Extending ISO/IEC 14443 Type A Eavesdropping Range using Higher Harmonics

Maximilian Engelhardt [1], Florian Pfeiffer [2], Klaus Finkenzeller [3], Erwin Biebl [1]

[1] Fachgebiet Höchstfrequenztechnik - Technische Universität München

[2] perisens GmbH

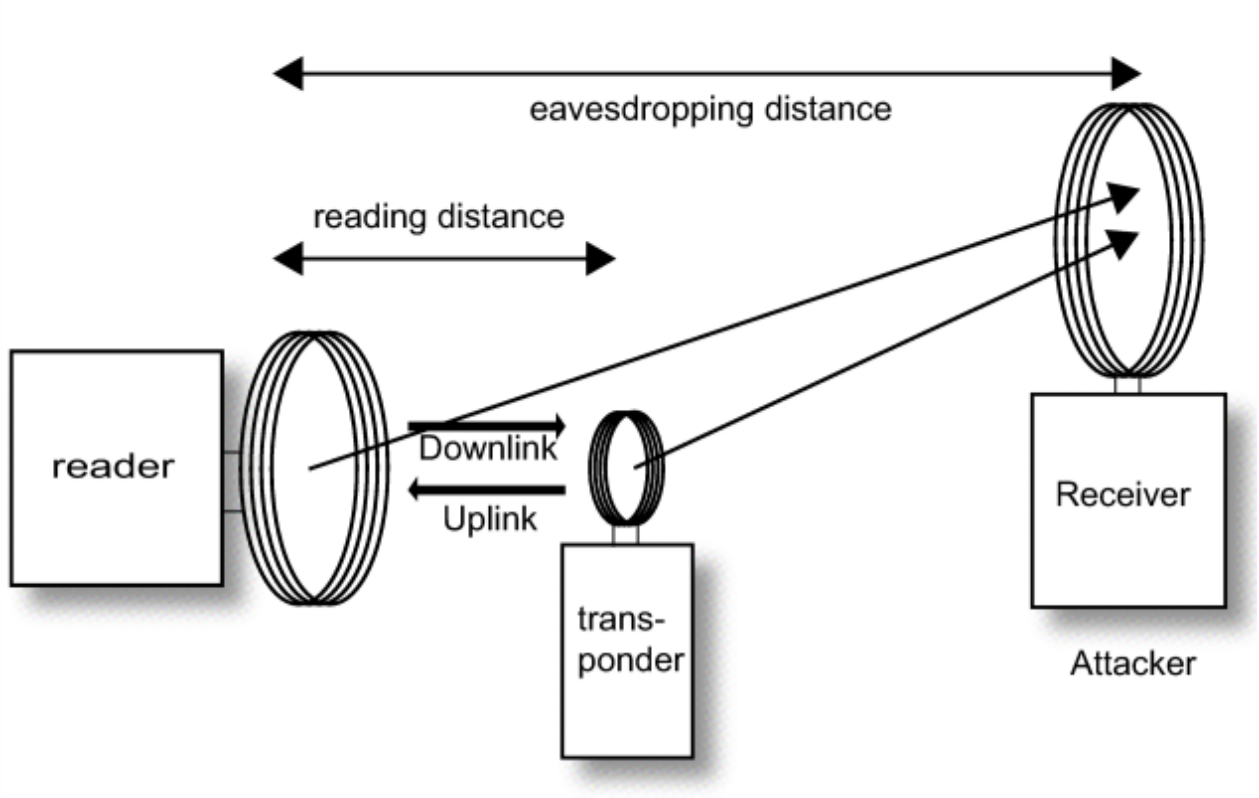
[3] Giesecke & Devrient

Smart SysTech 2013

Outline

Principle of Eavesdropping

Eavesdropping is generally possible on larger distances then active communication



K. Finkenzeller, RFID-Handbuch, 6th ed. München: Hanser, 2012, `http://rfid-handbook.com`

Motivation

- ISO/IEC 14443 type A
- Reader frequency at 13.56 MHz
- Short operating range is security feature in critical applications
- Wide usage: ticketing, access control, identity verification, etc.
- Uplink signal much weaker than downlink signal
- Focus on uplink signal

Frame Error Rate

For a 256 byte frame a bit error rate of less than 0.01 % is required for error free detection in 81.5 %

- Typical frame length 256 byte
- Probability that a frame with N-bits arrives without any bit error: $(1 - BER)^N$

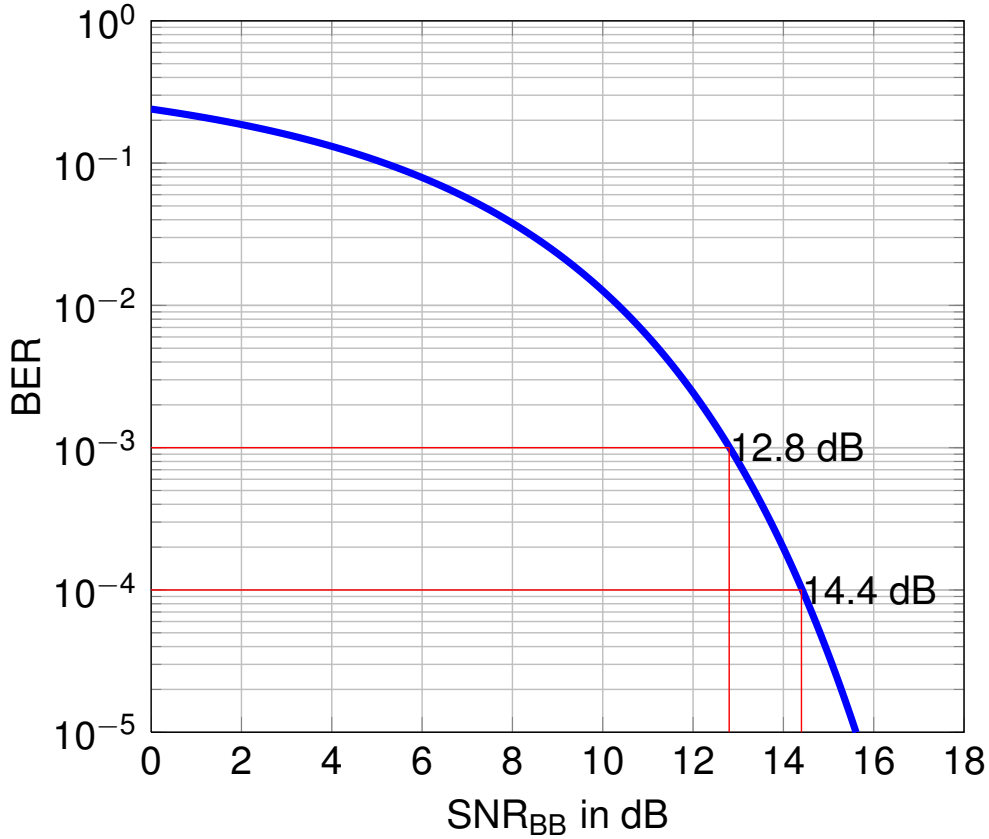
Frame length	BER			
	1 %	0.1 %	0.01 %	0.001 %
4 byte	72.5 %	96.6 %	99.7 %	100 %
16 byte	27.6 %	88.0 %	98.7 %	99.9 %
64 byte	0.6 %	59.9 %	95.0 %	99.5 %
256 byte	0 %	12.9 %	81.5 %	98.0 %

Bit Error Rate as a Function of SNR

To achieve a BER smaller than 0.01 % a baseband SNR better than 14.4 dB is required

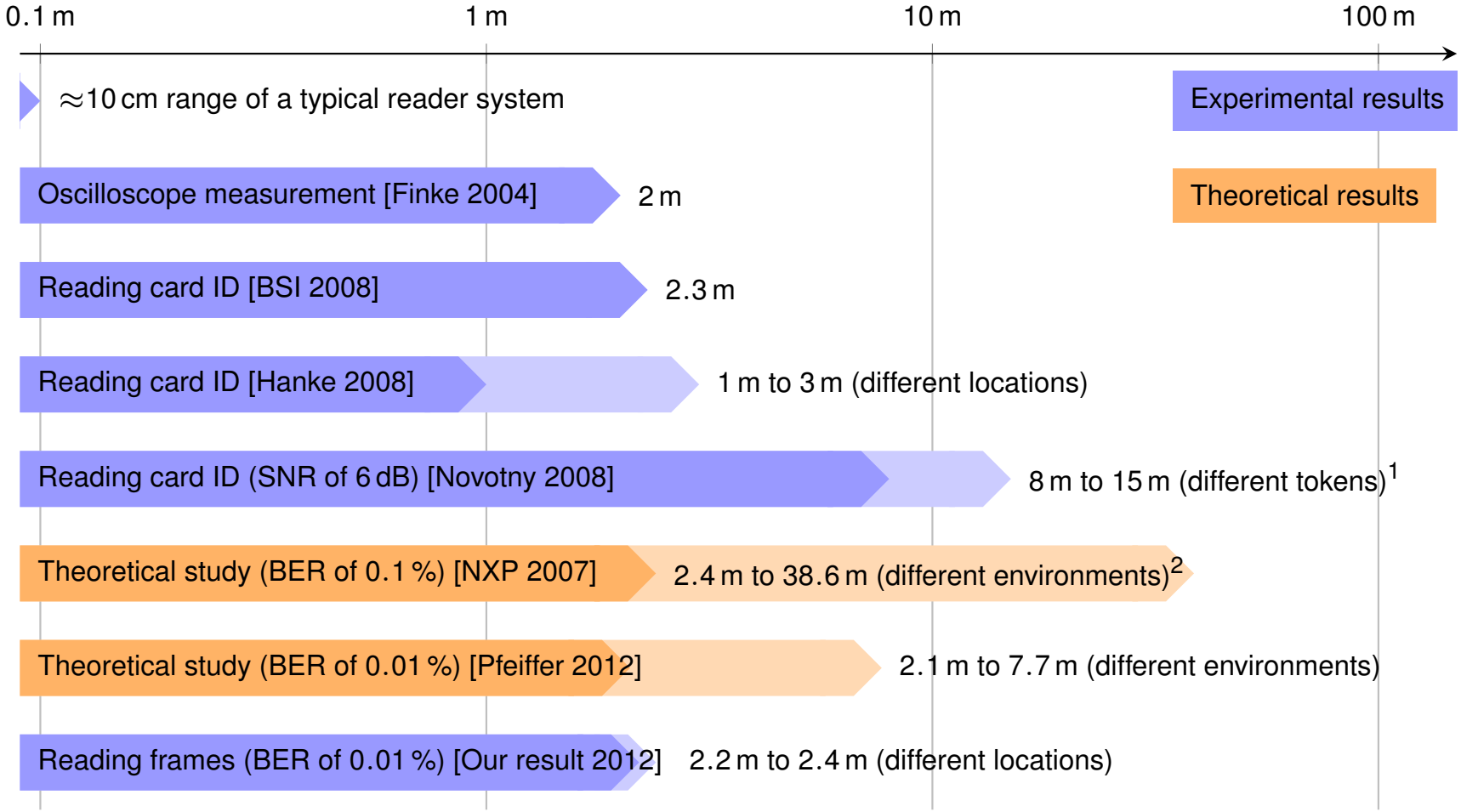
- Uplink Signal
- 848 kHz subcarrier
- Load-modulated with a 106 kbit/s Manchester code
- Baseband binary ASK signal corrupted with additive white Gaussian noise (AWGN):

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



Current Publications

Publications typically show an eavesdropping distance of 1 to 3 m for experimental studies investigating the fundamental wave.

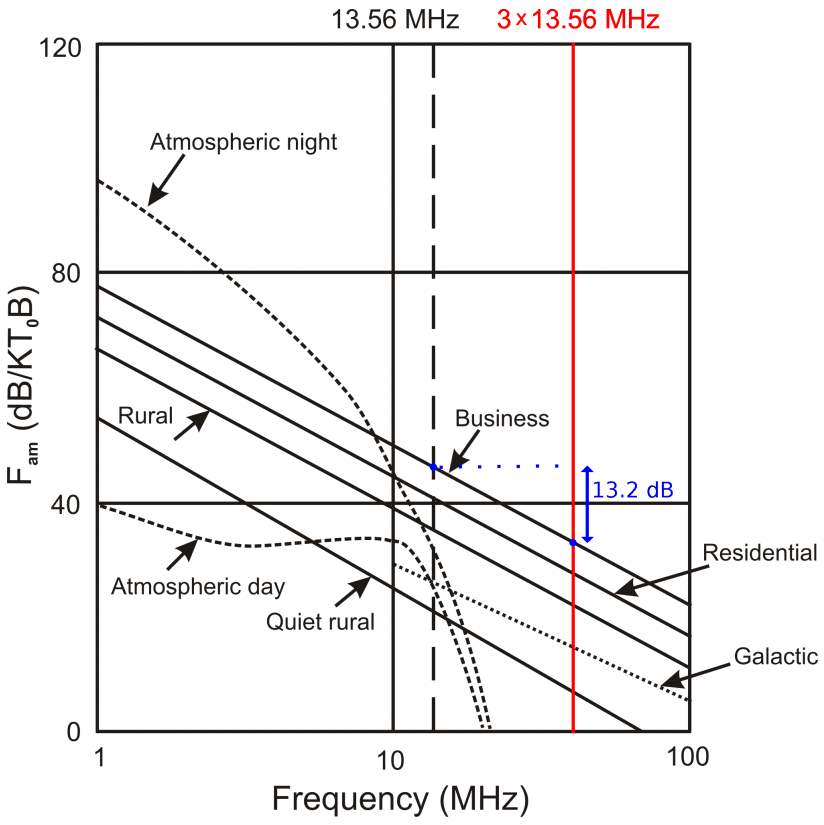


[1] Such great distances couldn't be verified by other measurements and don't match the theory, so we assume coupling effects were involved.

[2] This is only a theoretical value that cannot be reached in reality due to galactic noise

Advantages of Higher Harmonics

By using higher harmonics an eavesdropper has several advantages.

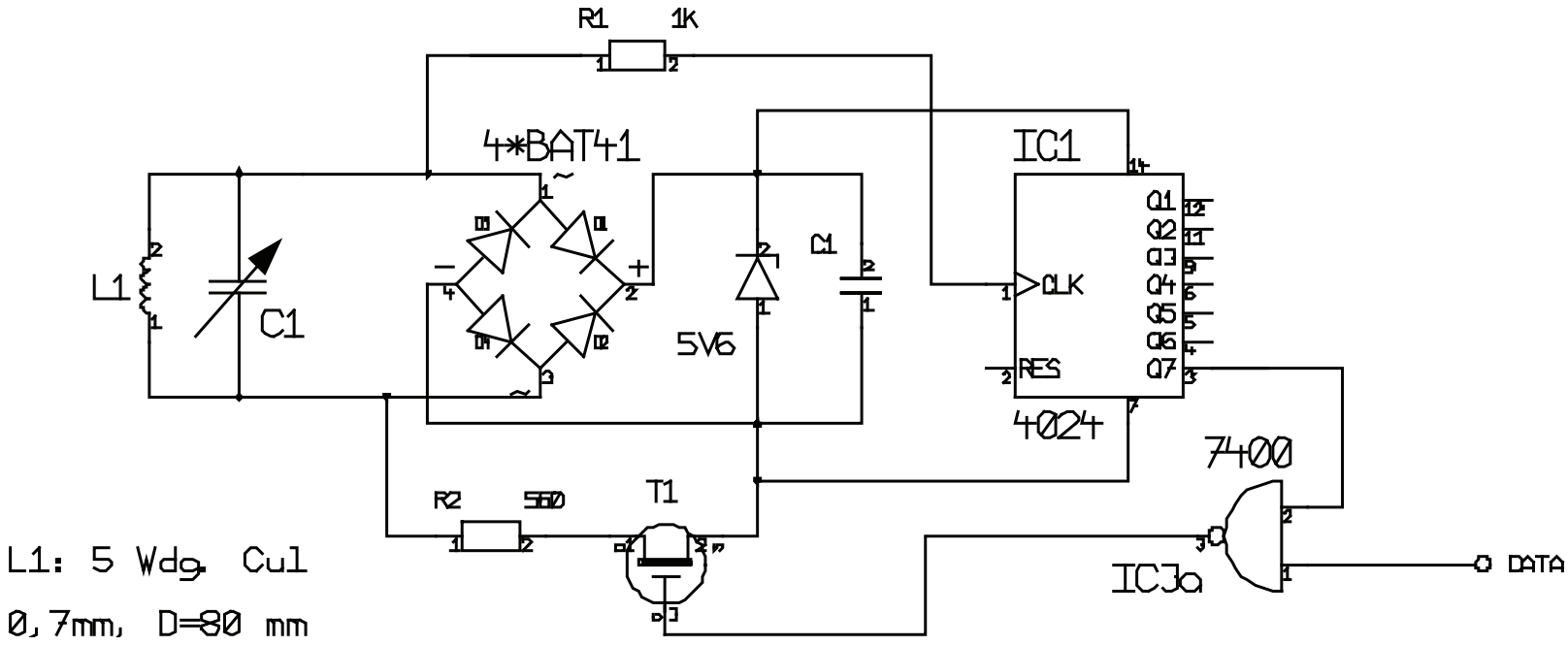


- Less noise from the environment
- Use of optimised antennas possible
- Wave propagation instead of magnetic coupling

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

Analog Frontend

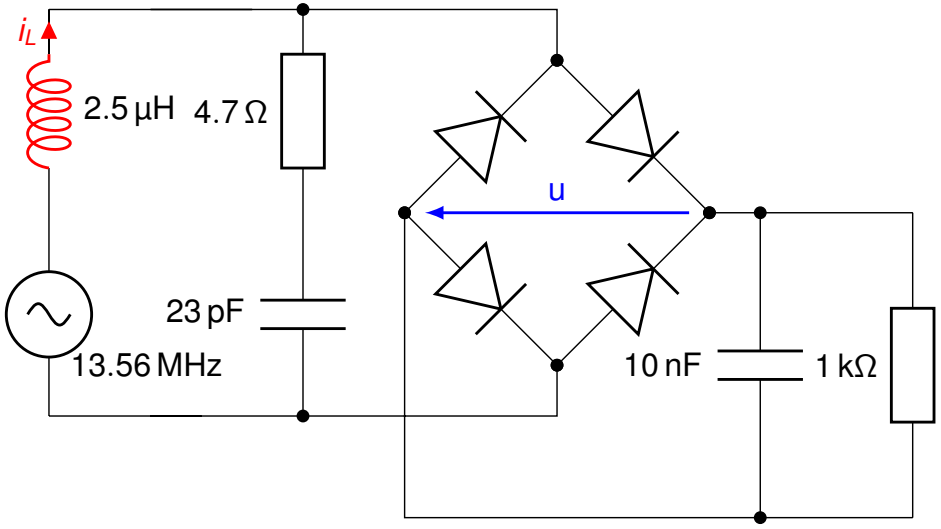
The analog frontend shown consists of a rectifier and means to generate load modulation

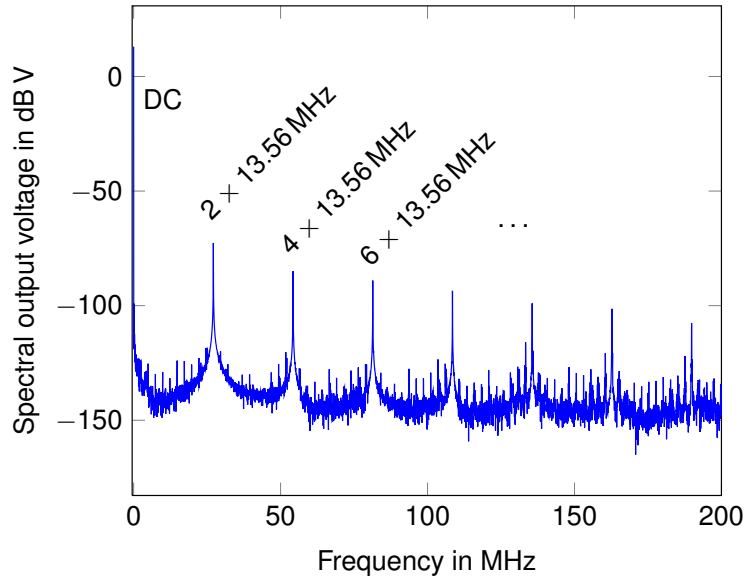


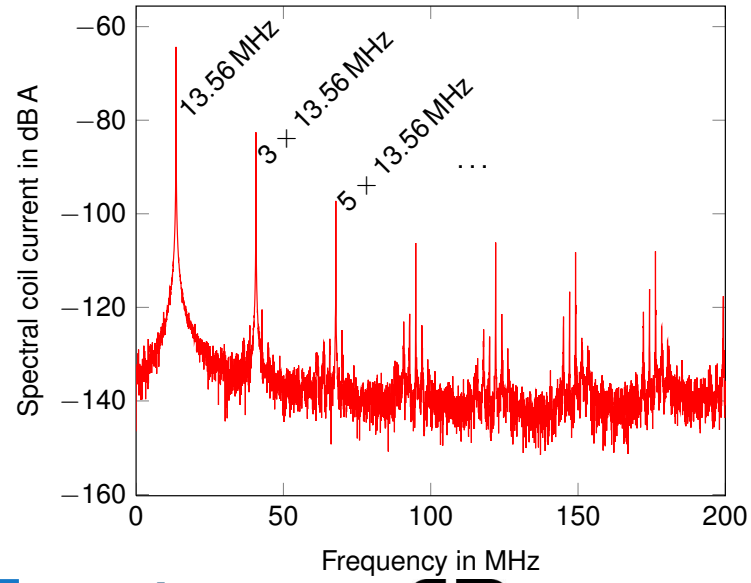
K. Finkenzeller, RFID-Handbuch, 6th ed. München: Hanser, 2012, `http://rfid-handbook.com`

Simulation

The rectifier circuit generates odd order harmonics in the current of the coil



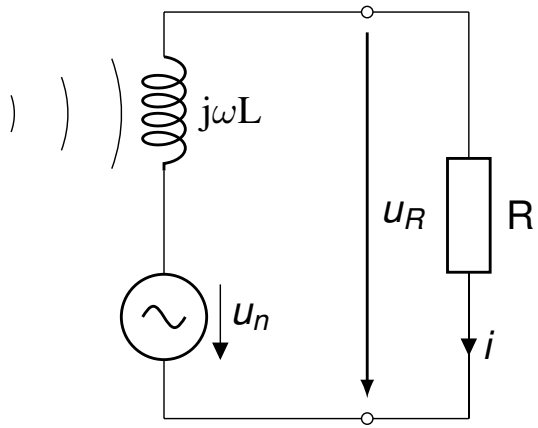




Near Field Measurement

Dominant in the near field are the odd harmonics

Near field measurement using a small coil placed on the card



$$u_n = u_R \frac{R + j\omega L}{R}$$

$R = 50\,\Omega$

$L = 0.8\,\mu H$

Harmonics	1	2	3	4	5	6	7
Frequency [MHz]	13.56	27.12	40.68	54.24	67.80	81.36	94.92
Power [dBc]	0	−54	−23	−58	−35	−56	−38

Far Field Measurement

Radiation of generated harmonics into the far field can occur

- Radiation into the far field depends on the availability of a suitable antenna.
- In our setup the USB cable connecting the reader acted as antenna.
- Coupling depends on the position of the card on the reader.
- Below are two exemplary positions where coupling and radiation did occur.

Far Field Measurement

We measured dominant field strength of the 3rd and 7th harmonic

Measurement of electric field strength at a distance of about 2.3 m.

Harmonic	2	3	4	5
Frequency [MHz]	27.9675	41.5275	55.0875	68.6475
el. field strength [dB µV/m]	−1	22	−7	−21

Harmonic	6	7	8	9
Frequency [MHz]	82.2075	95.7675	109.3275	122.8875
el. field strength [dB µV/m]	−14	17	−11	−5

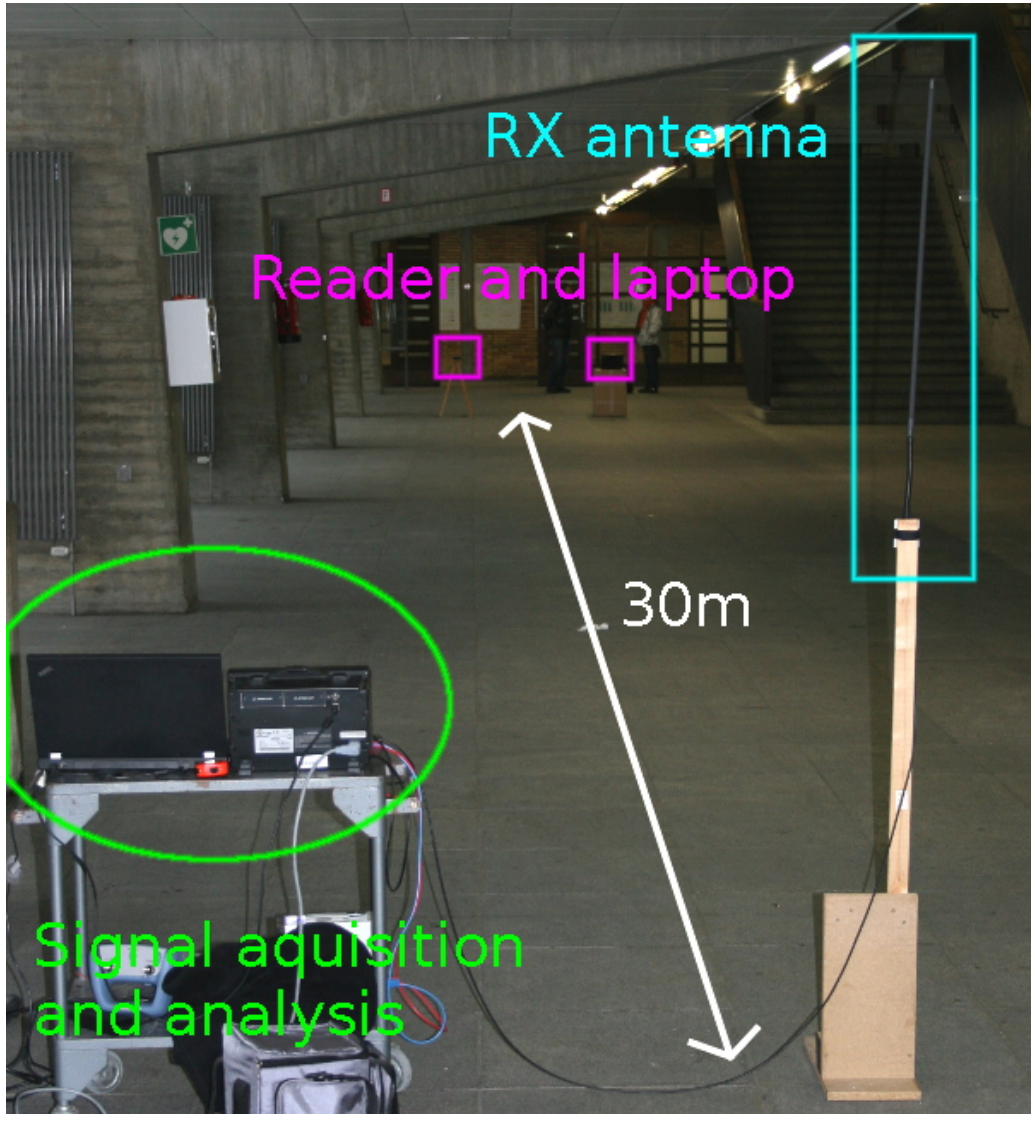
Measurement Setup

We performed measurements in a university corridor

- University corridor
- Mifare pegoda CL RD 701 reader
  - with factory supplied 2 m USB cable
- Shortened quarter wavelength antenna from Procom (SB 30-88-MU1)
- Low cost receiver using a TDA2542 IC
- A/D conversion using a digital oscilloscope

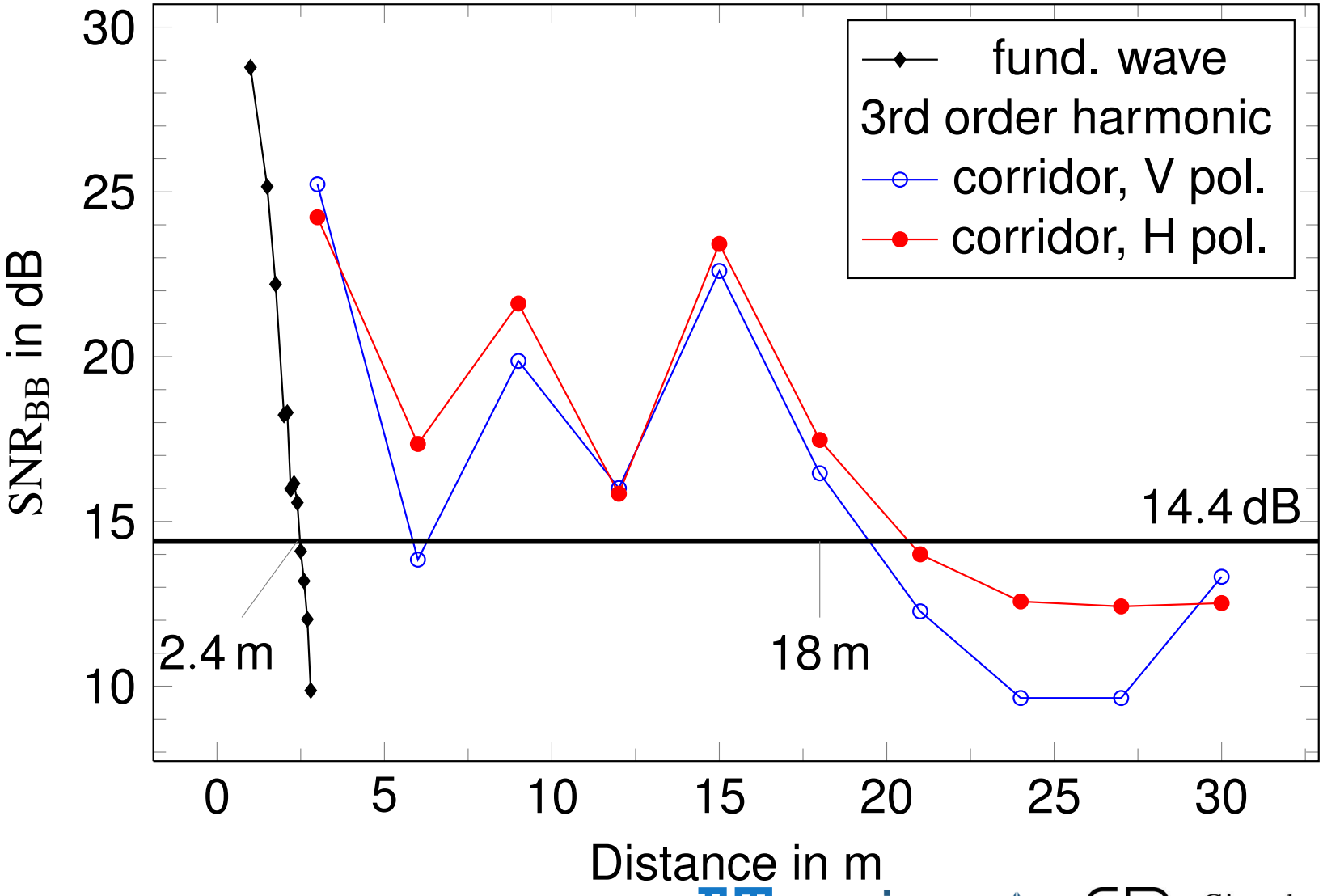
Measurement Setup in the Corridor

We perfomed measurements up to 30 m in the corridor using a low-cost receiver



Measurement Results

We were able to measure a SNR better than 14.4 dB in up to 18 m. In 30 m a SNR of 13.3 dB (BER of 5.4×10^{-4}) could still be measured



Comparison with Other Publications

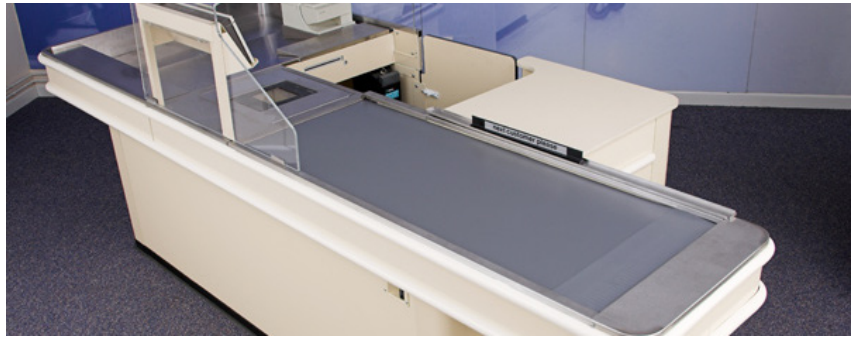
Our measured eavesdropping distance is more than 6 times larger than the ones measured at the fundamental wave.

- Published experimental results are in the range of 2 to 3 m
  - all studies at the fundamental wave
- Our results (experimental):
  - fundamental wave: 2.4 m
  - 3rd order harmonic: 18 m

Countermeasures

Avoid coupling and radiation of harmonics

- Suppress harmonic generation at card rectifier by using harmonic filters (difficult).
- Avoid radiation of connected cables, e. g. using snap-on ferrites.
  - In our case this was enough so no useful signal could be received any more at the frequencies of the harmonics.
- Avoid metal objects in close vicinity.



Summary

- Eavesdropping distances can be much larger using higher harmonics compared to the fundamental wave.
- Antenna for radiation of the harmonics into the far field is necessary.
- Countermeasures should be taken to prohibit this kind of attack.