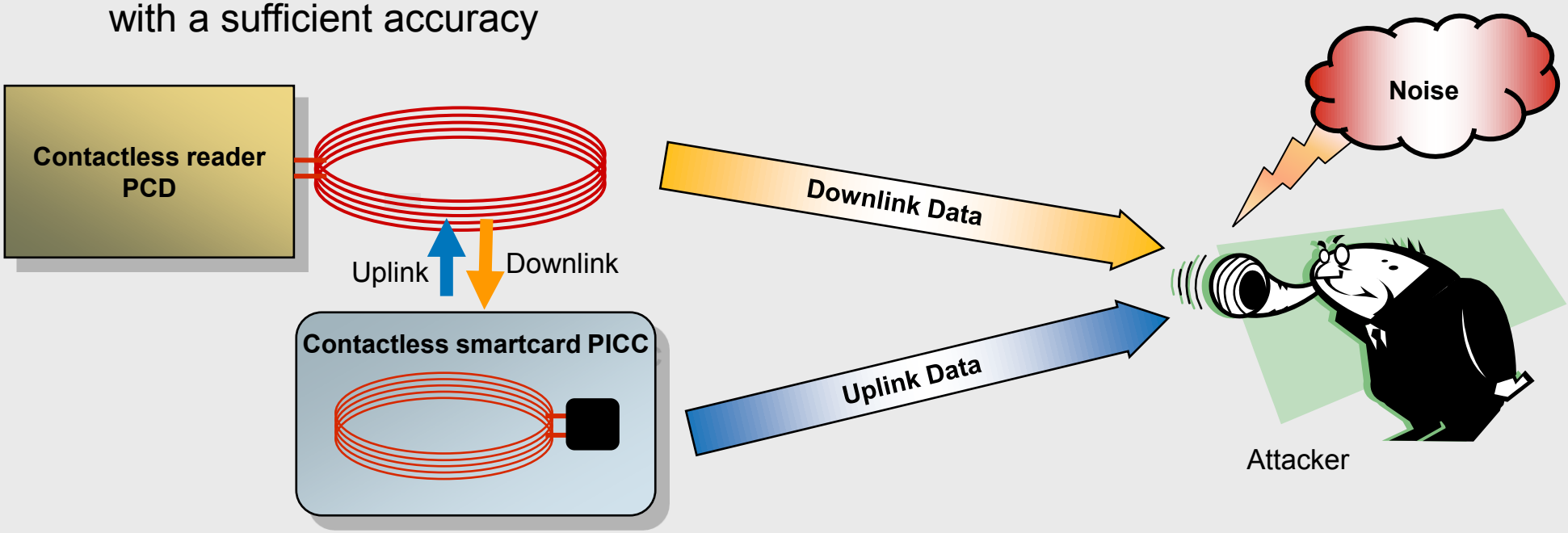
Motivation

Published practical and theoretical results show considerable differences in the eavesdropping range (ISO/IEC 14443 A)



Principle of Eavesdropping II

A successful attack requires that the attacker is able to detect the bidirectional data with a sufficient accuracy



In a real environment, noise degrades the signal detection and causes bit errors with a certain probability. To ensure a reliable detection the **bit error rate (BER)** has to be low enough.

Required Bit Error Rate

Typical frame length in ISO/IEC 14443 systems require a Bit Error Rate of 0.01% for reliable detection

Probability that a frame with N-bits arrives without any bit error = $(1-BER)^N$

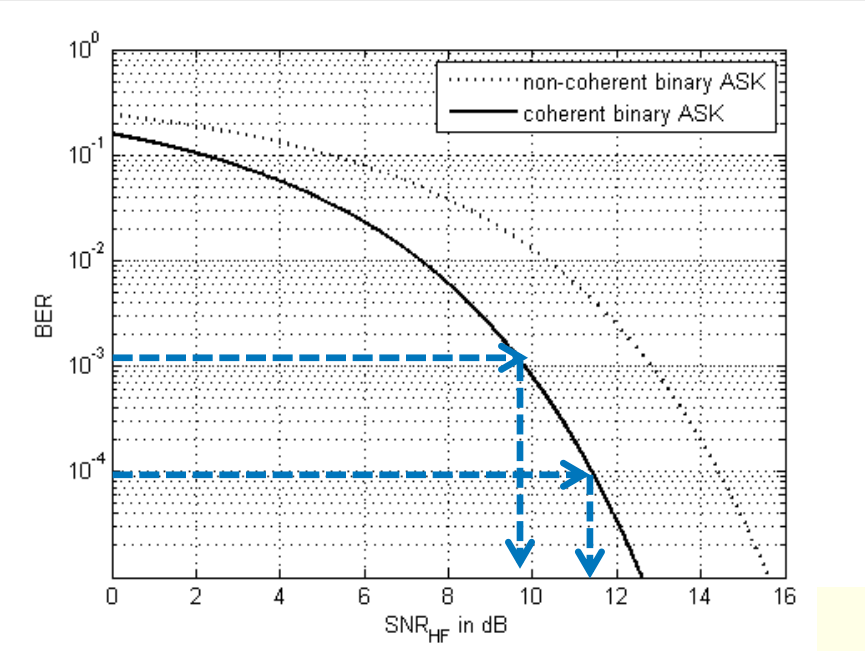
Data length	BER			
	1 %	0.1 %	0.01 %	
2 Bytes	85.1 %	98.4 %	99.8 %	e.g. 16bit CRC
4 Bytes	72.5 %	96.6 %	99.7 %	e.g. Transponder -ID
256 Bytes	0 %	12.9 %	81.5 %	e.g. Full data frame

No error correction considered here (according to ISO/IEC 14443), but...

- ➔ error detection (CRC, parity) could be used for error correction
- ➔ by forcing a frame retransmission (e.g. by interfering single bits) interleaving could be used to improve detection

Bit Error Rate as Function of the SNR

A reliable eavesdropping with a defined bit error rate (BER) requires a certain signal-to-noise ratio (SNR)



ISO/IEC 14443 A

- Amplitude Shift Keying (ASK)
- Additive white Gaussian noise
- Coherent demodulation
- Matched filter
- optimum threshold detector

$$BER = \frac{1}{2}\,\mathrm{erf}\left(\frac{1}{2}\sqrt{SNR_{HF}}\right)$$

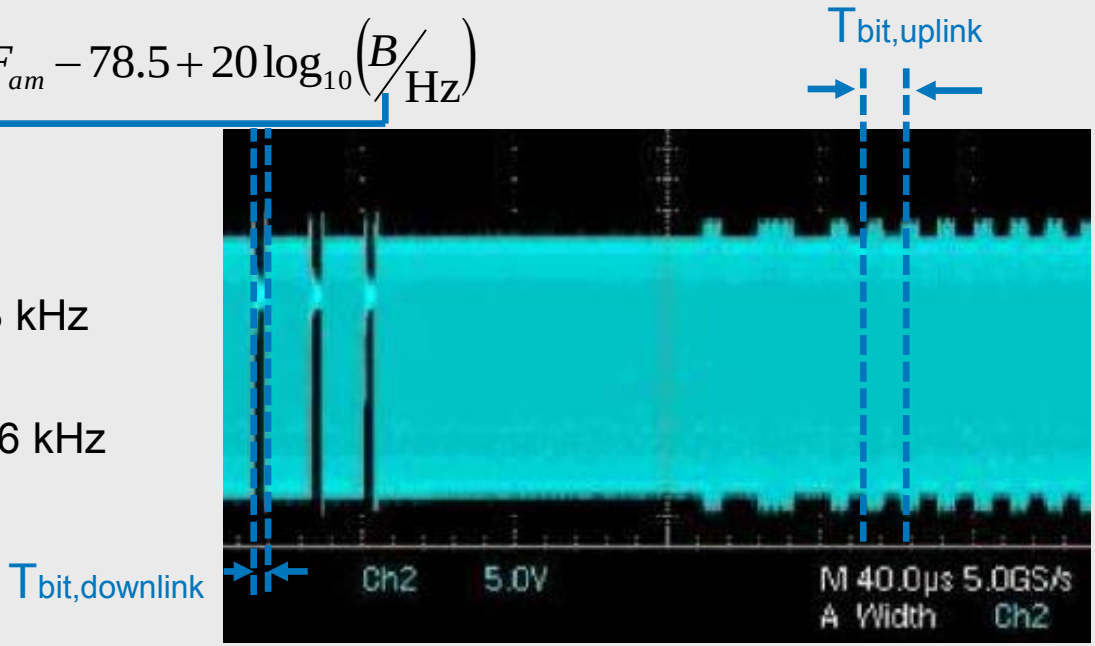
BER = 0.01%	→	SNR = 11.4dB
BER = 0.1%	→	SNR = 9.8dB
(BER = 2 %	→	SNR = 6dB)

Minimum Signal Field Strength H_{min}

The minimum magnetic field strength Hmin of the desired signal (at the location of the attacker) can be derived from noise level and required SNR

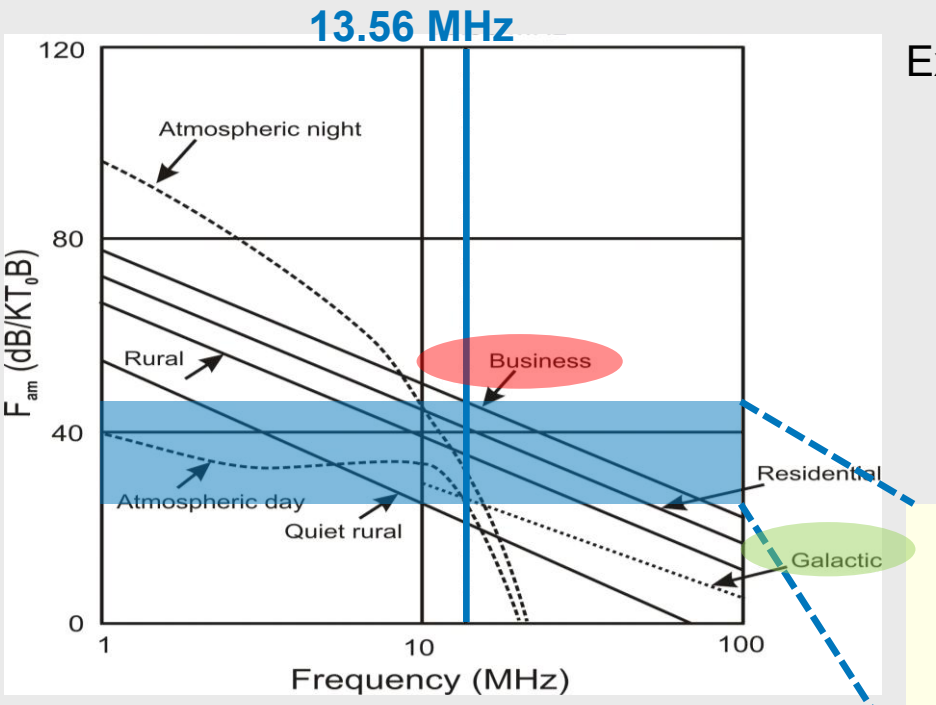
- Signal: $H_{\text{Signal,min}}\,[\text{dBuA/m}] = H_{\text{Noise}}\,[\text{dBuA/m}] + SNR$
- Noise: $H_{\text{Noise}}\,[\text{dBuA/m(rms)}] = F_{am} - 78.5 + 20\log_{10}\left(B/\text{Hz}\right)$
- With matched filter: $B = 1/T_{\text{Bit}}$
  - Downlink T = 3us / B = 333 kHz
  - Uplink T=9.4us / B = 106 kHz

Legend:
Fam… Noise figure,
B… Bandwidth, T… Bit duration



Noise Level in the HF-Band

In the HF-band the external noise normally exceeds the internal receiver noise



External noise sources:

- Man Made Noise (MMN) for
  - Business,
  - Residential,
  - Rural and quite rural environment
- Atmospheric noise
- Galactic noise

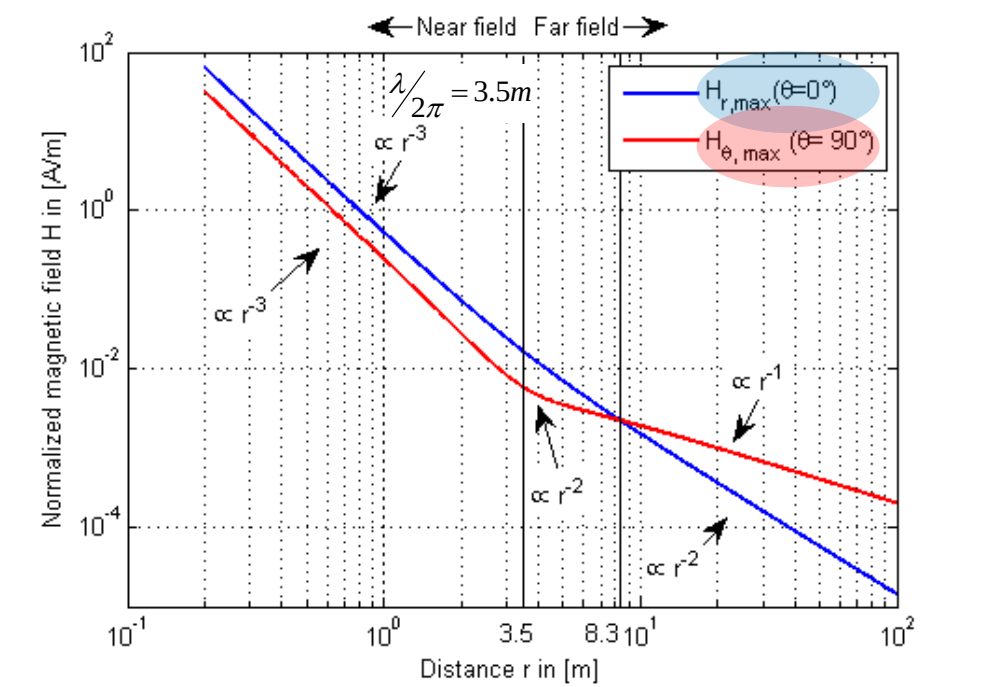
Assuming a non-directional antenna the noise figure lies between:

- 26 dB for galactic noise and
- 45.4 dB for MMN in a business environment

[erc99]: European Radiocommunications Committee (ERC): Propagation Model and Interference Range Calculation for Inductive Systems 10 kHz – 30 MHz. ERC report 69, 1999.

Small Circular Loop Antenna

Magnetic field of a small loop antenna in dependence of the distance depends on the antenna orientation



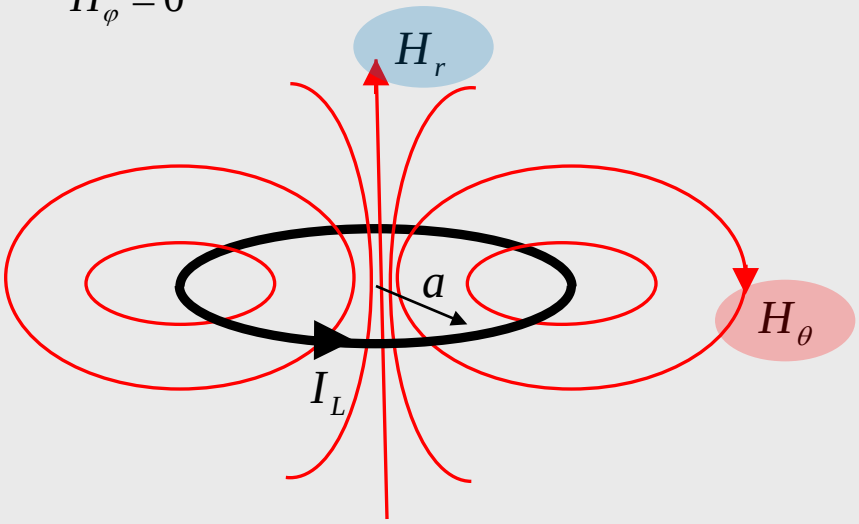
Legend:
a… loop radius, I_L … loop current,
k… wavenumber $k = 2\pi/\lambda$, r… distance

Magnetic fields:

$$H_r = j\frac{ka^2 I_L \cos\theta}{2r^2}\left(1+\frac{1}{jkr}\right)e^{-jkr}$$

$$H_\theta = j\frac{(ka)^2 I_L \sin\theta}{4r}\left(1+\frac{1}{jkr}-\frac{1}{(kr)^2}\right)e^{-jkr}$$

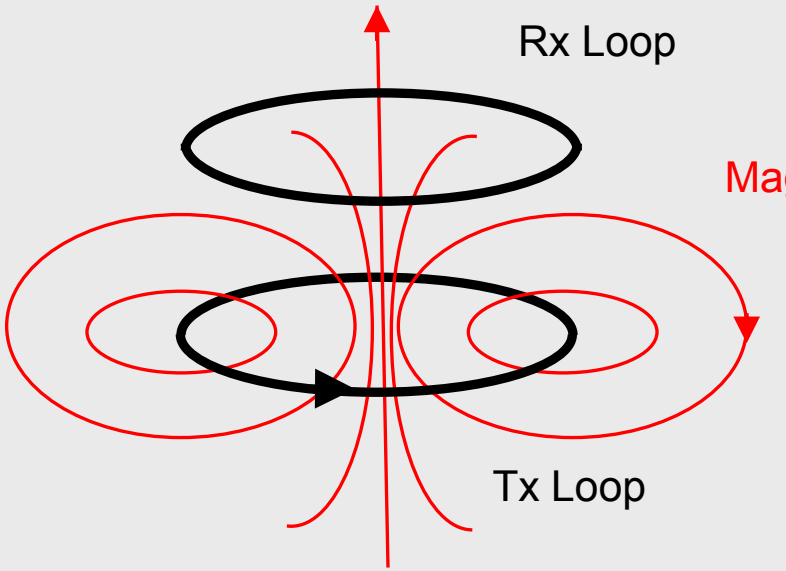
$$H_\varphi = 0$$



Optimum Loop Placement

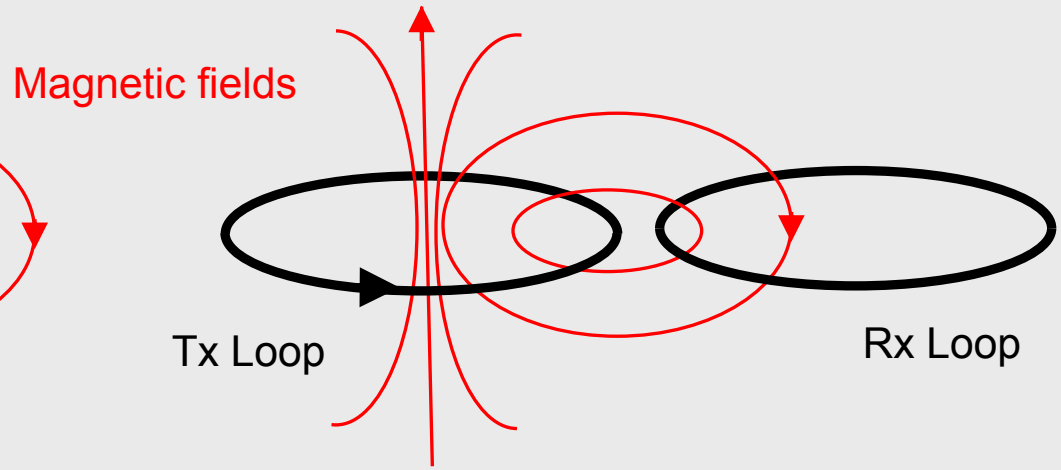
The optimum antenna placement depends on the distance between the two loops in relation to the wavelength

distance < 8.3m



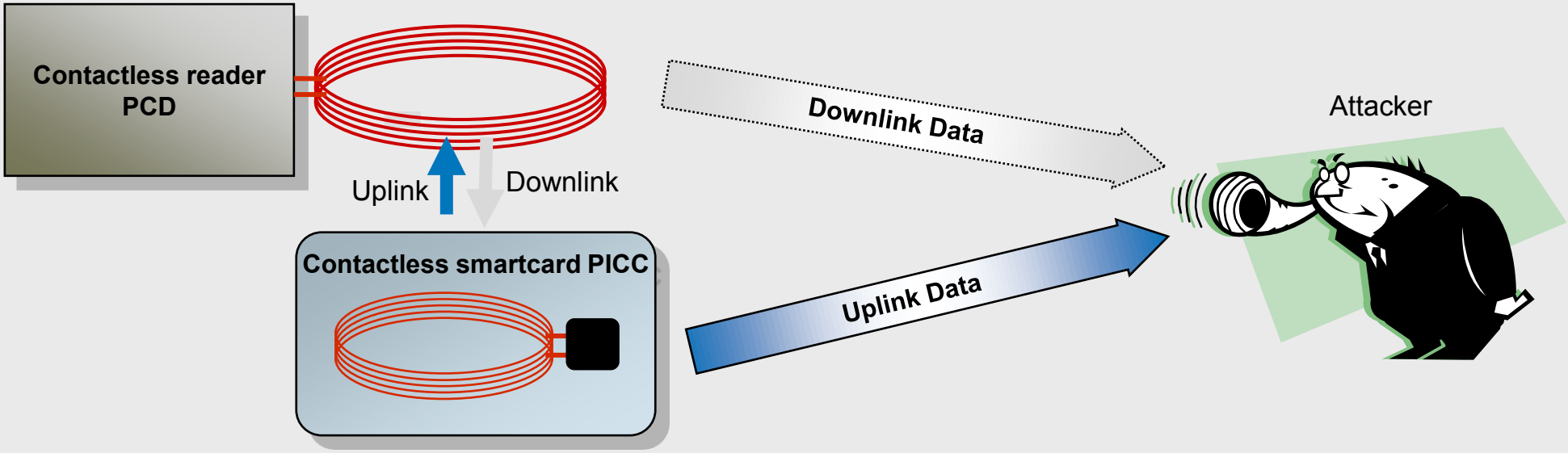
Coaxial orientation

distance > 8.3m



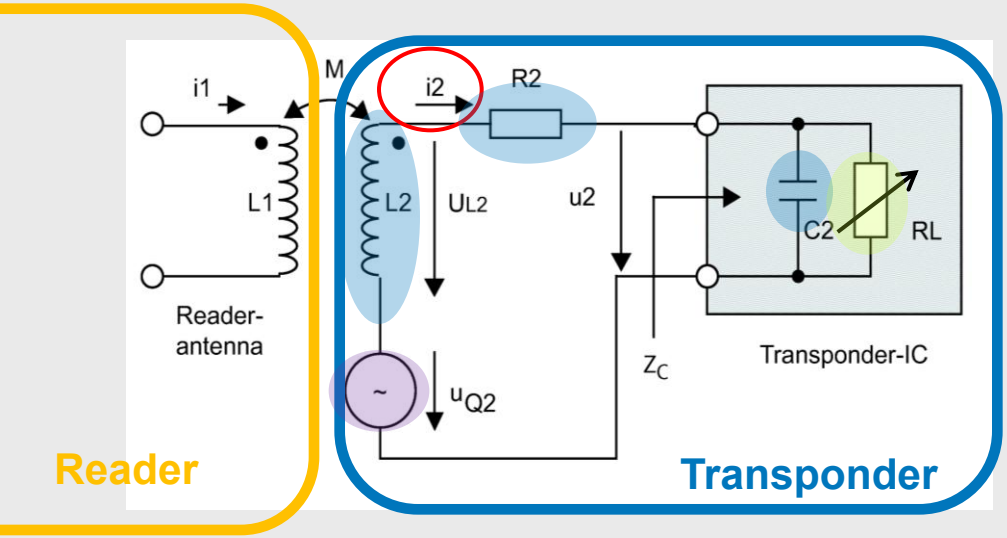
Coplanar orientation

Uplink Eavesdropping



Uplink: Reader / Transponder Model

Characteristic parameters of an exemplary tag (Mifare)



- L2, R2, C2 was measured using an impedance analyzer
- RL depends on the incident magnetic field and is calculated from the IC-voltage
- UQ2 depends on the incident magnetic field

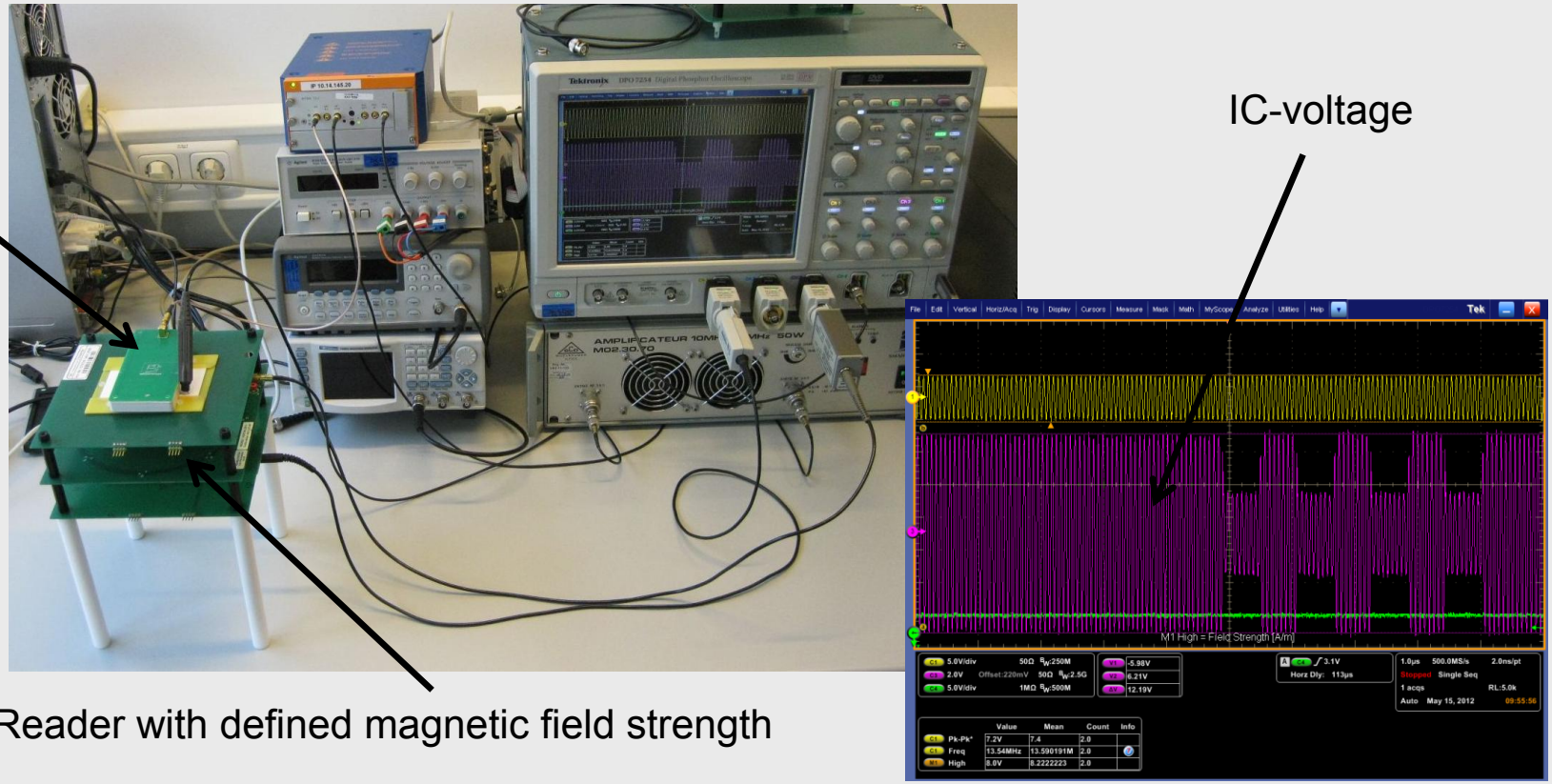
	L2 [uH]	Coil area [mm²]	Windings	R2 [Ohm]	C2 [pF]	f_res [MHz]
Mifare tag	4.0	68x38	7	3	28	15.0

Uplink: Measuring the IC-Voltage

The IC-voltage u2 was measured by applying a defined magnetic field, using the bridge according to ISO/IEC 10373-6

Transponder

IC-voltage



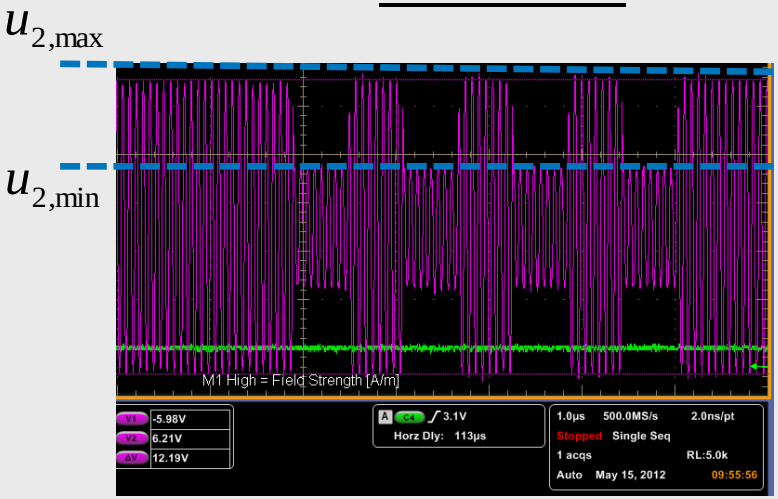
Reader with defined magnetic field strength

Uplink Signal

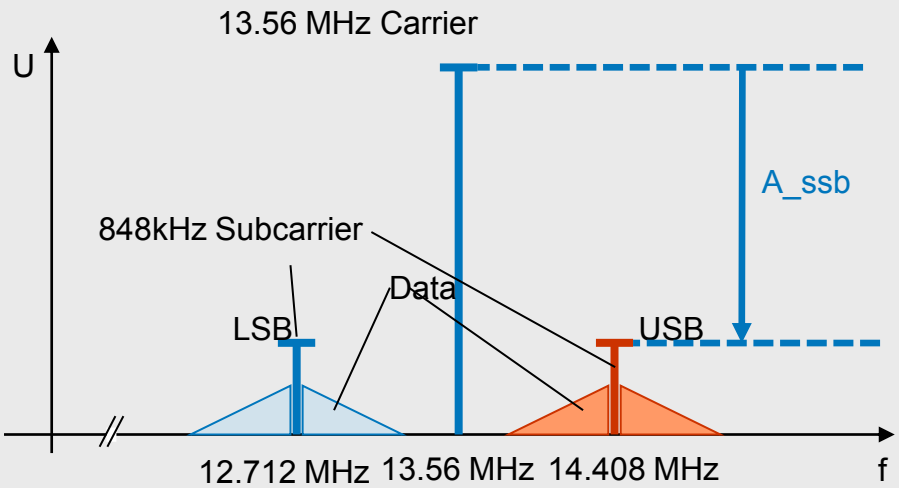
To eavesdrop the uplink data, it is sufficient to detect the upper side band:

ISO/IEC 14443A Mancester coded uplink signal with 847.5kHz subcarrier

Time domain



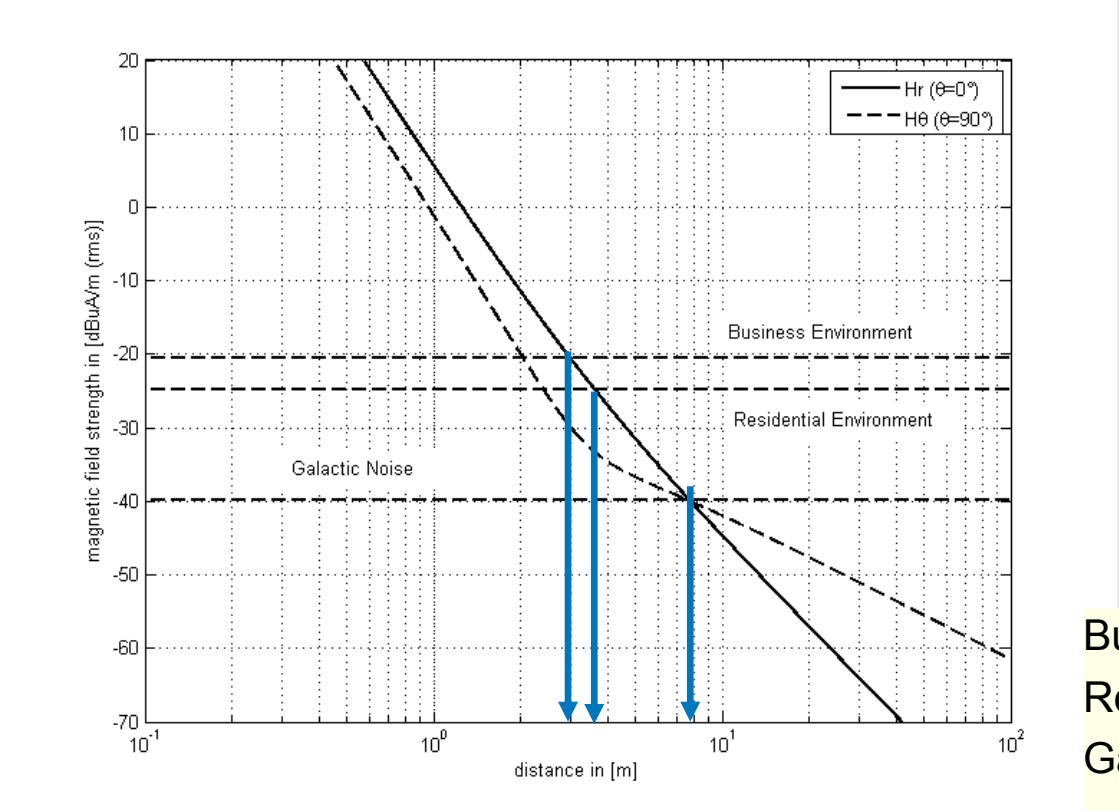
Frequency domain



	IC-Voltage U2 [V(rms)]	IC-Load R2 [Ohm]	Coil-Current I2 [A(rms)]	A_ssb [dBc]
1.5 A/m(rms)	3.5 / 1.5	426 / 175	11.7 / 9.1	-24.dBc
4.5 A/m(rms)	4.3 / 3.0	169 / 117	27.4 / 26.4	-40.6 dB

Uplink Results

Depending on the applied noise a eavesdropping distance between 3 and 8 m is calculated for H = 1.5 A/m



Business Environment	➔	3.0m
Residential Environment	➔	3.6m
Galactic noise	➔	7.7m

Uplink Results (Coherent Demodulation)

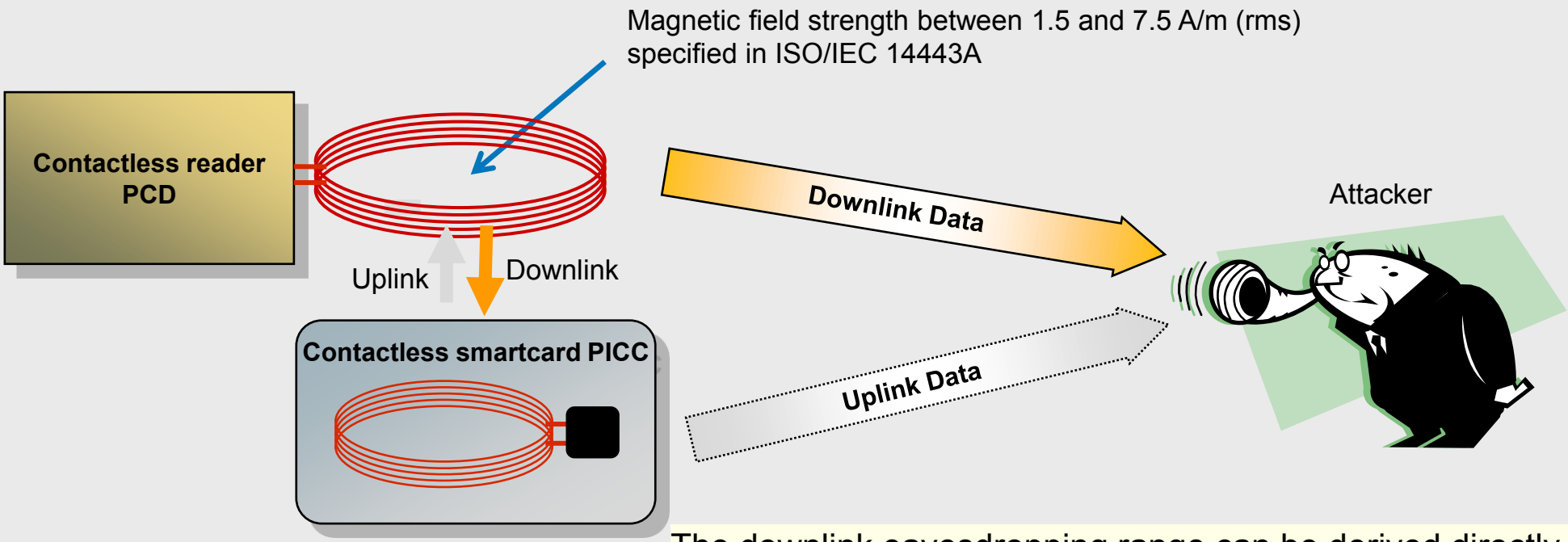
Maximum Eavesdropping distance depending on the BER, applied noise and field strength

	Noise Source		
	Business	Residential	Galactic
BER =0.1%			
1.5 A/m(rms)	3.2 m	3.9 m	9.4 m
4.5 A/m(rms)	2.2 m	2.7 m	5.5 m
BER=0.01%			
1.5 A/m(rms)	3.0 m	3.6 m	7.7 m
4.5 A/m(rms)	2.1 m	2.5 m	5.1 m

Eavesdropping range lies between

- 2.2 and 9.4 m for BER of 0.1%
- 2.1 and 7.7 m for BER of 0.01%
- With un-coherent demodulation the range decreases by 15 %

Downlink Eavesdropping



The downlink eavesdropping range can be derived directly from the magnetic strength at the reader's position

Downlink Results (Coherent Demodulation)

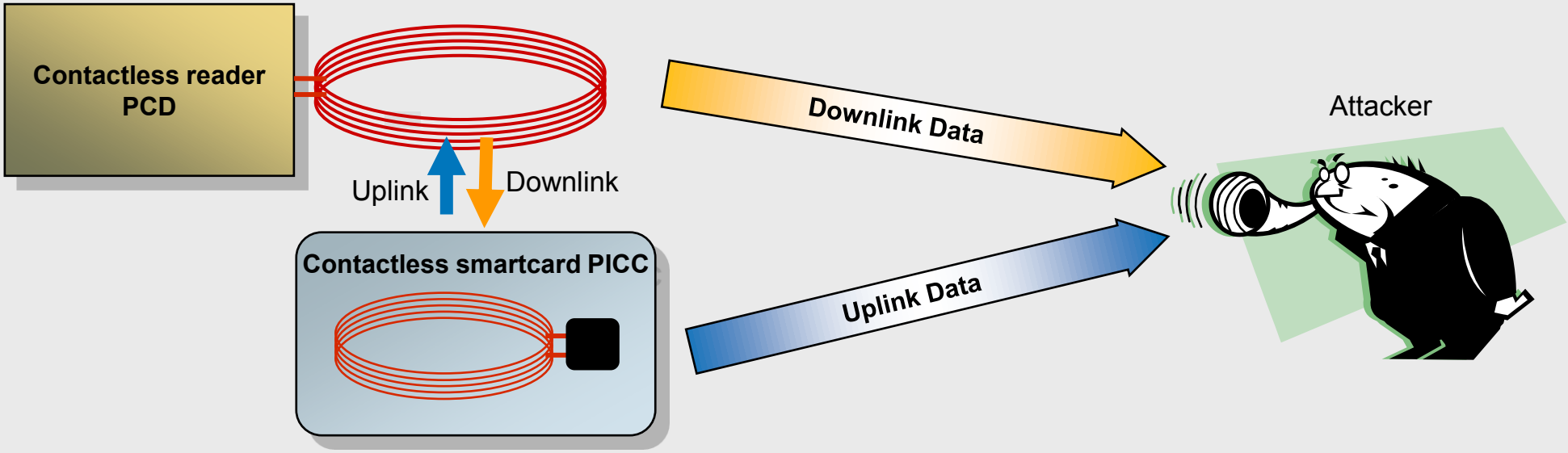
Maximum Eavesdropping distance depending on the BER, coil radius, applied noise and field strength

	Noise Source		
	Business	Residential	Galactic
BER =0.1%			
1.5 A/m(rms) / 3cm coil radius	10.9 m	18.4 m	107.8 m
7.5 A/m(rms) / 7.5cm coil radius	ca. 0.9 km	ca. 1.5 km	ca. 8.5 km
BER=0.01%			
1.5 A/m(rms) / 3cm coil radius	8.8 m	15.2 m	63.4 m
7.5 A/m(rms) / 7.5cm coil radius	ca. 0.7 km	ca. 1.2 km	ca. 7 km

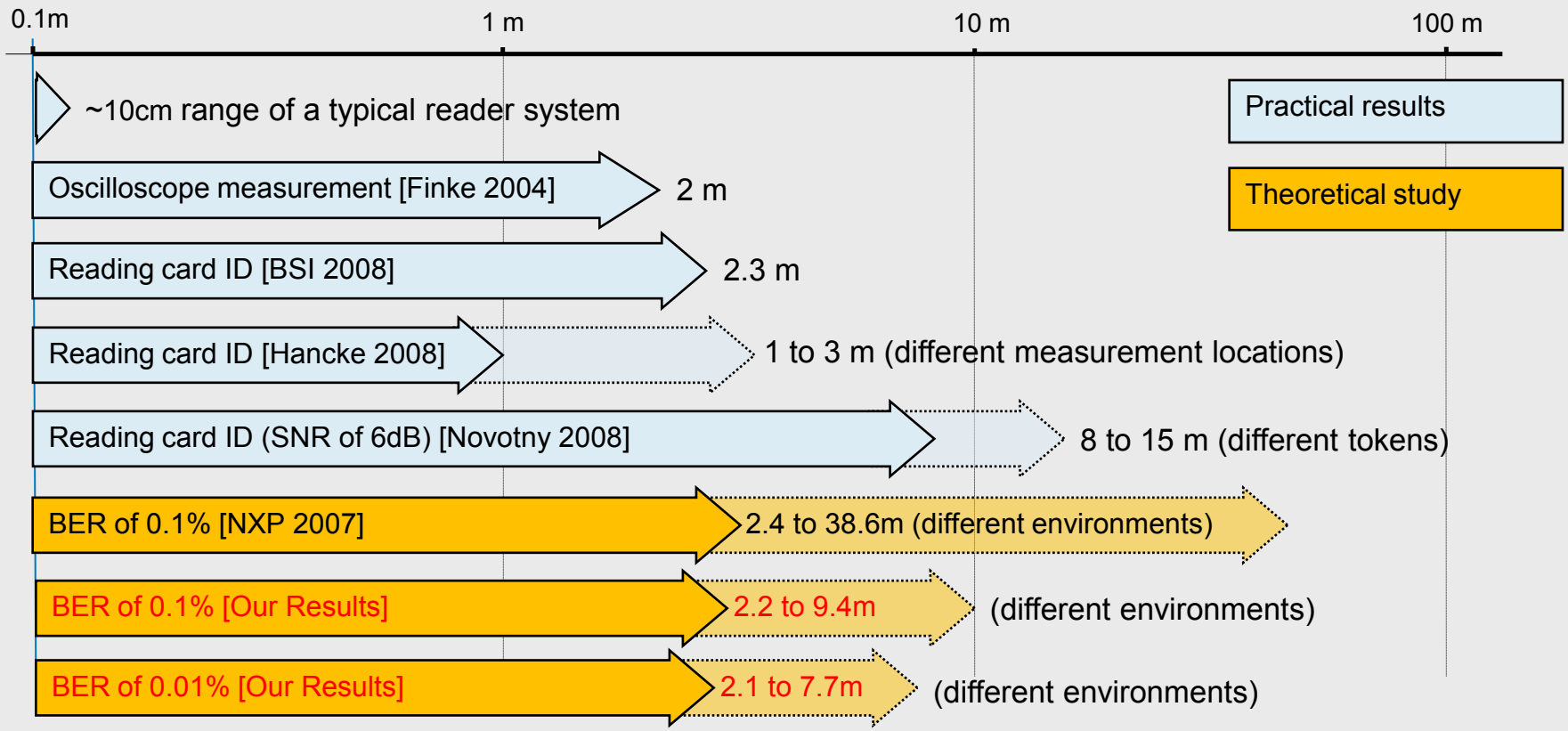
Eavesdropping range lies between

- 10.9 m and 8.5 km for BER of 0.1%
- 8.8 m and 7 km for BER of 0.01%
- With un-coherent demodulation the range decreases by 30%

Uplink & Downlink Eavesdropping



Our Results Compared to Literature



➔SNR of 9.8dB instead of only 6dB in the measurements (with 6dB we calculate a maximum distance of 15m)

➔Simplified assumptions like free space propagation against nearly undefined measurement conditions (as it is in a real environment)

Older Studies vs. this Study

Differences between older studies and this study

	Older Studies	This study
Required BER	0.1 %	0.1% / 0.01%
Noise floor	Man Made Noise in rural environment	Galactic noise
Noise bandwidth	= 1.5 / (Bit duration)	= 1 / (Bit duration)
Tag‘s loop current	= (Modulation voltage) / (Loop inductance)	Full circuit model
Physical model	Near field: Biot-Savart law Far field: Radiation (using radiation resistance)	Near & far field: Formulas for small loop antenna

Conclusion

- Bottleneck of the eavesdropping range is the detection of the uplink signal
- A higher magnetic field of the reader reduces the detection range of the uplink signal due to the control behaviour of the IC chip
- Theoretic range lies between 2.2 and 9.4m (for BER of 0.1%) and 2.1 and 7.7m (for BER of 0.01%) – both with coherent modulation
- Calculation are performed under simplified assumptions as free space propagation & pure Gaussian noise

  ➔ range limits can only give an indication for measurements
  (coupling into pipes/wires could also cause excessive range)