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

Maximilian Engelhardt*, Florian Pfeiffer†, Klaus Finkenzeller‡ and Erwin Biebl*
*Fachgebiet Höchstfrequenztechnik, Technischen Universität München, Arcisstr. 21, 80333 München
Email: maximilian.engelhardt@mytum.de, biebl@tum.de
†perisens GmbH, Landwehrstr. 61, 80336 München, Email: pfeiffer@perisens.de
‡Giesecke & Devrient GmbH, Prinzregentenstraße 159, 81607 München, Email: klaus.finkenzeller@gi-de.com

***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 show an approach, using higher-order harmonics to eavesdrop the data transmitted from a transponder to a RFID-reader (uplink). Practical distances for eavesdropping on higher-order harmonics are measured for exemplary ISO/IEC 14443 type A transponder and reader configurations in different environments.**

I. Introduction

Inductively coupled ISO/IEC 14443 compliant RFID systems are nowadays 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 maximum distance of about 10 cm. The short communication range of a smart card is also regarded as an important security feature. Extended range [1], skimming attacks [2] and eavesdropping are well known threats 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 unauthorised communication with a reader. Skimming is the unauthorised access of tag data without an authorised tag-reader connection. Eavesdropping is defined as unauthorised data access to an authorised reader-tag communication.

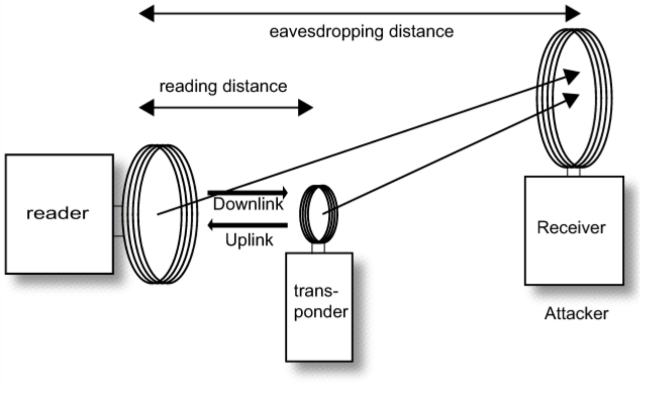

Fig. 1. Eavesdropping attack of a RFID communication [3]

In several studies eavesdropping attack scenarios have been analysed theoretically and experimentally. In [4] we have shown the theoretical limits of eavesdropping attacks, listening to the uplink (tag to reader) at the fundamental wave at 13.56 MHz of a contactless smart card, ID1 size. We resulted in an eavesdropping distance of between 2 m and approximately 10 m, depending on the tag type, the environmental noise figure and the field strength applied to the tag.

Looking at the analogue front end of a transponder however, one sees that the loop antenna is directly connected to a rectifier circuit in the RFID-chip, providing the power supply for the chip. This in the simplest case is done, using the strong nonlinear characteristic of diodes. As we know, any nonlinearity in an electronic component generally causes higher-order harmonics in the current, flowing through it. Therefore this higher-order components must also be a part of the current flowing through the transponder coil antenna connected to the rectifier, where they cause a magnetic field which finally gets radiated into the proximity of the transponder.

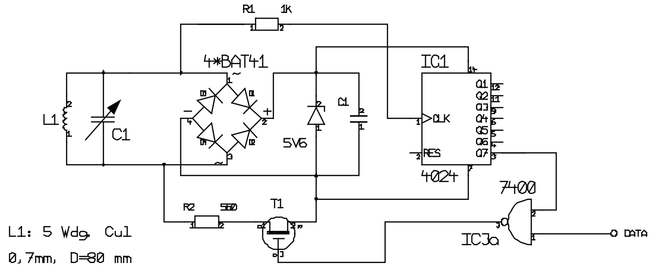

Fig. 2. Schematic of the power supply, voltage regulation and generation of load-modulation with a 848 kHz subcarrier of a RFID transponder circuit [3]

In this paper we focus on eavesdropping a transponder on the higher-order harmonics, generated by the nonlinear characteristic of the rectifier in the transponders analogue front end.

II. Advantage in Eavesdropping High-Order Harmonics

Receiving at higher frequencies offers several advantages:

A. Improved noise conditions

In the HF band the external noise with atmospheric, galactic and man-made noise is typically significantly greater than the internal receiver noise. [5] 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.

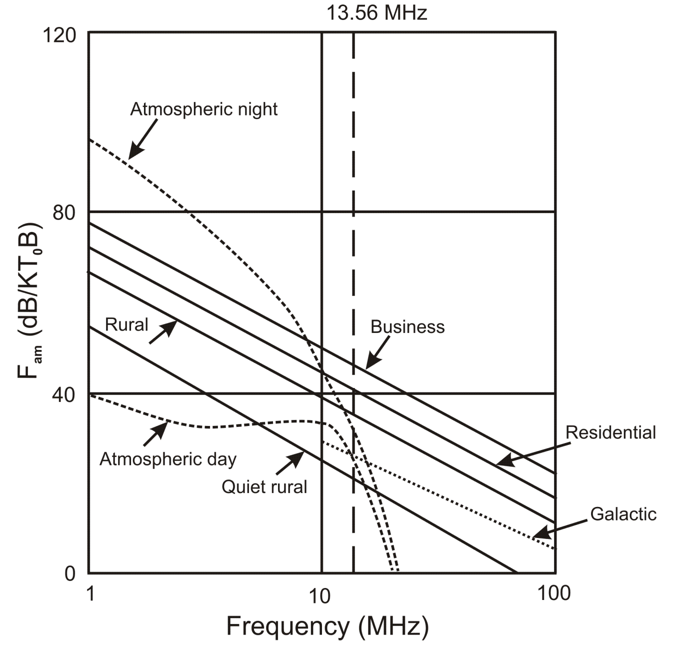

Fig. 3. Solid lines indicate median values of man-made noise in F_{am} (dB above thermal noise at 288 K), dashed lines indicate atmospheric noise and the dotted line shows the galactic background noise [6]

Between 10 and 100 MHz man-made noise is the predominant noise source in a business and residential environment which is the most critical environment for attack scenarios. In logarithmic scale the man-made noise decreases linearly with frequency. The noise factor F_{am} is defined according to [5] with

$$F_{\mathrm{am}} = c - d \log_{10}\left(\frac{f}{1\,\mathrm{MHz}}\right). \tag{1}$$

c and d are environment depending constants. The constant d determines the gradient of the noise figure curves. As we are interested in the harmonics of 13.56 MHz, the expression can be written as follows:

TABLE I. ENVIRONMENT DEPENDING CONSTANTS [5]

Noise source	Business	Residential	Galactic
c	76.8	72.5	52.0
d	27.7	27.7	23.0

$$F_{am} = c - d \log_{10}\left(n \cdot \frac{13.56\,\mathrm{MHz}}{1\,\mathrm{MHz}}\right) \tag{2}$$

$$F_{am} = c - d\left(\log_{10}(n) + 1.13\right) \tag{3}$$

In business and residential environment, the noise figure decreases by $27.7 \cdot \log_{10}(n)$ with the order n of the harmonic waves. Compared to the fundamental wave, the 3rd order harmonic wave has a noise level decreased by 13.2 dB, the 5th order harmonic wave by 19.4 dB.

Another advantage of higher frequency is the possibility to use directional antennas. Directional antennas with one major lobe and negligible minor lobes receive signals mainly from one direction. As consequence, the reception of interference can be reduced by aligning the maximum directivity of the antenna to the desired signal source.

B. Favourable propagation conditions

The most limiting factor of eavesdropping a magnetic near field communication is the strong decrease of the magnetic field strength. By eavesdropping at higher-order harmonic frequencies this factor could be overcome as the near to far field transition occurs at closer distance. Figure 4 shows the tangential and radial magnetic field strength of a small loop antenna in dependence of the distance at the fundamental frequency of 13.56 MHz.

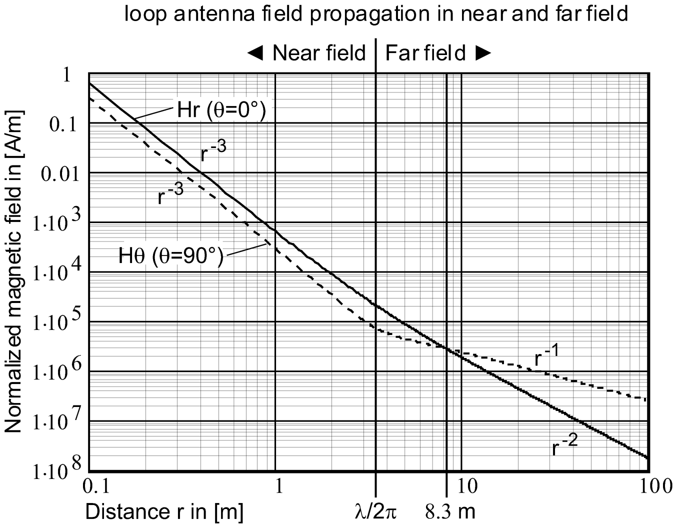

Fig. 4. Normalised tangential and radial magnetic field of a small loop antenna in dependence of the distance at 13.56 MHz [3]

At the near field to far field transition, the slope of the curve changes: For smaller distances, the magnetic field strength decreases with the inverse of distance to the power of three. For larger distances, it changes to a linear proportionality of the radial field. The location of the transition point is at $r = \frac{\lambda}{2\pi}$ and thus directly depends on the wavelength.

- In the near field with $r \ll \frac{\lambda}{2\pi}$: $H \propto r^{-3}$
- In the far field with $r \gg \frac{\lambda}{2\pi}$: $H \propto r^{-1}$

Therefore the location gets closer to the antenna with increasing frequency. The fundamental wave at 13.56 MHz has a near to far field boundary of 3.5 m, the 3rd order harmonic wave of 1.2 m and the 5th order harmonic wave of only 0.7 m. In most cases, the propagation conditions are more favourable in far field region, provided that there is a radiating element which transfers the near field energy into electromagnetic radiation. Wires on the electronic reader circuit or cables connected to the reader or placed near to the reader can act as radiating antennas.

III. Theory of High-Order Harmonics Generation

The high-order harmonics are generated due to the nonlinearities of the rectifier diodes. Typically, full-wave bridge rectifier circuits are used in smart cards. Such a commonly used circuit is shown in figure 5.

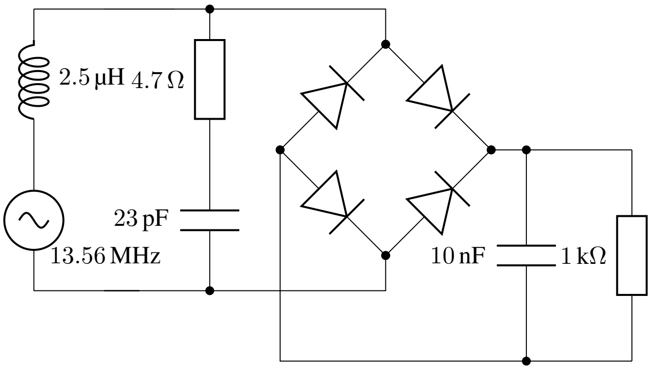

Fig. 5. Schematic circuit of a bridge rectifier in receiving mode

To produce a steady DC supply, a smoothing capacitor is used at the output. The rectifier's input is connected to the coil antenna of the smartcard which is put resonant using a capacitor. The resonant frequency is adjusted to 13.56 MHz.

To analyse the behaviour of the rectifier circuit, it is modelled using a Spice simulation tool. As diodes Schottky diodes are used. In Figure 6, the spectrum of the output voltage with the even harmonics of 13.56 MHz is shown.

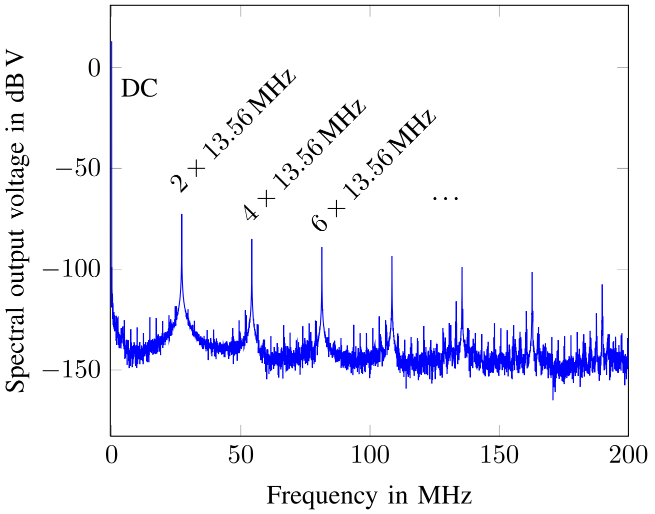

Fig. 6. Simulated frequency spectrum of voltage at the output of the bridge rectifier showing the even harmonics of 13.56 MHz

This result can easily be explained: A full wave rectifier with ideal diodes leaves the positive half cycle of an input sine unchanged and clips the negative half cycle. The ideal spectrum of such a rectified signal only consists of even harmonics of the sine wave frequency. However, at the input of the rectifier circuit the odd harmonics are produced. See figure 7 showing the simulated frequency spectrum of the coil current. Since the odd harmonics occur directly at the input of the smartcard circuit, there is a great risk of radiating especially these lower odd harmonics (3rd order harmonic at 40.68 MHz and 5th order at 67.8 MHz).

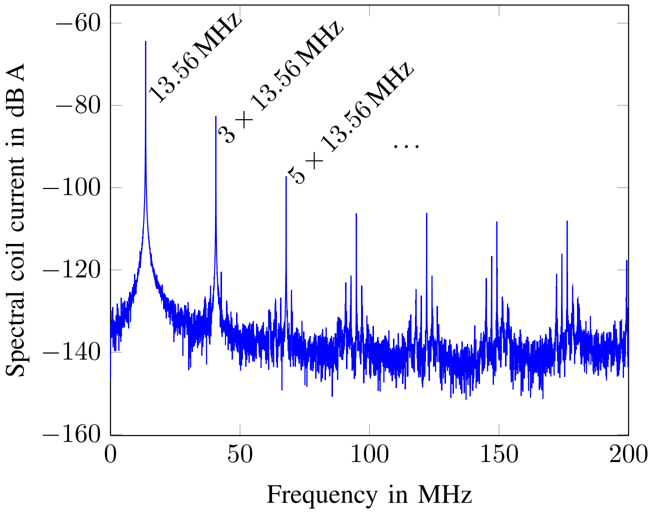

Fig. 7. Simulated frequency spectrum of coil current at the input of the bridge rectifier showing odd harmonics of 13.56 MHz

IV. 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 kbit/s. 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 (see figure 2).

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 maximises the SNR in presence of stochastic noise, while the synchronous detector with optimum threshold minimises the BER. For a binary ASK signal corrupted with additive white Gaussian noise (AWGN) the probability of bit errors reads as [7]

$$BER = \frac{1}{2}\,\mathrm{erfc}\left(\frac{1}{2}\sqrt{SNR_{BB}}\right), \tag{4}$$

where $\mathrm{SNR}_{\mathrm{BB}}$ 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

$$BER = \frac{1}{2}\,\mathrm{erfc}\left(\frac{1}{2}\sqrt{2SNR_{HF}}\right) \tag{5}$$

and for non-coherent demodulation

$$BER = \frac{1}{2}\,\mathrm{erfc}\left(\frac{1}{2}\sqrt{SNR_{HF}}\right). \tag{6}$$

Figure 8 shows the BER in dependence of the SNR for coherent and non-coherent demodulation.

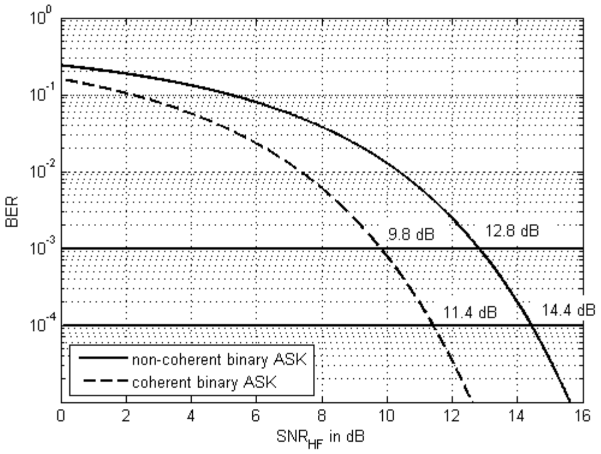

Fig. 8. Bit error rate in dependence of SNR for binary ASK signal corrupted with AWGN

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 generation of a random ID. 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 4096 bytes according to [8]. Assuming no 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:

$$1 - FER = (1 - BER)^{N} \tag{7}$$

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

According to Table II, a BER of 0.1 % - as used in [9] - is not sufficient for a reliable error-free detection of a 64 or 256 byte frame. Therefore, we also use 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.

TABLE II. PROBABILITY THAT A FRAME ARRIVES WITH NO BIT ERRORS (WITHOUT ANY ERROR-CORRECTION)

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 %

A BER of 0.1 % implies a minimum $\mathrm{SNR_{HF}}$ of 11.4 dB for coherent and 14.4 dB for non-coherent demodulation (see Figure 8). In our measurements we use an equivalent $\mathrm{SNR_{BB}}$ threshold of 14.4 dB for successful reception of the signal.

V. Near and Far Field Coupling of High-Order Harmonics

As proof of concept, initial field strength measurements are carried out in the near and far field.

1) Near field Measurements: To determine the power of the generated harmonics we performed near field measurements using a small coil located on the surface of the smart card while reading the smart card. Since the impedance of the coil is dependent on the frequency, we measured the inductivity of the coil and compensated the measured values accordingly.

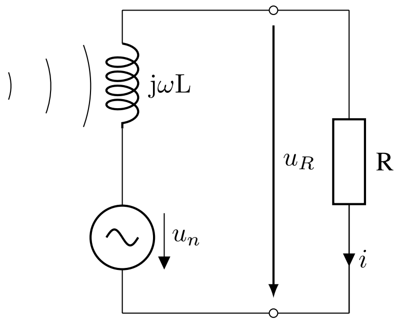

Fig. 9. Equivalent circuit of the measurement setup

Figure 9 shows the equivalent circuit of the measurement. R designates the 50 Ω input of the used spectrum analyser, jωL the inductivity of the coil and u_n the source voltage. Because the impedance grows with increasing frequency, u_R will decrease with constant source voltage. With this equivalent circuit one can easily derive equation 8.

$$u_n = u_R \frac{\mathrm{R} + \mathrm{j}\omega\mathrm{L}}{\mathrm{R}} \tag{8}$$

For all our measurements we used a Mifare pegoda CL RD 701 reader from NXP and a 1K Mifare transponder card from Philips. The reader was connected to a laptop with the supplied 2 m long USB cable. Reader and laptop were placed at roughly the same distance so that the USB cable was about parallel to the ground.

Table III shows the power of the harmonics after compensating the effect of the coil. According to the simulated results in chapter III, the odd harmonics are noticeably stronger than the even harmonics. The 3rd order harmonic is the strongest with 23 dB below the fundamental wave.

TABLE III. COMPARISON OF THE GENERATED HARMONICS

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

2) Far field Measurements: An crucial property for eavesdropping higher order harmonics is the radiation of those into the far field. As the signal of the transponder is the limiting factor for eavesdropping an ISO/IEC 14443 Type A RFID communication [4], we conducted measurements at the frequency of the upper side band of the transponder at different order harmonics.

In our measurements the Pegoda reader was connected to the laptop using a USB cable. The laptop was placed at a height of 0.5 m above ground, in a distance of about 2 m to the reader. The reader is about 1 m above ground. The complete setup is shown in figure 10.

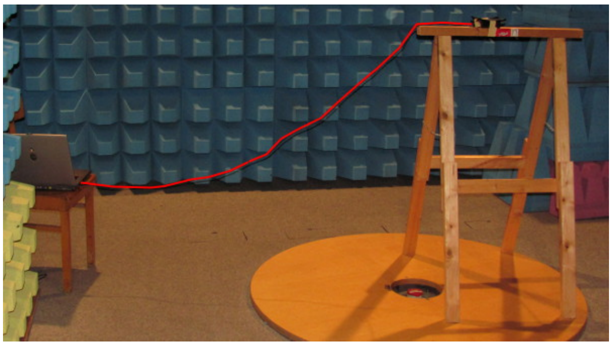

Fig. 10. Reader connected to a laptop via USB cable which acted as antenna (marked in red) in the EMC chamber

It turned out that the field of the higher harmonic frequencies coupled to the USB cable and the cable acted as antenna. The best results could be achieved when the transponder card was placed eccentrically on the reader. Figure 11 shows the setup we used in our measurements. In case of locating the transponder card centrally to the reader, nearly no radiation occurred.

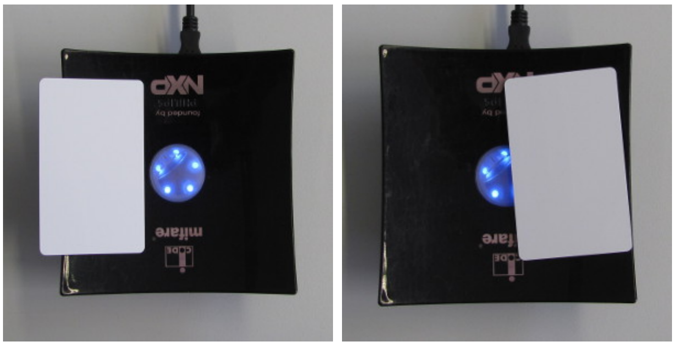

Fig. 11. Exemplary positions of the transponder card on the reader for radiation of higher order harmonics into the far field

Table IV shows the measured electrical field strength of the harmonics at a distance of about 2.3 m from the reader. The highest field strength could be measured at the 3rd and 7th order harmonics. As the spectrum of the 7th order harmonic lies in the FM broadcasting radio band and the signal at the 3rd order harmonic was stronger we decided to use this frequency for our further analysis.

TABLE IV. MEASURED ELECTRIC FIELD STRENGTH OF THE RADIATED HARMONICS AT THE UPPER SIDE BAND OF THE CARD SIGNAL

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

VI. EAVESDROPPING OF 3RD ORDER HARMONIC

We conducted measurements at different locations with different measurement equipment. As the limiting factor for eavesdropping an ISO/IEC 14443 type A communication is the uplink signal we concentrated our analysis only on this signal. Since the mixing products at the harmonics carry the spectrum of both, the reader and transponder communication, extracting the reader data is not much additional effort.

For our evaluation we made measurements in an experimental hall with a combined biconical and a log-periodic antenna from Rohde und Schwarz (HL562 ULTRALOG) as well as in a long corridor using a much smaller SB 30-88-MU1 shortened quarter wavelength antenna from Procom. Both locations are at the Technische Universität München. We intentionally wanted to perform measurements in an normal environment to simulate realistic eavesdropping attacks.

The measurements in the experimental hall were realised using a signal and spectrum analyser from Rohde und Schwarz. For the measurements in the corridor we used a self-developed receiver hardware consisting of a low noise amplifier, bandpass filter and a coherent receiver. The bandpass filter was tuned to the upper side band of the transponder signal at the 3rd order harmonic, the receiver used a low cost TDA2542 IC for demodulation the upper side band signal at 41.5275 MHz. The IQ baseband signal at the output of the receiver was quantised and sampled for further digital processing using an oscilloscope. Together with the much smaller antenna used in our measurement this setup is a more realistic example for an eavesdropping attack. Figure 12 shows the measurement setup at the corridor.

Figure 13 displays the result of the measurements as $\mathrm{SNR}_{\mathrm{BB}}$ after matched filtering over distance. For comparison we also performed measurements at the fundamental wave. The measurements in the experimental hall were done for horizontal polarisation, in the corridor we measured horizontal and vertical polarisation. During the measurements we only captured the raw signal. Additional filtering and SNR calculation was done later in the digital domain.

For a threshold value of 14.4 dB, as it is necessary for bit error rates smaller 0.01 %, we achieved a maximal eavesdropping distance of 2.4 m at the fundamental wave. In contrast at the 3rd order harmonic we were able to receive signals in as far as 18 m above this threshold. Noticeable are the SNR variations in the region up to 15 m for the measurements in the corridor

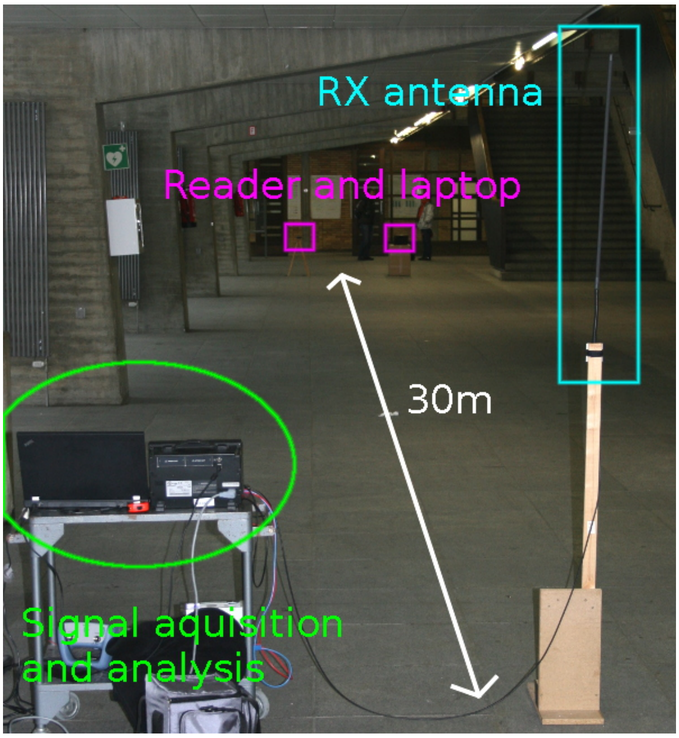

Fig. 12. Measurement setup in the corridor. The laptop and reader can be seen in the background, in the foreground are the receiving antenna and the reception hardware.

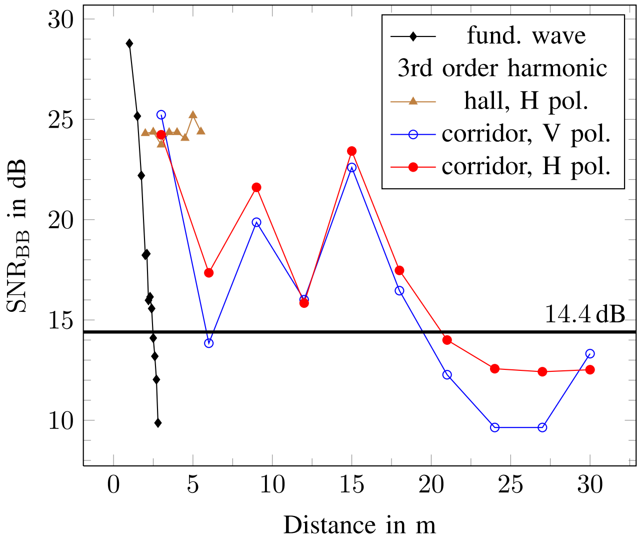

Fig. 13. Measured SNR versus antenna-reader distance for the fundamental wave and the 3rd order harmonic. Measurement in the hall using horizontal polarisation and in the corridor for vertical and horizontal polarisation.

in both polarisations. We explain this due to interference by multipath propagation of the signal.

To rule out problems with only a specific transponder card we additionally conducted some tests with different transponder cards but achieved roughly the same results. In our case the radiation of the 3rd harmonic occurred through the USB cable connecting the reader to the laptop. After adding a snap-on ferrite core to the USB cable at the readers side, we were no longer able to receive any usable signal.

VII. Conclusion

Using higher harmonics for eavesdropping has obvious advantages compared to eavesdropping at the fundamental wave. In HF band the noise level decreases with increasing frequencies and the near to far field transistion is getting closer to the antenna. In the far field, the field strength decreases only linearly with distance compared to the inverse of distance to the power of three in the near field.

In this paper, we explain how higher order harmonics are generated in a smartcard and how radiation can occur. We conducted measurements at the 3rd order harmonic for a exemplary ISO/IEC 14443 type A communication in different locations and achieved a maximal eavesdropping distance of 18 m. This is much higher than the distances published at the fundamental wave. Table V gives an overview over different published theoretical and experimental eavesdropping distances at the fundamental wave compared to our results.

TABLE V. Comparison of our results to other publications, ✏: theoretical, ➼: practical, ✕: coupling?

	current Publications	eavesdropping distance	comment
		Fundamental wave	
➼	Finke (2004) [10]	2 m	
➼	BSI (2008) [11]	2.3 m	reading ID
➼	Hanke (2008) [12]	1–3 m (different locations)	reading ID
➼✕	Novotny (2008) [13]	8–15 m (different cards)	reading ID
✏	NXP (2007) [9]	2.4–38.6 m (different locations)	BER < 0.1 %
✏	Pfeiffer (2012) [4]	2.1–7.7 m (different locations)	BER < 0.01 %
➼	Our results	2.2–2.4 m (different locations)	BER < 0.01 %
		3rd order harmonic	
➼	Our results	18 m	BER < 0.01 %

Comparing the experimental studies, only the results of [13] with up to 15 m are close to our results at the 3rd harmonic. All other measurements - our own included - show maximum eavesdropping ranges between 1 m and 3 m at the fundamental wave. Therefore, we assume coupling effects (e.g. in wires) as reason for the excessive range of [13]. The phenomenon of coupling effects at the fundamental wave are mentioned in [14].

In contrast to the fundamental wave, there is no system antenna at the higher harmonics frequency. Therefore radiation is only possible if coupling to surrounding metal objects (e.g. cables, wires) which act as antennas occur. In our measurements, the USB cable between reader and laptop acted as antenna. The intensity of radiation depended on the location of the transponder on the reader. The best results could be achieved with an eccentrically position on the reader. By using a simple snap-on ferrite at the reader's side of the USB cable a sufficient suppression of the radiation could be achieved.

To avoid possible eavesdropping attacks with high ranges at higher harmonics, measures are needed to minimise harmonic generation or at least to prevent coupling to possible surrounding metal objects which can act as antennas. Typically bridge rectifiers are used in transponders to provide the power supply. At the input of these rectifiers, odd harmonics are generated and directly transformed in a magnetic field at the transponder coil. Therefore, there is a large risk that the magnetic field of the higher harmonics couples through the reader circuit to a surrounding "antenna" where the energy is transfered into the far field. The harmonic generation has to be suppressed at the bridge rectifier of the transponder card. At the reader's side, the RF path to a surrounding "antenna" can be interrupted. This can be achieved, for example, by ferrite based isolators at connected cables or harmonic filters at critical spots in the reader circuit. In critical cases, on-side spectrum measurements might be useful as coupling strongly depends on the surrounding.

REFERENCES

[1] K. Finkenzeller, F. Pfeiffer, and E. Biebl, “Range extension of an ISO/IEC 14443 type A RFID system with actively emulating load modulation,” *RFID SysTech 2011; 7th European Workshop on Smart Objects: Systems, Technologies and Applications; Proceedings of*, pp. 1–10, may 2011.

[2] I. Kirschenbaum and A. Wool, “How to build a low-cost, extended-range RFID skimmer,” in *15th Usenix Security Symposium*, 2006, pp. 43–57.

[3] K. Finkenzeller, *RFID-Handbuch*, 6th ed. München: Hanser, 2012, http://rfid-handbook.com.

[4] F. Pfeiffer, K. Finkenzeller, and E. Biebl, “Theoretical limits of ISO/IEC 14443 type A RFID eavesdropping attacks,” in *Smart SysTech 2012 - European Conference on Smart Objects, Systems and Technologies*, 2012.

[5] European Radiocommunications Committee (ERC), “Propagation model and interference range calculation for inductive systems 10 kHz – 30 MHz,” *ERC report 69*, 1999.

[6] C. Bianchi and A. Meloni, “Natural and man-made terrestrial electromagnetic noise: an outlook,” *Annals of Geophysics*, vol. 50, no. 3, June 2007.

[7] D. M. Pozar, *Microwave and RF Design of Wireless Systems*. New York [u.a.]: Wiley, 2001.

[8] “ISO/IEC 14443-4:2008 (2nd edition). identification cards - contactless integrated circuit(s) cards - proximity cards, part 4: Transmission protocol,” 2008.

[9] “Application note AN200701: ISO/IEC 14443 eavesdropping and activation distance,” NXP, 2007.

[10] T. Finke and H. Kelter, “Radio frequency identification (RFID) – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO 14443-Systems,” Bundesamt für Sicherheit in der Informationstechnik, 2004.

[11] “Messung der Abstrahleigenschaften von RFID-Systemen (MARS), Teilbericht 1,” Bundesamt für Sicherheit in der Informationstechnik, 2008.

[12] G. Hancke, “Eavesdropping attacks on high-frequency RFID tokens,” in *4th Workshop on RFID Security (RFIDSec)*, 2008.

[13] D. Novotny, J. Guerrieri, M. Francis, and K. Remley, “HF RFID electromagnetic emissions and performance,” in *Electromagnetic Compatibility, 2008. EMC 2008. IEEE International Symposium on*, aug. 2008, pp. 1–7.

[14] P.-H. Thevenon, O. Savry, S. Tedjini, and R. Malherbi-Martins, “Attacks on the HF physical layer of contactless and RFID systems,” in *Current Trends and Challenges in RFID*. Cornel Turcu (Ed.), 2011.

ABOUT THE AUTHORS

Maximilian Engelhardt was born in Karlsruhe, Germany, in 1986. He is currently studying electrical engineering at the Technische Universität München, Munich, Germany. In 2012 he wrote his Bachelor Thesis at the Fachgebiet Höchstfrequenztechnik. He is now working towards completing his Diploma degree.

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 NI 17.8 (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.