Theoretical Limits of ISO/IEC 14443 type A RFID Eavesdropping Attacks

Florian Pfeiffer, perisens GmbH, Arcistr. 21, 80333 München, pfeiffer@perisens.de
Klaus Finkenzeller, Giesecke & Devrient GmbH, Prinzregentenstraße 159, 81607 München, klaus.finkenzeller@gi-de.com
Erwin Biebl, Fachgebiet Höchstfrequenztechnik der Technischen Universität München, Arcistr. 21, 80333 München, biebl@tum.de

Summary / Abstract

Inductively coupled ISO/IEC 14443 compliant RFID systems are used in many security-relevant applications. A key security feature is their very short range of about 10 cm. Eavesdropping attack scenarios are a well known and recognised threat for these systems. In this paper, we present a theoretical calculation of the maximum eavesdropping range of an inductive coupled reader-transponder communication with passive load modulation. Theoretical limits for eavesdropping distances are calculated for exemplary ISO/IEC 14443A transponder and reader configurations in different environments. According to our results the previously published range limits are stated as too high.

April 23, 2012

1 Introduction

Inductively coupled ISO/IEC 14443 compliant RFID systems are being used in a huge number of security-relevant applications such as payment (credit cards), ticketing (public transport and events), access control (company card) and identity verification (ePass, eID).

Typical ISO/IEC 14443 passive tags are designed to operate over a distance of about 10 cm. The short communication range of a smart card is an important security feature. Extended range [Fin11], skimming attacks [Kir06] and eavesdropping are well known threads for these systems which are seeking to overcome the short range. An extended range attack is the ability of an active tag to establish an unauthorized communication with a reader. Skimming is the unauthorized access of tag data without an authorized tag-reader connection. Eavesdropping is defined as unauthorized data access to an authorized reader-tag communication.

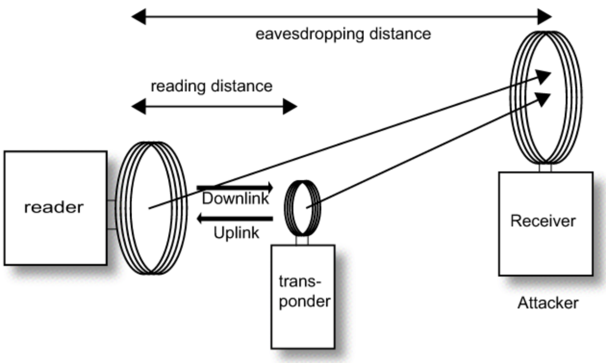

Figure 1: Eavesdropping attack of a RFID communication [Fin12]

In several studies eavesdropping attack scenarios have been analyzed theoretically and experientially, but still there is an ongoing discussion about the maximum eavesdropping distance. [Fin04] shows that it is possible to read an ISO/IEC14443A uplink communication within a range of up to 2 m by means of an oscilloscope measurement. In [BSI08] an ISO/IEC 14443A-eavesdropping of the ID card number was reliably carried out over a distance of 2.3 m. [Han08] successfully performed an ISO/IEC 14443A-eavesdropping attack over a distance of 1 m in an entrance hall and 3 m in the lab corridor. [Nov08] achieved a maximum eavesdropping distance between 8 and 15 m using different transponders.

The mentioned range differences show that many factors like environmental conditions, the definition of a successful eavesdropping, transponder and reader hardware strongly affect the measurement results. In a theoretical study, [NXP07] calculates a maximum 14443A-eavesdropping distance between 3.6 m for business and almost 40 m for quite rural environments. The theoretical results for business environments are in good accordance to the measurement results. But until now, it has not been possible to reach an eavesdropping distance even close to 40 m. According to our calculations the theoretical limits of the eavesdropping distance are substantially lower than the mentioned 40 m.

2 Communication Theory

A successful eavesdropping attack requires that the attacker is able to detect the bidirectional data communication between a reader and a transponder with a sufficient accuracy. The reliability of the data detection is directly connected to the bit error rate (BER). The BER itself is a function of the modulation scheme and the signal-to-noise ratio (SNR).

This paper concentrates on the eavesdropping of a reader transponder connection according to the ISO/IEC 14443 type A standard at a default bitrate of 106 kps. In the data transfer from the reader to the transponder (downlink) the standard specifies a 100 % Amplitude Shift Keying (ASK) with Modified Miller coding. To ensure a continuous power supply of the transponder, the width of the Miller glitches is limited to 2 – 3 µs. For the transponder to reader communication (uplink) the transponder's chip impedance is keyed by a modulated 848 kHz subcarrier, usually by switching a modulation resistor on and off in the transponder-IC. The subcarrier itself is ASK modulated with a Manchester coded data signal at the same bitrate.

As we are interested in the maximum reading distance, we assume optimum receiver architecture with a matched filter and a synchronous detector using an optimum threshold. The matched filter maximizes the SNR in presence of stochastic noise, while the synchronous detector with optimum threshold minimizes the BER. For a binary ASK signal corrupted with additive white Gaussian noise (AWGN) the probability of bit errors reads as [Poz08]

$$BER = \frac{1}{2}\operatorname{erfc}\left(\frac{1}{2}\sqrt{SNR_{\mathrm{BB}}}\right), \tag{2.1}$$

where SNR_{BB} is the baseband SNR. For a coherent demodulation of the amplitude modulated (AM) signal the baseband SNR is twice as high as the high frequency SNR. At high frequencies the noise power is divided equally into in-phase and quadrature (I&Q) components. Assuming the desired signal as in-phase, half of the noise power can be removed after down conversion. For coherent demodulation the BER reads as

$$BER = \frac{1}{2}\operatorname{erfc}\left(\frac{1}{2}\sqrt{2SNR_{\mathrm{HF}}}\right) \tag{2.2}$$

and for non-coherent demodulation

$$BER = \tfrac{1}{2}\operatorname{erfc}\left(\tfrac{1}{2}\sqrt{SNR_{\mathrm{HF}}}\right). \tag{2.3}$$

Figure 2 shows the BER in dependence of the SNR for coherent and non-coherent demodulation.

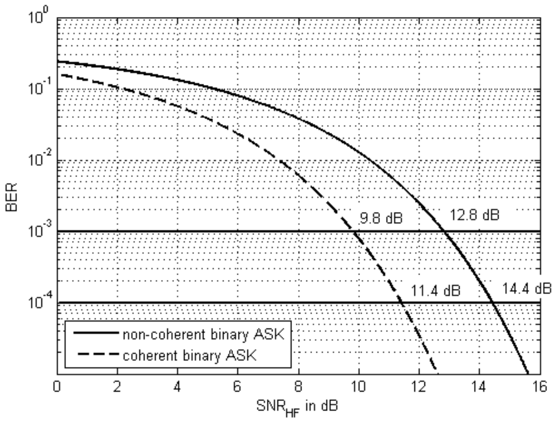

Figure 2: Bit error rate in dependence of SNR for binary ASK signal corrupted with AWGN

The required BER depends on the amount of information bits that are intended to be eavesdropped. It is obvious that the eavesdropping of a transponder-ID of only 4 Bytes allows a higher BER for reliable detection as a complete data frame of 256 Bytes. For security applications as identity verification (ePass, eID) the ISO/IEC standard allows a Pseudo-Unique PICC Identifier (PUPI) where the ID is randomly generated. Eavesdropping of such a randomly generated ID is completely worthless for every attacker. Therefore we concentrate on the eavesdropping of data frames containing up to 256 Bytes according to [ISO08]. Considering that the ISO/IEC 14443 type A standard does not provide an error-correction code, the probability that a frame with N bits arrives without any bit error $(1 - FER)$ is N times the product of the probability that a single bit arrives error:

$$1 - FER = (1 - BER)^{N} \tag{2.4}$$

In security relevant applications the communication is usually encrypted where a single bit error would significantly complicate or even prevent an unauthorized decryption. Table 1 shows the probability of an error-free detected frame in dependence of BER and frame length:

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%

Table 1: Probability that a frame arrives with no bit errors (without any error-correction)

According to Table 1, a BER of 0.1% - as used in [NXP07] - is not sufficient for a reliable error-free detection of a 64 or 256 byte frame. Therefore, we also include a BER of 0.01% in our study which allows an error-free detection of a 256 byte long frame in 81.5% of all attempts.

A BER of 0.1% implies a minimum SNR_{HF} of 9.8 dB for coherent and 12.8 dB for non-coherent demodulation. For a BER of 0.01% the minimum detectable signal must be even 11.4 dB and 14.4 dB above the noise level, respectively (Figure 2). A coherent demodulation requires an additional hardware effort from the attacker as the phase of the signal has to be reconstructed.

In the HF band the external noise with atmospheric, galactic and man-made noise is typically significantly greater than the internal receiver noise. [ERC99] gives an overview of average noise levels of external noise sources including atmospheric, galactic and man-made noise. Depending on the frequency, the environment conditions as well as the day and year time different noise sources can be relevant. The atmospheric noise strongly depends on the time of the day and even on the season of the year. Figure 3 shows the different noise levels expressed in noise factor F_{am} above thermal noise in dependence of the frequency.

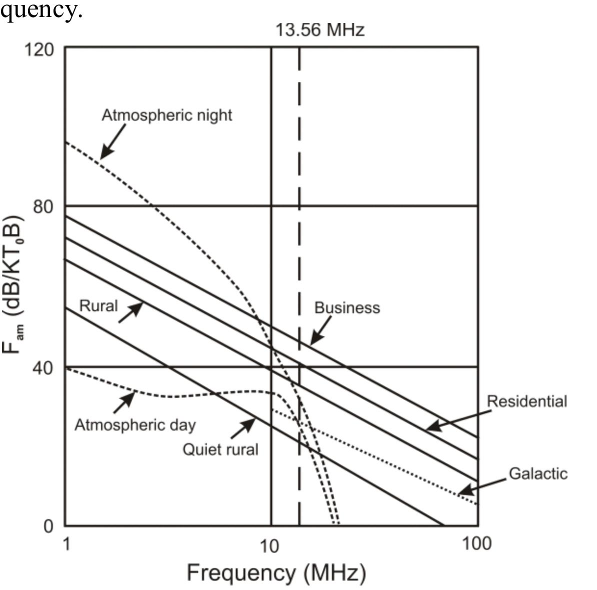

Figure 3: Solid lines indicate median values of man-made noise in F_{am} (dB above thermal noise at 288K), dashed lines indicate atmospheric noise and the dotted line shows the galactic background noise [Bia07]

Between 10 and 20 MHz man-made noise is the predominant noise source in a business or residential environment which is the most critical environment for attack scenarios. Besides the man-made noise in these two environments, this paper pays attention to the galactic noise as the absolute noise floor, but the reader should be aware that the theoretical maximum distance based on the galactic noise will usually not be achieved since atmospheric and/or man-made noise is often higher. To calculate the median value of the man-made noise level the noise factor F_{am} is defined according to [ERC99]

$$F_{\mathrm{am}} = c - d\log\left({}^{f}/_{1\mathrm{MHz}}\right) \tag{2.5}$$

c and d are environment depending constants. With the noise factor F_{am}, the center frequency f and the signal bandwidth B the median value of the electric noise field strength can be calculated as follows [ERC99]:

$$\begin{aligned}|E_{\mathrm{n}}|[\mathrm{dB\mu V/m}] = F_{\mathrm{am}} &- 95.5\\ &+ 20\log\left({}^{f}/_{1\mathrm{MHz}}\right)\\ &+ 10\log\left({}^{B}/_{1\mathrm{Hz}}\right)\end{aligned} \tag{2.6}$$

$|E_{\mathrm{n}}|[\mathrm{dB\mu V/m}]$ and $|H_{\mathrm{n}}|[\mathrm{dB\mu A/m}]$ are absolute values of the complex field strength. In the following calculations we use rms values, so 3 dB has to be subtracted.

$$\begin{aligned}E_{\mathrm{n}}&[\mathrm{dB\mu V/m(rms)}]\\ &= F_{\mathrm{am}} - 98.5\\ &+ 20\log\left({}^{f}/_{1\mathrm{MHz}}\right)\\ &+ 10\log\left({}^{B}/_{1\mathrm{Hz}}\right)\end{aligned} \tag{2.7}$$

Considering the free space impedance of 377 Ohm the corresponding magnetic field strength is

$$|H_{\mathrm{n}}|[\mathrm{dB\mu A/m}] = E_{\mathrm{n}}[\mathrm{dB\mu V/m}] - 20\log 377. \tag{2.8}$$

The noise field strength only depends on the centre frequency and bandwidth of the signal.

For the downlink signal (from the reader to the transponder) the centre frequency is 13.56 MHz as it is directly modulated on the carrier. In contrast, the uplink signal (from the transponder to the reader) is keyed by a modulated subcarrier of 848 kHz. The subcarrier itself is ASK modulated with the Manchester coded data signal at a bitrate of 106 kbps. The subcarrier modulation splits the data information in two side bands, which can both be used for demodulation (see Figure 4).

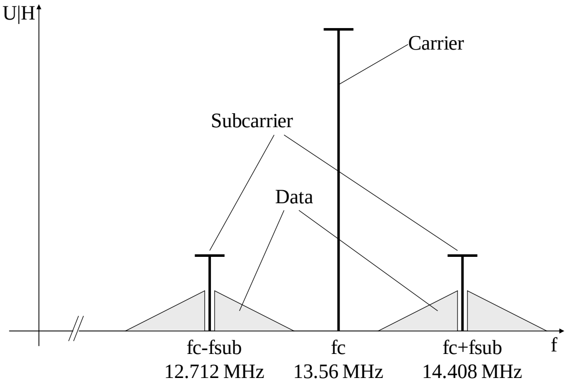

Figure 4: Spectrum of an ISO/IEC14443 uplink signal [Fin12]

According to Figure 3 the noise field strength decreases with frequency. Hence the upper side band should be evaluated regarding noise considerations. But as the difference in noise power is almost negligible between 12.712 MHz (lower sideband) and 14.408 MHz (upper sideband), it does only marginally affect the distance calculation. In our calculation we still use 14.408 MHz for the uplink and 13.56 MHz for the downlink case.

As we are assuming a matched filter receiver, the signal bandwidth can be obtained by the reciprocal of the effective bit length.

$$B = \frac{1}{T_\mathrm{B}} \qquad (2.9)$$

In the downlink case the effective bit length corresponds to a pulse width of up to 3 µs, as the signal only contains information within the glitch period. The “effective” signal bandwidth is therefore up to 333 kHz. For the uplink signal with a data rate of 106 kbps, the bandwidth is 106 kHz.

Using the equations (2.5) to (2.9), the noise field strength and the required minimum field strength at the attacker’s position can be calculated. Table 2 shows the median value of the noise factor and the resulting magnetic noise field strength for uplink and downlink.

The required minimum signal field strength can be calculated as follows:

$$H_{\mathrm{s,min}}[\mathrm{dB\mu A/m}] = H_\mathrm{n}[\mathrm{dB\mu A/m}] + SNR_{\mathrm{HF,min}} \qquad (2.10)$$

As stated before, the required $SNR_{\mathrm{HF,min}}$ is 9.8 dB for coherent and 12.8 dB for non-coherent demodulation to ensure a BER of 0.1% and 11.4 dB and 14.4 dB for a BER of 0.01 %, respectively.

Noise source	**Business**	**Residential**	**Galactic**
c	76.8	72.5	52.0
d	27.7	27.7	23.0
F_{am} in [dB]	45.4	41.1	26.0
Uplink $H_\mathrm{n}$in [dBµA/m(rms)]	-31.7	-36.0	-51.2
Downlink H_n in [dBµA/m(rms)]	-26.7	-31.0	-46.2

Table 2: Median value of the galactic and man-made noise factor in a business and residential environment and the resulting median value of the noise signal field strength at 13.56 MHz with a bandwidth of 333 kHz for downlink and 14.408 MHz with a bandwidth of 106 kHz for uplink [ERC99]

3 Theoretical Limits

In the previous section, the required signal field strength was determined, which allows the detection of an ISO/IEC14443A signal. In this section, we want to derive the resulting maximum distance from attacker to RFID system, where the required magnetic field strength can be assumed. For HF-RFID systems, loop antennas are usually used to generate or receive magnetic fields. At 13.56 MHz, loop antennas can usually be considered as small loops since the circumference is small compared to $\lambda/_{10} = 2.21$ m. Therefore a constant current can be assumed along the circumference of the loop.

For such a small loop antenna with a single winding and an observation distance greater than the radius of the loop ($\mathrm{r} > a$) the magnetic fields can be derived analytically [Bal05]:

$$H_\mathrm{r} = \mathrm{j}\frac{\mathrm{k}a^2 I_\mathrm{L}\cos\theta}{2\mathrm{r}^2}\left(1+\frac{1}{\mathrm{jk}r}\right)\mathrm{e}^{-\mathrm{jk}r} \qquad (3.1)$$

$$H_\theta = -\frac{(\mathrm{k}a)^2 I_\mathrm{L}\,\sin\theta}{4r}\left(1+\frac{1}{\mathrm{jk}r}-\frac{1}{(\mathrm{k}r)^2}\right)\mathrm{e}^{-\mathrm{jk}r} \qquad (3.2)$$

$$\mathrm{H}_\varphi = 0 \qquad (3.3)$$

Where a is the loop radius, I_L the loop current, $\mathrm{k} = {}^{2\pi}/_{\lambda}$ the wave number and r the observation distance. For a loop antenna with N turns of constant current the total magnetic field strength increases approximately linearly with the number of windings N. In this case, the length of the total loop structure has to be smaller than $\lambda/_{10}$.

Figure 5 depicts the coordinate system applied to the formulas of the small loop antenna.

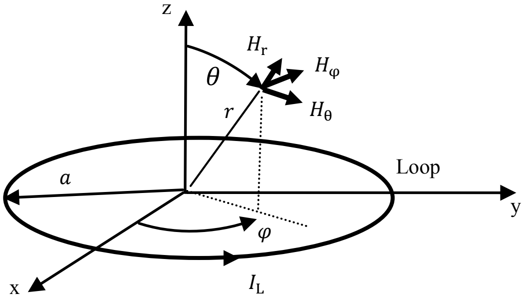

Figure 5: Coordinate system

Figure 6 shows the tangential and radial magnetic field strength of a small loop antenna in dependence of the distance.

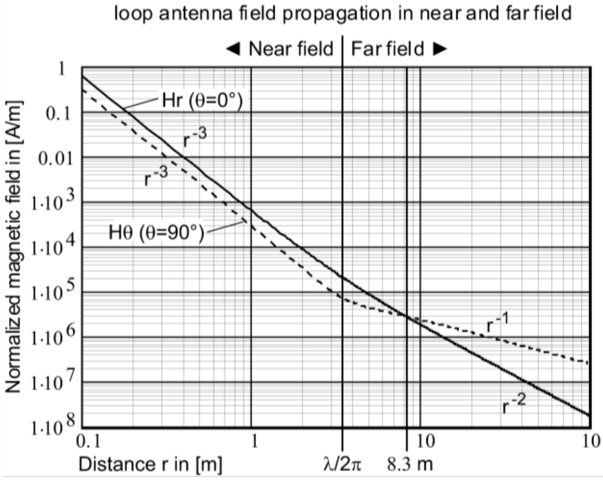

Figure 6: Normalized tangential and radial magnetic field of a small loop antenna in dependence of the distance at 13.56 MHz [Fin12]

In the near field ($r < 2\pi/\lambda = 3.5m$), the maximum radial field is twice the maximum tangential field. For $r >$

$2\pi/\lambda$, however, the radial field decreases faster than the tangential field and at a distance of 8.3 m, the maximum tangential field is larger than the maximum radial field. This point of interception depends only on the wavelength and not on the size of the antenna – provided that the aforementioned assumptions are satisfied. For the calculation of the maximum eavesdropping distance we assume an optimum antenna orientation as shown in Figure 7.

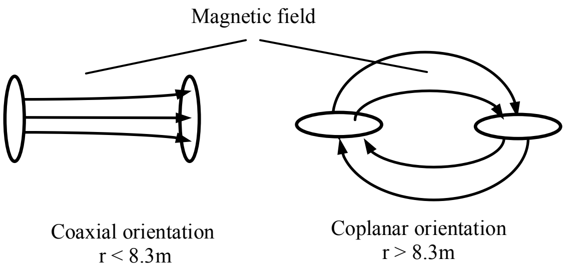

Figure 7: Optimum antenna orientation at 13.56 MHz

3.1 Eavesdropping of downlink signal

In this chapter the maximum eavesdropping distance of the downlink signal (from the reader to the attacker) is analyzed. ISO/IEC 14443 defines a magnetic field strength in zero distance to the reader between 1.5 and 7.5 A/m (rms) [ISO10]. For a circular loop antenna with radius a the loop current can be written as

$$I_{\mathrm{L}} = \frac{H_{\mathrm{r}}(\theta = 0, r = 0)2a}{N}. \qquad (3.4)$$

Inserting the loop current in (3.1) and (3.2), the magnetic field strength can be determined. Considering the noise field strength of Table 2 and the required SNR, the eavesdropping distance of the reader signal can be calculated.

$$H_{\mathrm{r},\theta}(r = r_{\max}) = H_{\mathrm{s,min}} \qquad (3.5)$$

Two different reader configurations with low magnetic field strength and small antenna size on the one hand and high magnetic field and large antenna size on the other hand (see Table 3) will be analyzed.

	Reader 1	Reader 2
Antenna radius a	3 cm	7.5 cm
$H_{\mathrm{r,max}}$	1.5 A/m (rms)	7.5 A/m (rms)

Table 3: Considered reader parameters

As an example, Figure 8 shows the reader field strength in dependence of the distance and the required field levels as horizontal dotted lines for non-coherent demodulation with a BER of 0.01%.

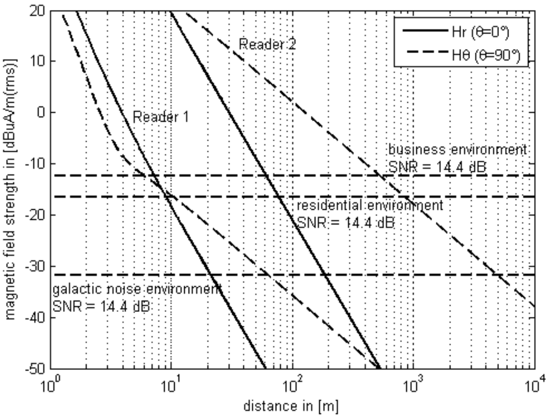

Figure 8: Eavesdropping distances for an ISO/IEC14443A downlink signal assuming different environments (business, residential and galactic noise) for non-coherent demodulation with a BER of 0.01% (SNR = 14.4 dB)

The theoretical downlink ranges for a BER of 0.1% and 0.01% are shown in Table 4 and Table 5.

	Noise source		
demodulation	**Business**	**Residential**	**Galactic**
Reader 1			
non-coherent	7.9 m	12.8 m	76.3 m
coherent	10.9 m	18.4 m	107.8 m
Reader 2			
non-coherent	ca. 0.6 km	ca. 1.0 km	ca. 6.0 km
coherent	ca. 0.9 km	ca. 1.5 km	ca. 8.5 km

Table 4: Maximum downlink eavesdropping range for different readers and environmental conditions calculated for a BER of 0.1%

	Noise source		
demodulation	**Business**	**Residential**	**Galactic**
Reader 1			
non-coherent	7.2 m	10.5 m	63.4 m
coherent	8.8 m	15.2 m	89.4 m
Reader 2			
non-coherent	ca. 0.5 km	ca. 0.9 km	ca. 5 km
coherent	ca. 0.7 km	ca. 1.2 km	ca. 7 km

Table 5: Maximum downlink eavesdropping range for different readers and environmental conditions calculated for a BER of 0.01%

Reader 2 with a high magnetic field strength of 7.5 A/m and large antenna size operating in a strongly disturbed business environment can theoretically be eavesdropped about half a kilometer with a BER of 0.01% and non-coherent demodulation. In a galactic noise environment the theoretical eavesdropping distance is about 5 km. It must be kept in mind that this calculation was performed with attention to ideal propagation in free space. In a real environment, obstacles will appear in the propagation path which increases the propagation loss and hence reduces the range.

In contrast, the eavesdropping distance for the reader 1 with smaller size and lower field strength is only between

7.9 and 76.3 m. Except in the case of reader 1 in a business environment, the distances are in the far field where a coherent demodulation increases the range by about 40%.

3.2 Eavesdropping of uplink signal

For the analysis of the uplink signal, it is necessary to derive the load modulated current in the transponder antenna. Figure 9 shows the circuit diagram of the reader antenna coupled to the transponder.

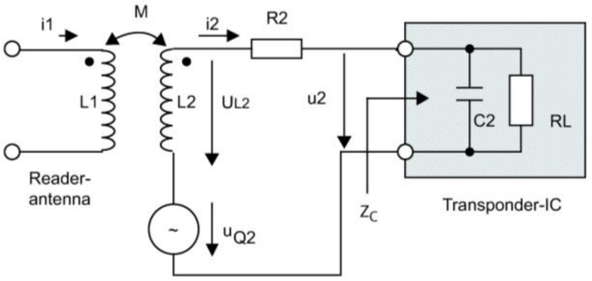

Figure 9: Circuit diagram of an inductively coupled reader transponder system [Fin12]

The inductance L_1 indicates the reader antenna, which is mutually coupled to the inductance L_2 of the transponder. The magnetic field of the reader antenna induces a voltage into the transponder inductance which is modelled by the voltage source u_{Q2}. The induced voltage u_{Q2} is proportional to the incident magnetic flux, which is normal to the plane of the loop. Assuming that the incident field is uniform over the loop area and normal to the loop plane, the induced voltage for an *N*-turn loop can be written as

$$u_{\mathrm{Q2}} = j\omega A N \mu_0 H_i. \tag{3.6}$$

The induced voltage drives a current i_2 which is modulated by the load of the transponder-IC R_L. According to the circuit diagram in Figure 9 the current i_2 can be written as

$$i_2 = \frac{\mathrm{u_{Q2}}}{Z_L + Z_C}, \tag{3.7}$$

where $Z_C$is the input impedance of the transponder-IC

$$Z_{\mathrm{C}} = \frac{\mathrm{R_L}}{j\omega C_2 R_L + 1} \tag{3.8}$$

and $Z_L$the impedance of the antenna coil

$$Z_{\mathrm{L}} = j\omega L_2 + R_2. \tag{3.9}$$

To calculate the loop current i_2 the component values for the loop antenna (R_2, L_2, A, N), the IC capacitance C_2, the load resistor R_L and the incident magnetic field H_i have to be known. Typically the antenna values are specified by the manufacturer or can be easily measured [Fin12]. The capacity C_2 of the transponder-IC is specified by the IC manufacturer. R_L results from the energy consumption of the chip and a parallel shunt resistor to keep the voltage at the chip almost at a constant level. Hence R_L has to be calculated for each value of the field strength H_i and each operational state (modulation resistor on and off). In our case, the value of the load resistor is calculated from the measured transponder-IC voltage u_2. The impedances Z_C and Z_L form a voltage divider and hence u_2 can be written as

$$u_2 = \frac{\mathrm{Z_C}}{Z_L + \mathrm{Z_C}} u_{\mathrm{Q2}}. \tag{3.10}$$

By inserting (3.8) and (3.9) and transforming the equation, the load resistor can be obtained as follows:

$$R_{\mathrm{L}} = \frac{u_2(\mathrm{R_2} + j\omega L_2)}{u_{\mathrm{Q2}} - u_2(1 + j\omega C_2 R_2 - \omega^2 L_2 C_2)} \tag{3.11}$$

To modulate the amplitude of the loop current i_2 and hence the magnetic field strength, the load resistor R_L is switched between two states and hence modulates the quality factor of the resonant circuit. A high load $R_{\mathrm{L,max}}$ creates a high loop current $i_{2,\mathrm{max}}$ while a low load $R_{\mathrm{L,min}}$ creates a low loop current $i_{2,\mathrm{min}}$. The amplitude variation of the loop current during load modulation is shown in Figure 10.

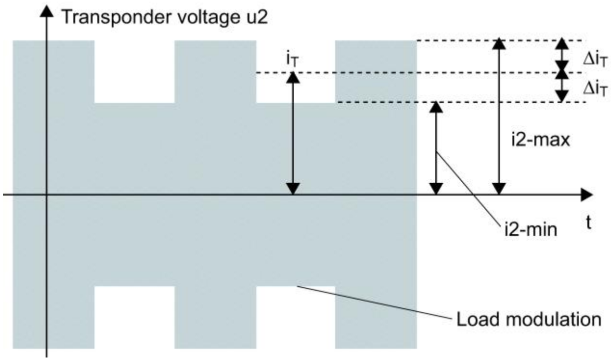

Figure 10: Amplitudes of the loop current due to load modulation [Fin12]

As mentioned before, it is sufficient to only detect one single sideband of the modulated 848 kHz subcarrier, where only parts of the total signal power are concentrated. For a rectangular amplitude modulated subcarrier with a modulation index of

$$m = \frac{|i_{2,\mathrm{max}}| - |i_{2,\mathrm{min}}|}{|i_{2,\mathrm{max}}| + |i_{2,\mathrm{min}}|}, \tag{3.12}$$

the power concentrated in one single sideband (upper or lower) is $^1/_2\, m^2$ times the carrier power level. Because of the characteristics of the Manchester code used for the downlink modulation, it has to be considered that the subcarrier is only applied to the signal half of the time (half the bit duration) and hence the sideband power is even lower.

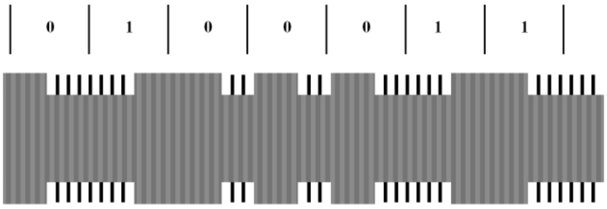

Figure 11: ISO/IEC1443 type A uplink signal [Fin08]

Considering this, the power level of each sideband normalized to the carrier power can be written as

$$\mathrm{A_{SB}} = \frac{P_{\mathrm{sideband}}}{P_{\mathrm{carrier}}} = \frac{1}{2\left(\left(\frac{1}{m}+1\right)^2 + \frac{1}{m^2}\right)}. \qquad (3.13)$$

Typically the modulation index is small enough to allow the following approximation of (3.13):

$$\mathrm{A_{SB}} \approx \frac{m^2}{4}, \text{for } m \ll 1 \qquad (3.14)$$

Now we are able to calculate the magnetic field strength of the upper side band at a distance r in dependence of the loop current i_2 and the coil parameters.

$$H_{\mathrm{USB}}[\mathrm{dB\mu A/m}] = 20\log\left(\frac{N\cdot\left|H(I_{\mathrm{L,carrier}}, a, \theta, r)\right|}{1\ \mathrm{\mu A/m}}\right) + A_{\mathrm{SB}}[\mathrm{dB}] \qquad (3.15)$$

$|H|$ is the absolute value of the complex magnetic carrier field strength given in (3.1) to (3.3) for a single loop. For small modulation indexes, the absolute value of the average complex 13.56 MHz carrier loop current can be approximated by

$$\left|I_{\mathrm{L,carrier}}\right| = \frac{\left|i_{2,\mathrm{max}}\right| + \left|i_{2,\mathrm{min}}\right|}{2}, \text{for } m \ll 1. \qquad (3.16)$$

At the maximum eavesdropping distance r_{max} the field strength H_{USB} is equal to the minimum required field strength $H_{\mathrm{Signal,min}}$.

$$H_{\mathrm{USB}}(r = r_{\mathrm{max}}) = H_{\mathrm{s,min}} \qquad (3.17)$$

As an example the maximum downlink eavesdropping distance of an exemplary transponder will be calculated. Table 6 shows the transponder parameters:

	Transponder 1
resonance frequency	15 MHz
coil resistance R_2	3 Ω
coil inductance L_2	4µH
IC capacitance C_2	28 pF
average coil area	68 mm x 38 mm
(equivalent coil radius a)	(29 mm)
Number of windings N	7

Table 6: Exemplary transponder values

The amplitude of the complex voltages u_2 for both modulation states are measured directly at the transponder chip using an oscilloscope. The measurements were carried out with a magnetic field strength of 1.5 and 4.5 A/m (rms) at the transponder location. Using (3.11) the high and low load resistor value can be calculated. The amplitude of the current i_2 can be derived with (3.7). Finally, (3.12) gives us the modulation index and (3.14) the single sideband power factor. Table 7 summarizes all results.

	Transponder 1	
H_i	1.5 A/m (rms)	4.5 A/m (rms)
$u_{2,\mathrm{max}}$	3.50 V (rms)	4.29 V (rms)
$u_{2,\mathrm{min}}$	1.48 V (rms)	2.98 V (rms)
$i_{2,\mathrm{max}}$	11.7 mA (rms)	27.4 mA (rms)
$i_{2,\mathrm{min}}$	9.1 mA (rms)	26.4 mA (rms)
$R_{L,\mathrm{max}}$	426 Ω	169 Ω
$R_{L,\mathrm{min}}$	175 Ω	117 Ω
m	12.3 %	1.9 %
A_{SB}	-24.2 dBc	-40.6 dBc

Table 7: Measured and calculated characteristic values for a magnetic incident field of 1.5 A/m (rms) and 4.5 A/m (rms) at 13.56 MHz

Considering equations (3.1) to (3.3), (3.15) and (3.16) the magnetic field strength of the USB signal can be calculated. It shows that the sideband power in the magnetic field strength decreases with increasing incident magnetic field, even though the coil current i_2 becomes bigger. This is due to the behaviour of the IC to nearly keep the IC-voltage constant by controlling the load R_L. A decreased R_L leads to a reduction of the modulation index and will reduce the sideband power.

Considering the magnetic noise field strength listed in Table 2 and the desired SNR value, the maximum range can be derived. As an example, Figure 12 shows the USB field strength in dependence of the distance and the required field levels as horizontal dotted lines for a BER of 0.01% and non-coherent demodulation.

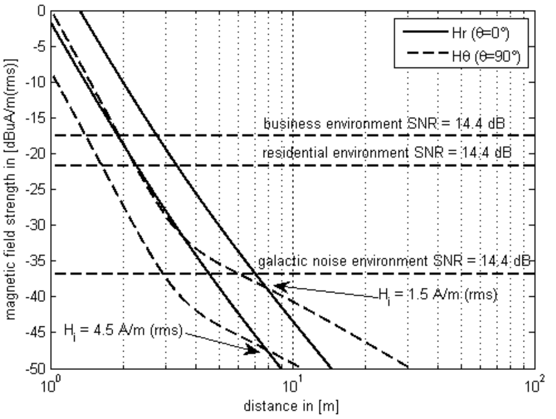

Figure 12: Eavesdropping distances for an ISO/IEC14443A uplink signal assuming different environments (business, residential and galactic noise) for non-coherent demodulation with a BER of 0.01%

Table 8 and Table 9 show the maximum eavesdropping ranges for the exemplary transponder assuming optimal antenna placement for a BER of 0.1% and 0.01%, respectively. For a range smaller than 8.3 m, the attacker's antenna should be oriented coaxial to the transponder's antenna. For larger distances, a coplanar orientation is appropriate.

$\boldsymbol{H_i}$ **demodulation**	**Business**	**Noise source** **Residential**	**Galactic**
1.5 A/m (rms)			
non-coherent	2.8 m	3.4 m	7.2 m
coherent	3.2 m	3.9 m	9.4 m
4.5 A/m (rms)			
non-coherent	2.0 m	2.4 m	4.7 m
coherent	2.2 m	2.7 m	5.5 m

Table 8: Maximum uplink eavesdropping range for different incident magnetic fields and environments calculated for a BER of 0.1%

$\boldsymbol{H_i}$ **demodulation**	**Business**	**Noise source** **Residential**	**Galactic**
1.5 A/m (rms)			
non-coherent	2.6 m	3.2 m	6.6 m
coherent	3.0 m	3.6 m	7.7 m
4.5 A/m (rms)			
non-coherent	1.8 m	2.2 m	4.4 m
coherent	2.1 m	2.5 m	5.1 m

Table 9: Maximum uplink eavesdropping range for different incident magnetic fields and environments calculated for a BER of 0.01%

For non-coherent demodulation with a BER of 0.01% and low incident magnetic field of 1.5 A/m (rms), the maximum eavesdropping range is between 2.6 for business and 3.2 m for residential noise environment. The absolute limit is 6.6 m in presence of galactic noise. With an incident magnetic field of 4.5 A/m (rms) the range reduces to 1.8 m and 2.2 m for business and residential environment, respectively. Therefore the absolute limit is 4.4 m. A coherent demodulator increases the range by approximately +15%. Comparing the results of Table 8 and Table 9, it shows that a reduction of the BER from 0.1% to 0.01% only slightly decreases the range (by less than 10%) as most of the ranges are still in the near field region.

It is important to us to point out again that the calculations were performed in a free space propagation model which differs from realistic situations. [The11] experimentally concludes that wirings, wall materials as reinforced concrete or metal framings of the doors could appear as antenna relays which could significantly increase the range.

4 Conclusion

In this paper we present a calculation of the theoretic possible eavesdropping range of an inductive coupled reader-transponder communication with passive load modulation. For the calculation we assume a receiver architecture with matched filter, un-coherent and coherent demodulation and a bit error rate of 0.1 and 0.01% for reliable detection. It is evident that the bottleneck of an eavesdropping attack is the ability to read the uplink communication (from the transponder to the reader). Considering an exemplary ISO/IEC14443 type A transponder-reader configuration and un-coherent demodulation the theoretical eavesdropping range lies between 2.6 m for a business and 6.6 m for a pure galactic noise environment assuming an incident magnetic field strength of 1.5 A/m (rms) at the transponder's location. A coherent demodulator could theoretically increase the range by approximately +15%. With a magnetic field strength of 4.5 A/m (rms) the range decreases to 1.8 and 4.4 m, respectively. This is due to the behaviour of the IC-transponder chip where the load resistance decreases with increasing incident field. As a result the sideband power which includes the signal information decreases with increasing incident field.

The derived theoretical limits show a good agreement with the published experimental results of 1 m to 3 m presented in [Fin04], [BSI08] and [Han08]. Only the results of [Nov08] with a maximum eavesdropping distance of 8 m to 15 m depending on transponder type are close to or even exceed the theoretical limits of a galactic noise environment. In contrast to our paper [Nov08] defines an SNR of 6 dB as sufficient for a reliable decoding. According to the theoretical BER curve in Figure 4, this would imply a bit error rate of about 2% assuming an optimum receiver for AWGN channels and coherent demodulation. Assuming an SNR of 6 dB in our calculations the theoretical eavesdropping distance increases to about 15 m in a galactic noise environment (assuming coherent demodulation and an incident field strength of 1.5 A/m (rms)). But without additional signal processing, such a low BER value is not even appropriate for a reliable error-free detection of a 4 byte long frame. One possibility to allow a lower SNR value is described in [Kfi05] for relay attacks. The authors propose that the transponder can be caused to retransmit each data frame multiple times. In this case the repeated bit sequence can be used for interleaving what will improve the detection. For relay attacks, the attacker itself can request several retransmissions for each frame, but in an eavesdropping scenario, every retransmission has to be caused by actively interfere the transmission of single bits. Without a direct connection to reader and/or transponder this is more difficult to realize.

Another reason for excessive range compared to our results may be due to coupling effects in surrounding metal objects (e.g. wires).

This shows that in order to obtain a real comparison between different results, it is important to be aware of the measurement conditions. Beside of the definition of a successful eavesdropping, the environmental conditions, the incident magnetic field strength at the transponder's location and the used transponder type can strongly affect the measured range.

Comparing our results for business and residential environment to the results of the theoretical study [NXP07] with 3.6 m and 4.2 m, respectively, it turns out that our results are slightly lower. In contrast to [NXP07], we use a full circuit model of the transponder to derive the loop current and calculate the magnetic field strength with the analytical model of a circular loop antenna. Additionally we assume a matched filter configuration with a lower signal bandwidth and also consider a lower BER of 0.01% (compared to only 0.1%) which is necessary for the detection of complete data frames. For the calculation of the absolute range limit [NXP07] uses the noise level of a quiet rural environment (according to [ERC99]) which is lower than the galactic noise level and hence is not an appropriate model for the noise floor. This explains the big difference of the maximum range of 7.2 m (for non-coherent demodulation and a BER of 0.1%) in our calculation compared to 38.6 m as stated in [NXP07].

In conclusion, it is important to emphasize that our calculations are performed under simplified assumptions like free space propagation and average noise levels. Therefore theoretical range limits can only give an indication for practical limits in a real world situation.

5 Literature

[Bal05] Balanis, C., A.: *Antenna Theory*. Third edition, Hoboken, New Jersey: John Wiley & Sons, Inc., 2005.

[Bia07] Bianchi, C.; Meloni, A.: *Natural and man-made terrestrial electromagnetic noise: an outlook*, Annals of Geophysics 3 / 50, June 2007.

[BSI08] Study of the Bundesamt für Sicherheit in der Informationstechnik (BSI): *Messung der Abstrahleigenschaften von RFID-Systemen* (MARS), Teilbericht 1, 2008.

[ERC99] European Radiocommunications Committee (ERC): *Propagation Model and Interference Range Calculation for Inductive Systems 10 kHz – 30 kHz.* ERC report 69, 1999.

[Fin04] Finke, T., Kelter; H.: *Radio Frequency Identification – Abhörmöglichkeit der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO 14443- Systems*, 2004.

[Fin11] Finkenzeller, K; Pfeiffer, F.; Biebl, E.: Range Extension of an ISO/IEC 14443 type A RFID System with Actively Emulation Load Modulation. RFID Systec 2011, Proceedings of, 2011.

[Fin12] Finkenzeller, K.: *RFID-Handbuch*. 6. edition, Carl-Hanser Verlag München, 2012.
http://rfid-handbook.com

[Fin08] Finkenzeller, K.: *RFID-Handbuch*. 5. edition, Carl-Hanser Verlag München, 2008.

[Han08] Hancke, G.: *Eavesdropping Attacks on High-Frequency RFID Token*, 2008.

[ISO08] ISO/IEC 14443-4:2008 (2nd edition). Identification cards - Contactless integrated circuit(s) cards - Proximity cards, Part 4: Transmission protocol, 2008.

[ISO10] ISO/IEC 14443-2:2010 (2nd edition). Identification cards - Contactless integrated circuit(s) cards - Proximity cards, Part 2: Radio frequency power and signal interference, 2010.

[Kfi05] Kfir, Z.; Wool, A.: *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems*, Cryptology ePrint Archive, Report 2005/052, 2005.

[Kir06] Kirschenbaum, I., Wool, A.: *How to Build a Low-Cost, Extended-Range RFID Skimmer*. 15th Usenix Security Symposium, pp. 43-57 of the Proceedings, 2006.

[NXP07] NXP. Application note AN200701: *ISO/IEC 14443 Eavesdropping and Activation Distance*. 2007.

[Nov08] Novotny, D.R.; Guerrieri, J.R.; Francis, M.; Remley, K.: *HF RFID electromagnetic emissions and performance*, Electromagnetic Compatibility, 2008. EMC 2008. IEEE International Symposium on, vol., no., pp.1-7, 18-22 Aug. 2008

[The11] Thevenon P.-H., Savry O., Tedjini S. and Malherbi-Martins R.: *Attacks on the HF Physical Layer of Contactless and RFID Systems*, Current Trends and Challenges in RFID, Cornel Turcu (Ed.), 2011.

[Poz08] Pozar, D.: *Microwave and RF Designa of Wireless Systems*. first edition, John Wiley & Sons, Inc.. New York, 2001.

About the authors

Florian Pfeiffer was born in Starnberg, Germany, in 1976. He received the Dipl.-Wirtsch.-Ing. (FH) degree in industrial engineering from the Fachhochschule München, Munich, Germany, in 2001, the Dipl.-Ing. and Dr.-Ing. degrees in electrical engineering from the Technische Universität München, Munich, Germany, in 2005 and 2010, respectively. In 2009, together with Erwin M. Biebl, he founded an engineering company for high frequency electronics (perisens GmbH), where he is chief executive.

Klaus Finkenzeller was born in Ingolstadt, Germany in 1962. He received his Dipl.-Ing. (FH) degree in electrical engineering from the Munich University of Applied Sciences (FH), Munich Germany. In 1989 he joined Giesecke & Devrient. Since 1994 he has been involved in the development of contactless smart cards and RIFD systems. He is currently working as a technology consultant for RFID/security, where he is involved in basic development and innovation projects.

Since 1994 he has been engaged in the standardisation of contactless smartcards and RFID Systems (DIN NI 17.8, NI 31.4, SC17/WG8), where he has been vice chair of the German DIN NI17.8 (ISO/IEC 14443) for more than 10 years now.

Up to now he has published more than 130 individual patent applications, mainly in the RFID field of technology.

In 1998 he published the RFID handbook, which now is available in its 6th edition and in 7 different languages. In 2008 Klaus Finkenzeller received the Fraunhofer SIT smartcard price for his work on RFID, especially the RFID handbook.

Erwin M. Biebl was born in Munich, Germany, in 1959. He received the Dipl.-Ing., Dr.-Ing., and Habilitation degrees from

the Technische Universität München, Munich, Germany, in 1986, 1990, and 1993, respectively. In 1986, he joined Rohde & Schwarz, Munich, Germany, where he was involved in the development of mobile radio communication test sets. In 1988, he was with the Lehrstuhl für Hochfrequenztechnik, Technische Universität München. In 1998, he became a Professor and Head of the Optical and Quasi-Optical Systems Group. Since 1999, he has been Head of the Fachgebiet Höchstfrequenztechnik, Technische Universität München. He has been engaged in research on optical communications, integrated optics, and computational electromagnetics. His current interests include quasi-optical measurement techniques, design and characterization of microwave and millimeter-wave devices and components, sensor and communication systems, and cooperative approaches to sensor and communication systems and networks. Dr. Biebl is a member of the Informationstechnische Gesellschaft (ITG) in the Verband Deutscher Elektrotechniker (VDE), Germany, a senior member of the IEEE and an appointed member of the commission B of URSI, Germany.