Radio Frequency Identification
–
Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems

Thomas Finke, Harald Kelter

Kurzfassung:
Das Abhören der Kommunikation zwischen Lesegerät und RFID-Tag ist eine der spezifischsten Bedrohungen der kontaktlosen Technologie. Da die Kommunikation handelsüblicher Tags häufig entweder im 125 kHz- oder im 13,56 MHz-Bereich abläuft, ist das Abhören grundsätzlich mit einfachen Mitteln möglich. Häufig wird hier argumentiert, dass normkonforme RFID-Systeme lediglich Abstände von 10 bis 15 cm (ISO 14443) oder maximal 1,5 m (ISO 15693) als typische Arbeitsabstände zulassen. Vergessen wird jedoch, dass dies lediglich die aktive Kommunikation betrifft. Die bei den genannten Normen verwendeten Feldstärken geben Anlass zu der Vermutung, dass das passive Abhören der Kommunikation noch in mehreren Metern Entfernung möglich ist. Der in diesem Artikel beschriebene Messaufbau wurde zur Verifikation dieser Vermutung verwendet.

Stichworte:
RFID-System, Transponder, Tag, Abhören, ISO 14443, Feldstärken, Reichweite

Was sind RFIDs ?

Die zunehmende Verbreitung der Radio Frequency Identification – Technologie findet weitestgehend unsichtbar statt. Allenfalls in Warensicherungsettiketten werden die einfachsten Formen dieser leistungsfähigen Technik vom Verbraucher wahrgenommen. Hierbei kommen 1-bit-Transponder zum Einsatz, die unter Ausnutzung physikalischer Effekte ausschließlich eine Ja/Nein-Information speichern und nicht explizit beschreibbar bzw. programmierbar sind. Darüber hinausgehend existiert jedoch eine Vielzahl weiterer Produkte. Diese besitzen oft deutlich mehr Funktionalitäten als einfache Artikelsicherungssysteme. Es handelt sich um leistungsfähige Identifikations- und Datenerfassungssystem mit kontaktloser Datenübermittlung auf Basis der Radiofrequenztechnologie. Anwendung findet diese Technik zur Zeit hauptsächlich in den Bereichen

- Industrieautomation,
- Zutrittssysteme,
- Tieridentifikation,
- Warenmanagement und
- bei Elektronischen Wegfahrsperren.

Für den praktischen Einsatz verwendet man sogenannte RFID-Systeme. Ein RFID-System besteht dabei immer aus einem Transponder, der die zu speichernden und bei Bedarf zu übermittelnden Informationen enthält, einem Schreibgerät zur Programmierung und dem Schreiben von Identifikationsdaten auf den Transponder sowie einem Lesegerät, das die im Transponder enthaltenen Informationen ausliest.

RFID-Systeme gibt es in den unterschiedlichsten Ausführungen. Für ein mögliches Klassifizierungsschema wird im Allgemeinen von einer Aufteilung in die Bereiche

- Versorgungsart,
- „Intelligenz“ bzw. Rechenleistung,
- Speicherkapazität und
- Reichweite
- ausgegangen.

Im Folgenden werden die Begriffe RFID-Chip, RF-Chip, Chip, RFID-Tag, Tag, RFID-Label und Label synonym verwendet, da sich noch kein einheitlicher Sprachgebrauch durchgesetzt hat.

Grundsätzliche Funktionsweise

Lässt man sogenannte aktive RFID-Tags, die über eine eigene Spannungsversorgung verfügen, außer acht, funktionieren alle herkömmlichen RF-Chips nach dem gleichen Prinzip:

Ein Lesegerät generiert ein magnetisches Wechselfeld, das über seine Induktionswirkung im Antennenkreis des Tags eine Spannung induziert. Diese elektrische Spannung dient der Versorgung der auf dem Tag vorhandenen Steuerlogik. Dabei kann es sich um eine einfache „verdrahtete“ Logik (ein Zustandsautomat) handeln oder eine leistungsfähige Prozessoreinheit incl. verschiedener Co-Prozessoren für Spezialaufgaben wie das Berechnen elektronischer Signaturen.

Hat der RFID-Chip erkannt, dass er sich im Feld eines Lesegerätes befindet, sendet er seine Seriennummer durch die Modulation des angelegten magnetischen Wechselfeldes an das Lesegerät. Dieses kann nun den Chip selektieren (schließlich könnten sich mehrere RF-Tags im Lesefeld befinden) und mit der Kommunikation beginnen.

Leistungsfähigkeit

Welche Operationen ein RF-Chip ausführen, kann hängt von vielen Faktoren ab. Einer dieser Faktoren wurde eben bereits eingeführt: die zur Verfügung stehende Rechenleistung. Moderne RF-Chips können in dieser Hinsicht heute durchaus mit kontaktbehafteten Smartcards konkurrieren und besitzen Prozessoreinheiten

mit Taktfrequenzen zwischen 1 MHz und 15 MHz sowie leistungsstarke, meist für die Realisierung kryptographischer Funktionen vorgesehene Co-Prozessoren.

Auch die Speicherkapazität von RFID-Chips, vor allem in ihrer Ausprägung als Dual-Interface-Smartcard, steigt stetig. Während im Bereich der Logistik und der Zutrittskontrolle zur Zeit noch Systeme eingesetzt werden, die nur wenige Kilobit durch den Nutzer beschreibbaren Speicher zur Verfügung stellen, sind 32 Kilobyte nichtflüchtiger Speicher für Dual-Interface-Karten keine Seltenheit mehr. Einige Kartenhersteller haben sich sogar die Realisierung von 1 Megabyte-Speichern zum Ziel gesetzt.

Oft diskutiert wird die Reichweite von RFID-Systemen. Gemeint ist hiermit der Abstand zwischen Lesegerät und RFID-Tag. Dieser beträgt unabhängig von der sonstigen Leistungsfähigkeit des Chips zwischen wenigen Zentimetern (Proximity Coupling) und etwas mehr als einem Meter (Vicinity Coupling). Eine Steigerung dieser Reichweiten durch Erhöhung der Sendeleistung des Lesegerätes ist nur bedingt möglich, da das Tag auch bei einer hohen Sendeleistung nicht unbedingt in die Lage versetzt wird, das Feld für den Leser verständlich zu modulieren.

Relevante Normen

Die International Organization for Standardization (ISO) hat mehrere Normen für den Bereich der RFID-Technik verabschiedet. Dies sind die unter anderem die Normen

- ISO 10536 (Close Coupling),
- ISO 14443 (Proximity Coupling),
- ISO 15693 (Vicinity Coupling) und
- ISO 18092 (Near Field Communication).

Während die ISO 10536 wegen der mangelnden Verbreitung der Close-Coupling-Technologie (Reichweite von ca. 1 cm und deshalb meist nur als Einstecklösung realisiert) heute nahezu keine Bedeutung mehr besitzt, ist vor allem im Bereich der Zutrittskontrolle und der Smart Labels die ISO 14443 häufig anzutreffen. Diese Norm spezifiziert neben der verwendeten Kopplungs- und Modulationsart für die Kommunikation zwischen Tag und Lesegerät auch elementare Funktionalitäten wie das zu verwendende Übertragungsprotokoll, die möglichen Übertragungsgeschwindigkeiten sowie Arbeitsreichweiten.

Nahezu identisch zur ISO 14443 ist von der Struktur her die Norm ISO 15693. Auch hier werden neben den physikalischen Eigenschaften der Übertragungstechnik die logischen Abläufe für die Kommunikation spezifiziert.

Unterschiedlich sind jedoch die spezifizierten Werte: Während ISO 14443-konforme Systeme Arbeitsreichweiten bis zu 15 cm aufweisen und dabei Daten-

raten von 424 kBit/s realisieren, sind ISO15693-konforme Systeme für Arbeitsabstände von bis zu 1,5 m bei einer Übertragungsrate von 26,48 kBit/s ausgelegt.

Beiden Normen ist die Arbeitsfrequenz von 13,56 MHz gemein.

Ebenfalls innerhalb dieses Frequenzbands werden RFID-Systeme aktiv sein, die sich an der recht neuen Norm für Near Field Communication (NFC) orientieren. Der NFC-Standard, hauptsächlich durch die Firmen Sony und Philips vorangetrieben, sieht ebenfalls Übertragungsraten von 424 kbit/s im Bereich des Proximity Couplings vor und soll kompatibel zu ISO 14443-Systemen werden.

Risiken des RFID-Einsatzes

In den vorhergehenden Abschnitten wurde die Funktionsweise von RFID-Systemen beschrieben. Klar wurde dabei, dass sich vor allem im Bereich der leistungsfähigeren RFIDs die Technologie der klassischen kontaktbehafteten Smartcards fast nicht mehr von der RFID-Technologie unterscheidet. Dementsprechend richten sich spezifische Bedrohungen fast immer gegen die Kommunikationsverbindung zwischen Leser und Tag. Die folgenden Abschnitte beschreiben kurz die Möglichkeit des Abhörens von RFID-Kommunikation.

Grundsätzliches zum Abhören der Kommunikation

Offensichtlich ist das Abhören der Kommunikation zwischen Lesegerät und RFID-Tag eine der spezifischsten Bedrohungen der kontaktlosen Technologie. Da die Kommunikation handelsüblicher Tags entweder im 125 kHz- oder im 13,56 MHz-Bereich abläuft, ist das Abhören grundsätzlich mit einfachen Mitteln möglich. Die im Standard ISO 14443 definierte Funkschnittstelle, als Frequenz werden die eben aufgeführten 13,56 MHz verwendet, liegt bspw. im Kurzwellenband und ist somit prinzipiell mit handelsüblichen Breitband- oder Weltempfängern empfangbar.

Häufig wird hier argumentiert, dass normkonforme RFID-Systeme lediglich Abstände von 10 bis 15 cm (ISO 14443) oder maximal 1,5 m (ISO 15693) als typische Arbeitsabstände zulassen. Vergessen wird jedoch, dass dies lediglich die aktive Kommunikation betrifft. Die bei den genannten Normen verwendeten Feldstärken geben Anlass zu der Vermutung, dass das passive Abhören der Kommunikation noch in mehreren Metern Entfernung möglich ist. Der im Folgenden beschriebene Messaufbau wurde zur Verifikation dieser Vermutung verwendet.

Meßaufbau

Neben den Daten überträgt das Lesegerät auch die zum Betrieb erforderliche Energie induktiv auf die Karte. Leser und Karte verfügen über großflächige Spulen mit mehreren Windungen, die Frequenz des Magnetfeldes beträgt beim un-

tersuchten System 13,56 MHz. Die Datenübertragung vom Leser zur Karte erfolgt durch Amplitudentastung, d. h. das Magnetfeld wird entsprechend den zu sendenden Daten ein- und ausgeschaltet, wobei die Daten derart codiert sind, dass das Magnetfeld jeweils nur sehr kurzzeitig ausgeschaltet wird, um die Energieversorgung der Karte sicherzustellen.

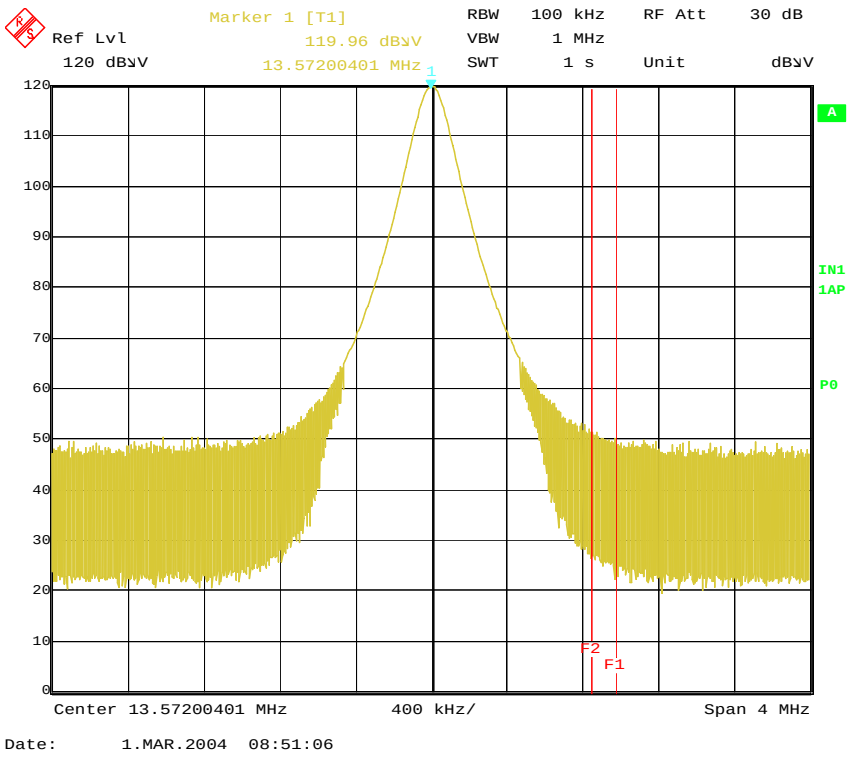

Bild 1: Träger des Lesegerätes ohne Modulation

Die Datenübertragung in umgekehrter Richtung erfolgt durch Lastmodulation, ein Lastwiderstand wird im Takt der zu übertragenden Daten geschaltet. Da Sende- und Empfangsspule wie ein Transformator gekoppelt sind, bewirkt dies eine Amplitudenmodulation des Signals in der Sendespule. Da die Kopplung aber sehr lose ist, liegt das Modulationssignal 60 bis 80 dB unter dem Trägersignal [FINK1998]. Zur sichereren Auswertung erzeugt die Karte daher einen Hilfsträger mit der Frequenz von 847 kHz um die Frequenz der Leseantenne und moduliert ihm die Daten auf. Der Empfänger des Lesegerätes wird dann auf ein Seitenband eines der Hilfsträger abgestimmt.

Mit der Testkarte aus [FINK2002] wurde die Auswirkung der Lastmodulation auf das HF-Feld des Lesers untersucht. Deutlich sind die Hilfsträger zu erkennen. Die Spule der Testkarte besteht aus 4 Windungen in den üblichen Abmessungen, die Lastmodulation geschieht durch einen im Takt der Daten geschalteten 1kOhm Widerstand.

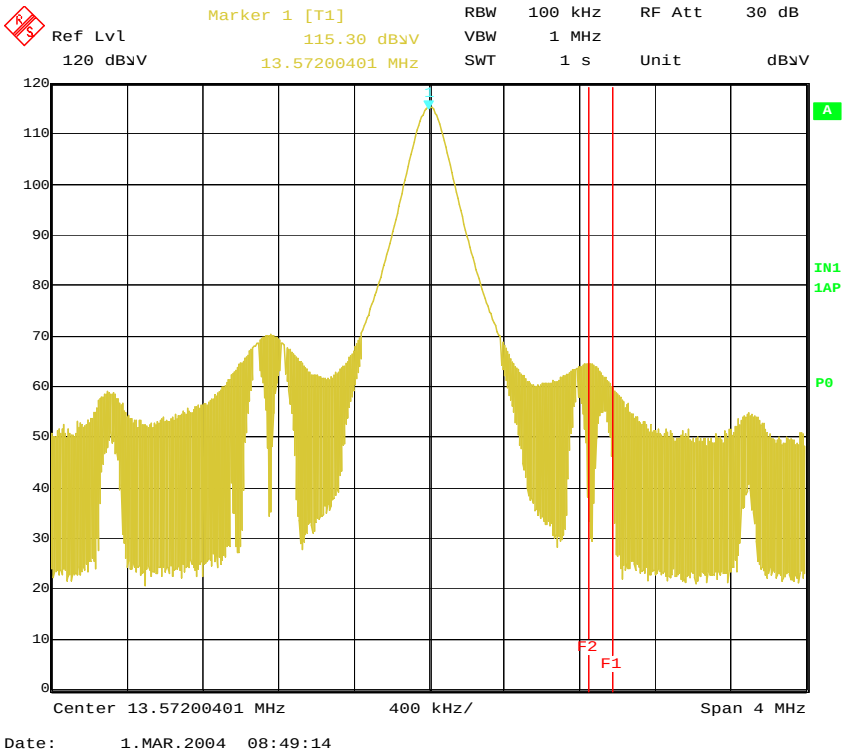

Bild 2: Hilfsträger, Karte sendet konstante ‚1'-Folge

Abhören der Kommunikation

Der Testaufbau wurde unter normalen Umgebungsbedingungen, außerhalb einer Meßkabine aufgebaut (Bild 3). Als Antenne dient eine magnetische Loopantenne für den Frequenzbereich bis 30MHz, Leser und Antenne befinden sich in einer Ebene, ein gegenseitiges Verdrehen verschlechtert die Ergebnisse stark. Die Karte liegt direkt auf dem Leser auf.

Der Empfänger (ESI) wurde auf 14,54MHz abgestimmt (F1 in Bild 2), die Empfängerbandbreite beträgt 300kHz. Das Ausgangssignal wird von einem Speicheroszilloskop aufgezeichnet.

Bild 3: Versuchsaufbau

Während der Messung führt die Testsoftware „MiFareWND“ die Funktion „HighLevel Read“ aus, dabei wird in einer Schleife ständig eine bestimmte Adresse der Speicherkarte ausgelesen. Der erste Versuch fand bei einem Abstand von 1m zwischen Kartenleser und Antenne statt, es ergibt sich ein empfangenes Signal nach Bild 4.

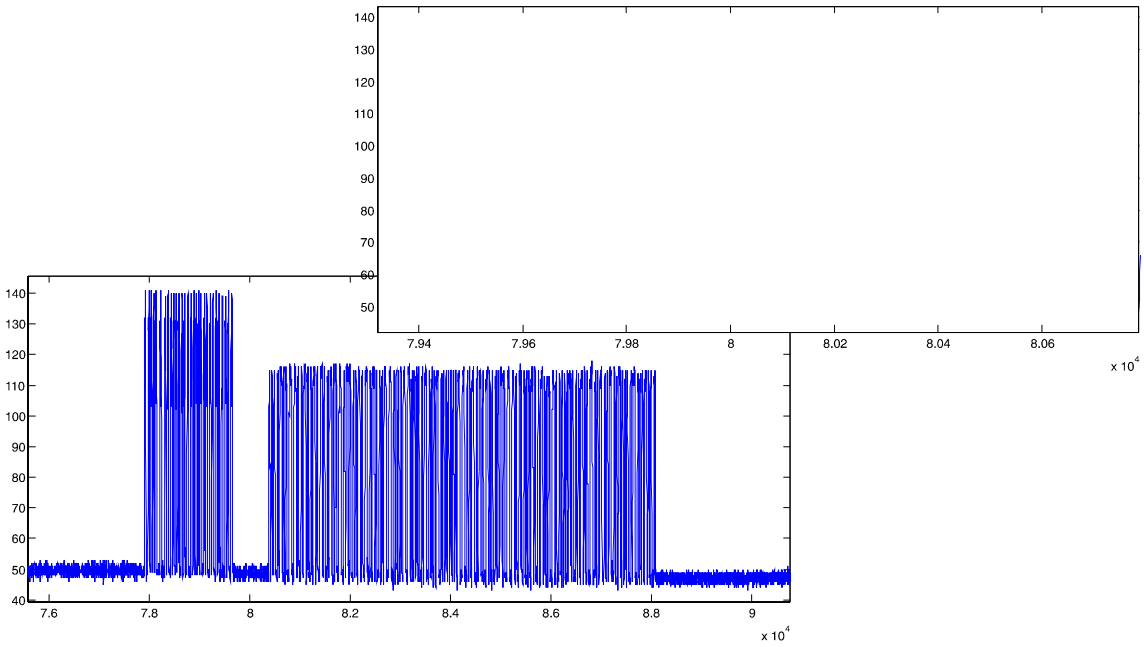

Bild 4: Datentelegramm bei 1m Abstand

Deutlich zu erkennen sind die Bitströme von Sender und Empfänger. Die annähernd gleiche Amplitude von Sende- und Empfangssignal ist dadurch zu begründen, daß bei der Abstimmung auf den Hilfsträger nur noch Oberwellen des Sendesignals empfangen werden. Der Sender verwendet offensichtlich einen Code, bei dem das HF-Feld abhängig von den Daten jeweils kurz ausgetastet wird (Laut Literatur [RAEF1999] soll es sich um eine ‚Millercodierung’ handeln, hierbei ergab sich jedoch ein Widerspruch). Die Karte antwortet in Übereinstimmung mit der Literatur in einer Manchester-Codierung. Stellt man mehrere Telegramme übereinander dar, ergibt sich eine Kommunikation nach Bild 5:

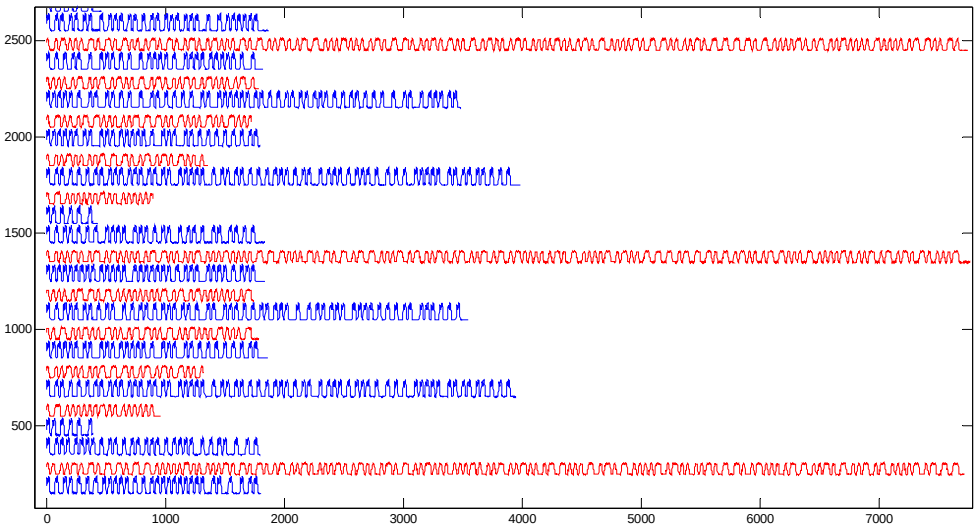

Bild 5: Kommunikation zwischen Leser und Karte (blau: Leser, rot: Karte)

Deutlich zu erkennen ist der stets gleiche Rahmenaufbau eines Schleifendurchlaufes, die tatsächlich ausgetauschten Daten unterscheiden sich allerdings von mal zu mal.

Die folgenden Bilder (6 und 7) zeigen die Verschlechterung des Signals mit zunehmender Entfernung zwischen Antenne und Leser.

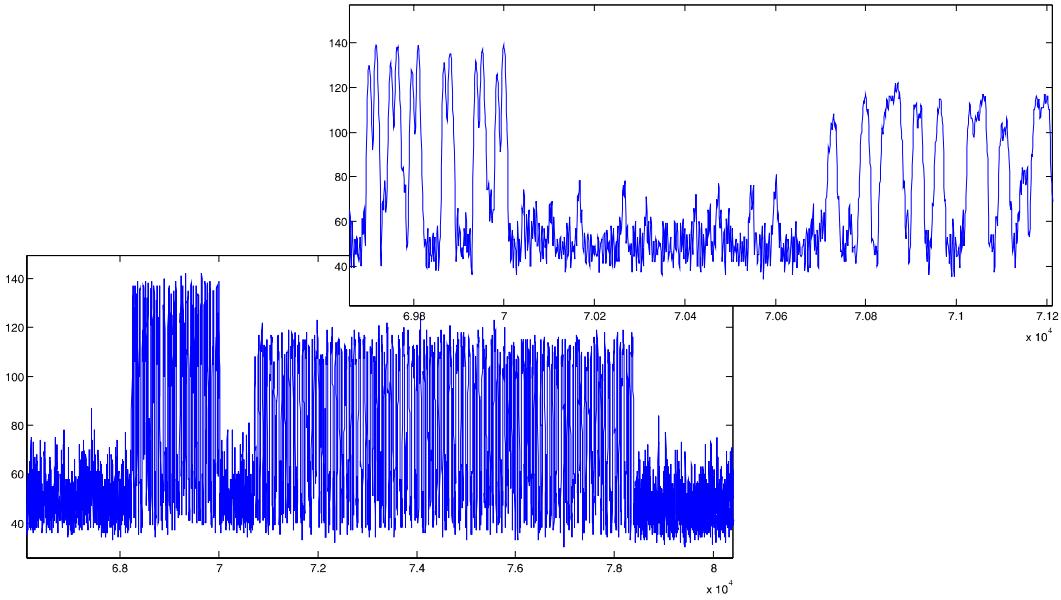

Bild 6: Datentelegramm bei 2m Abstand

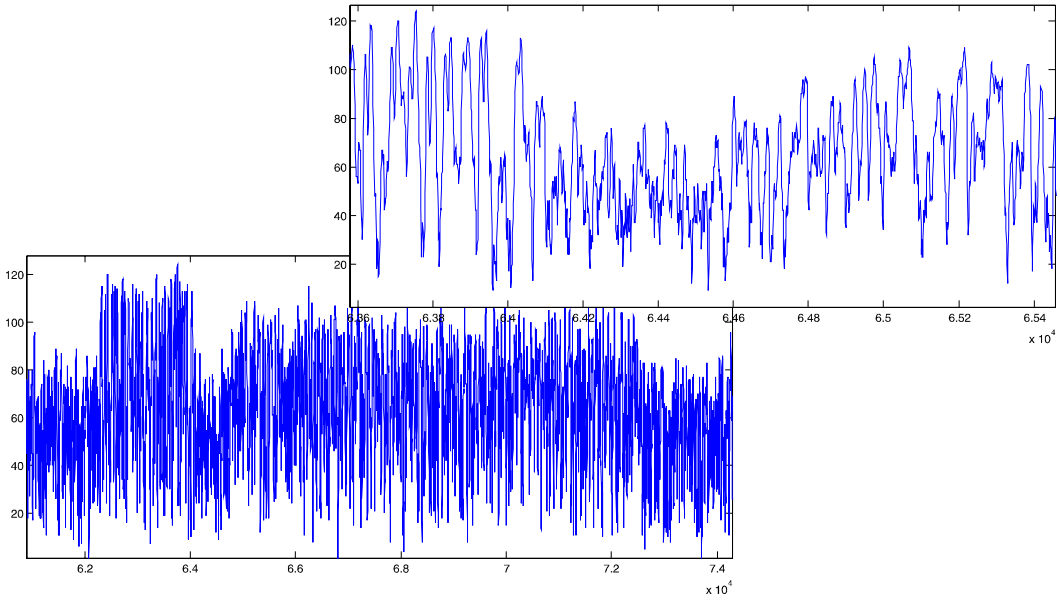

Bild 7: Datentelegramm bei 3m Abstand

In 2m Abstand läßt sich die Kommunikation noch ohne weiteres mitlesen, ab 3m kann man zwar noch deutlich die Telegramme ausmachen, ein bitgenaues Mitlesen dürfte aber bei *einer* Messung nicht möglich sein.

Fazit

Ein Abhören der Kommunikation von RFID-Karten nach ISO 14443 ist weit über den spezifizierten Arbeitsbereich von 10 – 15cm hinaus möglich. Mit den hier beschriebenen einfachen Labormitteln waren mehrere Meter zu überbrücken. In weiteren, noch durchzuführenden Untersuchungen soll festgestellt werden, wie weit sich diese Reichweite etwa durch abgestimmte Antennen, Vorverstärker usw. verbessern läßt.

Literatur

[DuD_0604] Kelter, H., Wittmann, S., RFID – Radio Frequency Identification, Chancen und Risiken des RFID-Einsatzes

[FINK1998] Klaus Finkenzeller, Kontaktlose Chipkarten, Funkschau 1998

[FINK2002] Finkenzeller, K., RFID-Handbuch – Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten, 3. Auflage, Carl Hanser Verlag, München, 2002

[HE1_2004] Just, C., Near Field Communication: Helfer-Funk für Mobilgeräte, Heise-Online, 29.03.2004, verfügbar unter http://www.heise.de/newsticker/meldung/46084

[HE2_2004] RFID-Störsender für Hacker und Verbraucher, 25.02.2004, Heise-Online, verfügbar unter http://www.heise.de/newsticker/meldung/45009

[RAEF1999] Rankel, W., Effing, W., Handbuch der Chipkarten, 3. Auflage, Carl Hanser Verlag, München, Wien, 1999