hochschule für angewandte wissenschaften
FACHBEREICH ELEKTROTECHNIK UND INFORMATIK hamburg
university of applied sciences

Kurze Zusammenfassung des Vortrages:

RFID

Eine kleine Einführung in Technik und Anwendung
UND
Die Einsatzmöglichkeiten in unserem Ferienclub

Martin Stein
2005

Einleitung

Am 20. April 2005 wurde im Rahmen der AW1-Vorlesung ein Vortrag von Martin Stein zum Thema RFID gehalten. Diese hier vorliegende Kurzzusammenfassung dieses Vortrages ist in Kombination mit dem Foliensatz zu diesem Vortrag zu lesen. Der Inhalt richtet sich primär an die Teilnehmer des Master-Projektes im kommenden Wintersemester 2005/2006.

Eine der Technologien, die im Rahmen des Master-Projektes zum Einsatz kommen sollen, ist RFID. Die Abkürzung RFID steht für „Radio Frequency Identification“, was auf Deutsch soviel wie Funkerkennung heißt. Diese Namensgebung bringt jedoch nur einen einzelnen, wenn auch wichtigen Aspekt dieser Technologie zum Ausdruck. Einsatzmöglichkeiten der RFID-Technologie, die auch über das eindeutige Erkennen von Objekten hinausgehen, werden später in diesem Vortrag angesprochen. Zuvor soll jedoch erstmal ein kurzer Blick auf die physikalisch-technische Seite von RFID geworfen werden.

Die physikalisch-technische Seite von RFID

Die Grundidee hinter der RFID-Technologie ist es, Siliziumchips zur Speicherung von Daten zu haben, welche ihre Daten kontaktlos zu einem Lesegerät übertragen können. Zudem sollen diese Datenspeicher möglichst ohne eigene Energiequellen wie Batterien oder Netzteile auskommen können. Stattdessen soll die Energie, die zum Betrieb des elektronischen Datenträgers benötigt wird, ebenfalls kontaktlos durch das jeweils zugreifende Lesegerät bereitgestellt werden. Darüber hinaus sollen die aufkommenden Hardwarekosten für die kabellose Datenschnittstelle zwischen RFID-Lesegerät und RFID-Transponder soweit wie möglich auf Seiten des RFID-Lesegerätes liegen, um die Kosten für die RFID-Transponder möglichst gering zu halten. Die typischen RFID-Transponder, welche auch Tags ([tɛk, tæg], Plural: [tɛks, tægz]) genannt werden, kann man sich als eine Art kontaktlose Smartcards vorstellen, welche durch ihre Datenübertragung per Funk einem gegenüber den herkömmlichen Smartcards drastisch reduziertem Verschleiß unterliegen. Zudem bietet diese Funkübertragung entgegen kontaktbehafteter Smartcard- oder auch optischen Barcode-Verfahren den großen Vorteil einer demgegenüber deutlich reduzierten Abfertigungszeit, da ein Einstecken oder Ausrichten für das Lesegerät entfällt.

Der prinzipielle Aufbau der Kommunikationsschnittstelle zwischen RFID-Lesegerät und RFID-Transponder ist in der Abbildung „Prinzip der Datenübertragung über Lastmodulation“ zu sehen ([EP01], Folie 3). Bei der Lastmodulation[1] sind die Antennenspule des Lesegeräts und die Antennenspule des RFID-Tags wie ein Transformator induktiv gekoppelt. Der resonante RFID-Tag entzieht dem magnetischen Wechselfeld der Lesegerätantenne Energie. Durch das Ein- und Ausschalten eines Lastwiderstandes an der Antenne des RFID-Tags, kann die entzogene Energie verändert werden. Je nach entzogener Energie stellt sich an der Antenne des Lesegerätes eine andere Spannung ein. Durch eine Amplitudenmodulation der Spannung in der Antenne des Lesegeräts kann so die Information, die der RFID-Tag zum Lesegerät senden möchte, transportiert werden.

Neben den sogenannten passiven Tags – das sind die RFID-Transponder, welche keinerlei eigene Stromversorgung besitzen und ihre gesamte Energie aus dem Feld, welches das

[1] An dieser Stelle soll nur grob das Verfahren der amplitudenmodelierten Lastmodulation angedeutet werden. Um ein erstes Verständnis für die RFID-Technik zu bekommen, sollte dieser vereinfachte Blick auf die elektrotechnische Seite reichen. Dem interessierten Leser sei an dieser Stelle jedoch wärmstens die Lektüre des RFID-Handbuchs (ISBN 3446220712) von Klaus Finkenzeller empfohlen.

Lesegerät erzeugt, beziehen – gibt es auch noch die aktiven Tags. Diese werden durch das Feld des Lesegerätes nur aus einem energiesparenden Tiefschlaf geweckt, um dann anschließend mit Hilfe einer Batterie mit dem Lesegerät zu kommunizieren. Nach dem Ende der Kommunikation fallen diese aktiven Transponder wieder in ihren Tiefschlaf zurück. Zurzeit sind aktive Transponder die einzige Möglichkeit RFID-Systeme mit Reichweiten von deutlich über zwei Metern aufzubauen. Doch es bleibt die Hoffnung, dass die Nanotechnologie in (womöglich) absehbarer Zeit elektronische Schaltungen hervorbringen kann, welche nur noch einen Bruchteil der heute nötigen Energie erfordern wird. Dadurch erwartet man einen beträchtlichen Sprung für die Reichweiten von passiven Systemen (siehe Folie 5). Zudem erhofft man sich durch diesen nanotechnologischen Ansatz, zukünftig auch den Einzelpreis für einfache RFID-Tags auf deutlich unter fünf Cent drücken zu können. Eine weitere und wohl bereits in näherer Zukunft greifbare Möglichkeit der Preisreduzierung bei der Produktion der einzelnen Tags verspricht man sich durch einen anderen nanotechnologischen Ansatz. Bei dieser zweiten Variante sollen die elektronischen Schaltkreise der RFID-Tags quasi „gedruckt“ werden. Diese sogenannten Polymerchips, sollen um einiges günstiger als ihre Vorfahren aus Silizium werden. Ob diese gedruckten Schaltungen auch eine Reichweitenerhöhnung durch geringeren Leistungsverbrauch möglich machen, bleibt abzuwarten.

Eine Besonderheit der RFID-Technik ist die sogenannte Pulkerfassung. Hierbei kann sich eine große Anzahl von RFID-Tags gleichzeitig im Lesebereich eines Lesegerätes befinden und das Lesegerät ist dennoch in der Lage, jedes von ihnen einzeln zu erfassen. Hierbei zu beachten ist, dass RFID-Tags normalerweise beim Betreten eines HF-Lesegerätsfeldes sofort anfangen ihre ID auszusenden, damit das Lesegerät überhaupt wissen kann, dass sich ein Tag mit einer bestimmten ID im Lesebereich befindet. Aus diesem Grund müssen zur Pulkerfassung Antikollisionsverfahren zur Anwendung kommen, welche dafür sorgen, dass sich die RFID-Tags nicht gegenseitig stören (siehe Folie 17). Nun folgend sind zwei typische Verfahren kurz aufgeführt:

„Slotted Aloha“ kommt zum Einsatz, wenn sich nur wenige RFID-Tags gleichzeitig in Lesegerätreichweite befinden. Bei diesem Verfahren stehen den RFID-Tags mehrere Timeslots zur Aussendung ihrer ID zur Verfügung. Jeder Tag in Reichweite wählt sich nun zufällig einen dieser Slots aus und sendet in diesem seine ID aus. Wenn in einem der Slots nur ein Tag seine Adresse aussendet, hat das Lesegerät diesen Tag erkannt. Daraufhin schickt ihm das Lesegerät einen adressierten Befehl, mit welchem dem Tag gesagt wird, dass er nun erstmal nicht mehr seine Adresse aussenden soll. Das Aussenden der IDs in den einzelnen Timeslots wiederholt sich nun so lange, bis alle Tags erkannt und stummgeschaltet sind.

Das zweite hier nur kurz vorgestellte Verfahren basiert auf einem „Binärer Suchbaum“. Dieses Verfahren hat den Vorteil, dass es immer funktioniert, egal wie viele Tags sich in Reichweite befinden. Der Nachteil ist jedoch, dass es langsamer ist als „Slotted Aloha“. Bei diesem zweiten Verfahren senden die Tags nun nicht mehr „ungefragt“ ihre ID einfach los, stattdessen sendet das Lesegerät einen adressierten Befehl aus, der besagt, dass der angesprochene Tag seine ID (=Adresse) aussenden soll. Da das Lesegerät ja noch nicht die Adresse kennen kann, schickt es zusammen mit dem adressierten Befehl eine Bitmaske aus, welche besagt, welche von den Adressbits von den Tags ausgewertet werden sollen. Wenn sich nun mehrere Tags gleichzeitig angesprochen fühlen, kommt es bei der Antwort zur Kollision und das Lesegerät muss die Bitmaske anpassen. So tastet sich das Lesegerät langsam an die richtige Adresse heran, so dass es zu einer bitgenauen Kollisionserkennung kommt. Wenn nun irgendwann ein einzelnes Tag selektiert werden konnte, wird diesem ein

adressierter Befehl zum Stummschalten geschickt und die Suche nach den übrig gebliebenen Adressen wird fortgesetzt.

Eindeutige Identifizierung

Die Anwendungsbereiche für RFID sind vielfältig. In Handel- und Logistik-Bereich erhofft man sich weit reichende Optimierungsmöglichkeiten in der Warenlogistik. Das heute eingesetzte EAN-Strichcode-Systems gibt zum Beispiel nur an, dass es sich bei dem vorliegenden Produkt um ein Tiefkühlhuhn der Firma X handelt. Ob das Suppenhuhn vielleicht kurz vor seinem Haltbarkeitsdatum steht oder gar schon darüber hinaus ist, kann durch das Strichcode-System nicht ermittelt werden. RFID soll dieses Problem lösen, indem jedes einzelne Produkt (in diesem Beispiel also jedes einzelne Huhn) seine eigene ID bekommt. Um das Haltbarkeitsdatum zu speichern, soll das RFID-Tag diese Information jedoch nicht in sich selber speichern. Dazu wäre nämlich zusätzlicher Speicherplatz in den Tags nötig, die höhere Kosten für die einzelnen Tags zur Folge hätten. Um das Haltbarkeitsdatums zu speichern, soll diese Information unter Verwendung der eindeutigen ID des Artikels in einer externen Datenbank abgelegt werden. Der Vorteil für diese Vorgehen ist ganz klar, dass auf diese Weise quasi beliebig viele Informationen zu einem Produkt abgelegt werden können – ganz unabhängig davon, was vielleicht ein RFID-Tag an Speicherkapazität haben würde.

Die Eigenschaft, mit RFID-Tags markierte Objekte eindeutig wieder erkennen zu können, macht man sich auch in vielen Anwendungen zunutze, wo eine Person durch den Besitz eines Gegenstandes (RFID-Tag) authentifiziert werden soll. So wird RFID zum Beispiel bereits heute in vielen Zugangssicherungssystemen (Türschlössern) eingesetzt (siehe Folie 6).

Datenspeicherung in den RFID-Tags

Anders als nur eine eindeutige Identifizierung von Objekten durch die einzigartige Seriennummer der RFID-Tags zu ermöglichen, können viele Tags auch weitere Informationen direkt in sich speichern und so zum Beispiel ortsabhängige Informationen enthalten. So sind in den Eurobalisen der Bahn die jeweiligen Streckenkilometer und viele weitere wichtige Informationen elektronisch direkt auslesbar, ohne dass man mit Hilfe eines weiteren Kommunikationskanals auf eine entfernt gelegene Datenbank zurückgreifen müsste (siehe Abbildung [P09], Folie 7).

RFID-Sichtungen als Trigger

Ein weiterer interessanter Einsatzzweck für RFID ist auch, dass die Sichtung eines RFID-Tags bestimmte Aktionen auslösen kann. So ist es denkbar, dass ein Mobiltelefon, welches mit einem RFID-Lesegerät ausgestattet ist, automatisch anbieten würde, eine Telefonnummer, die in einem Tag gespeichert ist, anzurufen, wenn man das Telefon direkt an diesen RFID-Tag halten würde. Ein etwas konkreteres Beispiel hierfür ist in der Vortragsfolie Nummer 10 zu sehen. Dort wird vorgeschlagen, ein RFID-Tag an einem Versicherungsvertrag zu befestigen, sodass ein RFID-Mobiltelefon automatisch eine Verbindung zu dem zuständigen Sachbearbeiter aufbauen kann. Denkbar wäre auch, dass das Telefon auch gleich die Policennummer automatisch an den Sachbearbeiter übermittelt würde.

RFID als kostengünstiges Dateninterface

Ein anderer Anwendungsbereich für RFID ist der „Missbrauch“ der Technik als kostengünstiges und kabelloses Dateninterface (siehe Folie 9). Man könnte sich heute zu vielerlei Gerätschaften im Niedrigstpreissegment kaum vorstellen, dass es sich kosten-/nutzentechnisch irgendwie rentieren könnte, ein Dateninterface in diese einzubauen. So besitzen beispielsweise viele Menschen einen kleinen und billigen 2 Euro Taschenrechner, den sie immer wieder mal für kleine Berechnungen benutzten. Kein Hersteller solcher Billigtaschenrechner würde auf die Idee kommen, ab Werk ein kostspieliges Dateninterface, wie eine Bluetooth-Schnittstelle in solches 2 Euro Produkt einzubauen. Die Mehrkosten, welche auf den Kunden umgelegt werden müssten, wären nicht damit zu rechtfertigen, dass der Benutzer nun ab und zu mal das Ergebnis des Tasschenrechner nicht mehr in den PC abtippen müsste, sondern dann direkt in dessen Zwischenablage kopieren könnte. Wenn man jedoch als Hersteller solcher Taschenrechner die Möglichkeit hat, ein RFID-Transponder-Interface für nur wenige Cent in so ein „Billigprodukt“ einzubauen, könnte dieser schon eher geneigt sein, dem Kunden so ein Zusatz-Gimmick anzubieten. Viele weitere derartige Möglichkeiten sind denkbar. In einem Fall solch einer kreativen Umnutzung des RFID-Systems zu einem Dateninterface hat man sich sogar entschlossen, einen ganz eigenen Namen dafür zu kreieren: Es handelt sich dabei um die Near Field Communication – kurz NFC. Verwendung findet die NFC beispielsweise in einem Pilotprojekt des Rhein-Main-Verkehrsverbundes in Kooperation mit Nokia und Philips bei dem NFC-Mobiltelefone zum „Handy Ticketing“ eingesetzt werden.

Das klassische Tracking

Nun kommen wir aber wieder zurück zur ursprünglichen Idee, die hinter RFID steht: Der automatischen elektronischen Identifizierung von Objekten – und zwar der eindeutigen Identifizierung! Einen besonders großen Nutzen aus RFID, erhofft man sich in der Warenlogistik, in welcher verschiedene Ausprägungen von RFID-Objekt-Tracking-Systemen zum Einsatz kommen sollen. RFID-Objekt-Tracking-Systeme sind Systeme, die dafür gedacht sind, Objekte in ihrer Ortslage zu verfolgen, um anschließend aus diesen gewonnenen Daten zu bestimmen, wie der weitere Lebensweg der getrackten und anderer Objekte verlaufen soll. Hierbei werden die zu verfolgenden Gegenstände mit RFID-Transpondern ausgestattet. Beim „klassischen“ RFID-Tracking werden an strategisch sinnvoll festgelegten Wegpunkten, an denen das Passieren von RFID-Transpondern überwacht werden soll, Lesegeräte aufgestellt (siehe Folie 11). Die Anzahl der Lesegeräte ist sowohl abhängig von der Größe und der räumlichen Aufteilung der „Welt“ in der sich die zu trackenden Objekte bewegen sollen, als auch von der benötigten Positionsabschätzungsgenauigkeit.

„mobiles RFID-Tracking“

Ein ganz anderer Ansatz als beim „klassischen RFID-Tracking“ wird beim „mobilen RFID-Tracking“ verfolgt (siehe Folie 12). Hier wird angenommen, dass die Positionsveränderungen der zu trackenden Objekte von einer Person ausgeführt werden, welche ein RFID-Lesegerät bei sich trägt. Damit das Tracking automatisch ablaufen kann, wird für das mobile Lesegerät zudem noch ein Positionsbestimmungsverfahren benötigt.

„verteiltes mobiles RFID-Tracking“

Gegenüber dem einfachen „mobilen RFID-Tracking“ dürfen beim „verteilten mobilen RFID-Tracking“ mehrere Personen die zu trackenden Objekte in ihrer Position beeinflussen (siehe Folie 16). Die Anzahl der Lesegeräte ist abhängig von der Anzahl dieser Personen. Eine Möglichkeit der Weitergabe von erhobenen Trackinginformationen wäre zum Beispiel, dass sich Lesegeräte beim direkten aneinander Vorbeigehen gegenseitig darüber informieren, wer die jüngeren Sichtungen von einzelnen Objekten gespeichert hat, um sich daraufhin gegenseitig zu aktualisieren.

Sicherheitsprobleme

Nun folgend werden einzelne ausgewählte Sicherheitsprobleme mit RFID-Systemen aufgeführt (siehe Folie 18). Zum einen ist da das allgemeine Problem der fehlenden Anonymität von RFID-Tags. Die Adresse des Tags ist immer auch gleich dessen ID, sodass jeder diese weltweit eindeutige ID auslesen kann. Zudem ist es bei einer Vielzahl von RFID-Systemen problemlos möglich die Kommunikation zwischen RFID-Tag und Lesegerät abzuhören, da meist auf Kryptographie verzichtet wird, da für diese viel elektrische Energie notwenig wäre, was bei passiven Tags eine drastische Reichweitenverminderung zur Folge hätte und bei aktiven Tags die Lebenszeit stark verkürzen würde. Ein Problem, unter dem vor allem Systeme zu leiden haben, welche auf Authentifikation durch Besitz basieren, ist der „Repeater-Angriff“. Hierbei wird ausgenutzt, dass zwischen Lesegerät und RFID-Tag kein mechanischer Kontakt besteht und die gesamte Kommunikation per Funk erfolgt. Die systembedingte geringe Reichweite zwischen Tag und Lesegerät wird nun mittels Repeatern heimlich verlängert, sodass sich das zur Authentifikation hergenommene Tag überhaupt nicht in der Nähe des Lesegerätes befinden muss.

Mein Angebot an den Ferienclub

Ich möchte innerhalb des Ferienclubs Gäste, Mitarbeiter und Gegenstände/Inventar tracken. Dazu sollen vorerst feste Lesegeräte eingesetzt werden. Darauf folgend ist eine Erweiterung auf mobile Lesegeräte angedacht (mit allen Ihren möglichen Updatestrategien untereinander und mit dem Hauptsystem). Die Trackingdaten sollen den anderen Gruppen je nach ihren Bedürfnissen angeboten werden. Die „Standartschnittstellen“ sollen SQL-Datenbank-Views sein. Andere Schnittstellen (SOAP/WSDL, etc.) werden auf Wunsch natürlich ebenso angeboten (siehe Folie 19). Die Trackingdaten möchte ich auch selber für eine mobile Testanwendung nutzen, welche versuchen soll, die Animateure bei ihrer Arbeit zu unterstützen (siehe Folie 20). Für die Erfassung und Auswertung der Trackingdaten möchte ich herausfinden, in wieweit sich Software, die eigentlich für EPC-Anwendungen gedacht ist, auch in unserem Ferienclub anwenden lässt.

Literaturliste

Finkenzeller, Klaus: *RFID-Handbuch* 3. Auflage, ISBN 3446220712,
http://www.rfid-handbook.de

Stein, Martin: *Entwicklung eines auf RFID basierenden mobilen Objekt-Tracking-Systems*
http://users.informatik.haw-hamburg.de/~ubicomp/arbeiten/diplom/stein.pdf

Hennig, Ladkin, Sieker (RVS Group, Universität Bielefeld):
Privacy Enhancing Technology Concepts for RFID Technology Scrutinised,
http://www.rvs.uni-bielefeld.de/publications/Reports/SPC2005_Privacy_Enhancing_Technology_Concepts_for_RFID_Technology_Scrutinised.pdf

BSI: *Risiken und Chancen des Einsatzes von RFID-Systemen*
http://www.bsi.bund.de/fachthem/rfid/RIKCHA.pdf

Langheinrich, Marc: *Die Privatsphäre im Ubiquitous Computing - Datenschutzaspekte der RFID-Technologie*
http://www.vs.inf.ethz.ch/publ/papers/langhein2004rfid.pdf

Finke, Thomas und Kelter, Harald (BSI):
Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems
http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf

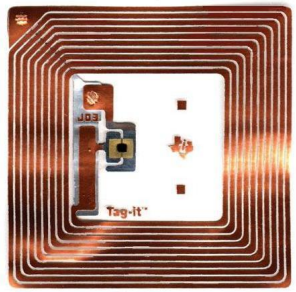
hochschule für angewandte wissenschaften
FACHBEREICH ELEKTROTECHNIK UND INFORMATIK hamburg
university of applied sciences

Thema: RFID

Eine kleine Einführung in Technik und Anwendung
UND
Die Einsatzmöglichkeiten in unserem Ferienclub

RFID-Technik

Radio Frequency Identification



passiver RFID-Tag [P01]

- Siliziumchip zur Speicherung von Daten
- Kontaktlose Datenübertragung zwischen Lesegerät und Tag (Verschleißfreiheit!)
- Tags (zumeist) ohne eigene Energiequelle

→ So etwas wie „kontaktlose Smartcards“

RFID-Technik

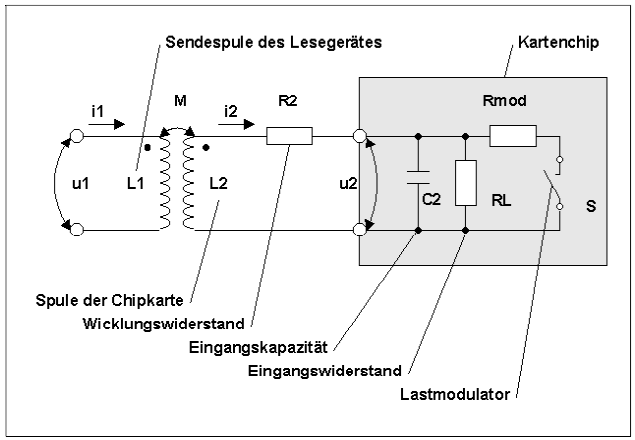
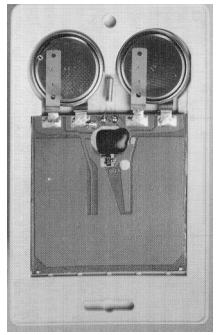


Abbildung: Prinzip der Datenübertragung über Lastmodulation [EP01]

RFID-Technik

Es gibt nicht den RFID-Tag.



aktiver RFID-Tag [P02]

Wichtige Unterscheidungskriterien:

1.) Aktive und passive Tags
2.) Reichweiten und Kopplungsarten:
   a.) Close Coupling bis ca. 1cm
   b.) Remote Coupling bis ca. 1,5m
   c.) Long-Range bis ca. 15 Meter
3.) Übertragungsgeschwindigkeiten
4.) Speicherkapazitäten
5.) Antikollisionsverfahren
6.) Kryptographische Verfahren

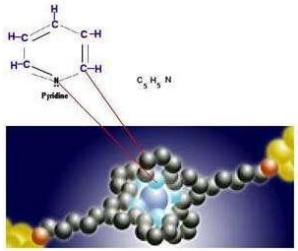
RFID-Technik

Passive RFID-Tags heute:

Wenn heute für passive Tags „hohe“ Reichweiten gefordert werden, müssen große Antenne und/oder sehr hohe Sendeleistung in den Lesegerätegeräten verwendet werden, da der Energieverbrauch der auf Siliziumchips basierenden Tags relativ hoch ist.

Kleine Zukunftsvision:

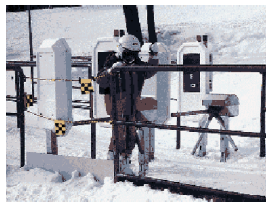
Die Nanotechnologie wird in (womöglich) absehbarer Zeit Schaltungen auf molekularer Ebene liefern können, welche nur noch einen Bruchteil an Energie von dem benötigt, was seine Vorfahren aus Silizium benötigt haben.



Nano-Transistor [P03]

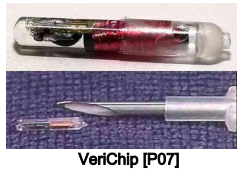
Anwendung

Authentifikation durch Besitz



Skipass [P04]

VIP-Area im Baja Beach Club (Barcelona) [P08]



VeriChip [P07]

RFID-Gaderobenschränke [P06]

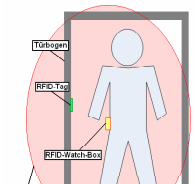
- Türschlösser
- Skipass
- ÖPNV-Ticket
- Mexikanische Staatsanwaltschaft (VeriChip)

Elektronisches Schloss mit RFID-Armband [P05]

Anwendung

Ortsabhängige Informationen

- Eurobalise der Bahn
- Landmarken in meiner Diplomarbeit
- Zukünftig zum Beispiel denkbar:
  - Verkehrsschilder zusätzlich mit Tags
  - Parkverbotszonen mit Tags
  - „Einkaufsfelder“ (siehe Tafel)
  - etc.



Landmarke am Türbogen [P10]

Eurobalise [P09]

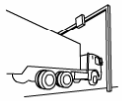
Anwendung

Weiter Anwendungen (heute und morgen)

- Child-Seat Presence and Orientation Detection (CPOD)
- Objekt-Tracking (DHL, Containerhafen, Einzelhandel, etc.)
- Mauterfassung (Österreich: GO-Box)
- Kühlkettenüberwachung (Sensor-RFID)
- Idee: Gerät-Heil/Defekt-Erkennung durch Überwachung des Stromverbrauchs über die Zeit und Erkennung von verdächtigen Veränderungen (einfaches Bsp.: Glühbirne)

GO
MAUTSYSTEM FÜR LKW UND BUS

GO-Box Logo [P11]



Anwendung

RFID – Die Technik bietet mehr, als der Name verspricht!

- Der Name spricht nur von Funkerkennung
  (vgl. Transpondertechnik in der Fliegerei)
- In Wirklichkeit auch ein sehr preiswertes kabelloses Interface!
- Das Lesegerät kostet relativ viel – die Gegenseite unglaublich wenig
  - Bluetooth: mehr als 5 Euro/Gerät
  - IrDA: mehr als 1 Euro/Gerät
  - RFID: weniger als 50 Cent/Gerät
- Anwendungsbeispiele:
  - Auch Billigstgeräte könnten eine Schnittstelle bekommen
  - z.B. Taschenrechner (kein Ergebnis abtippen mehr)
  - Beispielszenario „Fitnessclub“ (siehe Tafel)

Anwendung

Nokia Xpress-on™ RFID-Reader-Shell

Nokia RFID-Cover [NP01]

Vorstellbare Anwendungen:

„Halten Sie bitte Ihr Handy an diese Stelle Ihres Versicherungsvertrages, sie werden umgehend mit dem für Sie zuständigen Sachbearbeiter verbunden (12 Cent/Min.)“

„Halten Sie nun Ihr Handy an Ihre Wasseruhr, um den Zählerstand an die Hamburger Wasserwerke zu übermitteln. (0800-SMS-Freecall)“

…und vieles, vieles mehr ist noch denkbar.

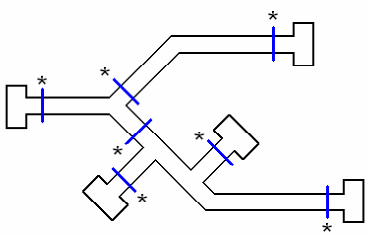
Technische Eckdaten [NP02]

Color:	Black
Dimensions:	106.5 x 46.8 x 26.7 mm (with the phone)
Weight:	111.2 g (with the phone)
Display:	Phone display: 27.3 x 27.3 mm, 4096 colors in 128 x 128 pixels 5 lines for text in basic mode with 16-pixel font
Durability:	Xpress-on™ RFID Reader Shells provide protection against splashes and dust
Power:	Phone battery: BL-5B, 760mAh, talk time up to 2h-5h
Frequency:	13.56 MHz
Protocol:	MIFARE® UltraLight
Read range:	Typically 2-3 cm, tag dependent
Standard:	ISO 14443A

Klassisches RFID-Tracking

- Viele stationäre Lesegeräte
- Lesegerätschleusen werden strategisch positioniert
- „Welt“ muss vorher bekannt sein
- Zentraler Server sammelt Tracking-Informationen (Kommunikationsnetz!)

RFID-Lesegerät-Schleuse [P13]

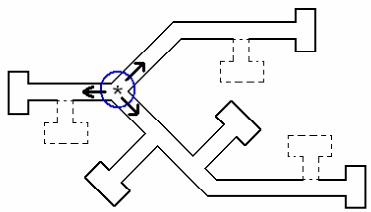


* fest installiertes RFID-Lesegerät

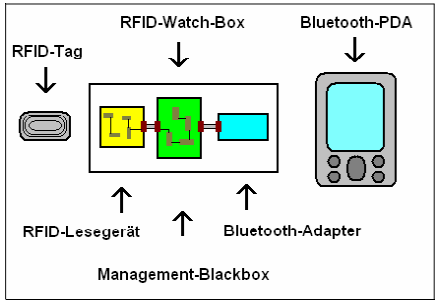
RFID-Lesegerät-Schleuse [P12]

„mobiles RFID-Tracking“

- Ein mobiles Lesegerät
- Es wird angenommen, das Positionswechsel der zu trackenden Gegenstände (meist) durch den Träger des Lesegeräts stattfindet
- „Welt“ darf in gewissen Grenzen vorher auch unbekannt sein



* ortsveränderliches RFID-Lesegerät

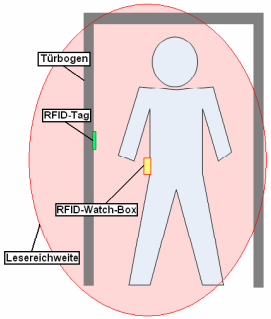


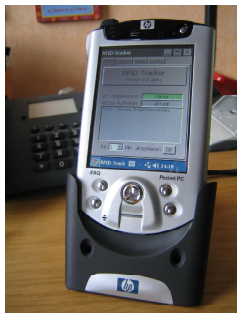
„mobiles RFID-Tracking“

Zwei Aufgabentypen:

1.) Eine fortwährende Überwachung der Umgebung nach auftauchenden und wieder verschwindenden RFID-Tags (Objekte und Landmarken) durch die RFID-Watch-Box

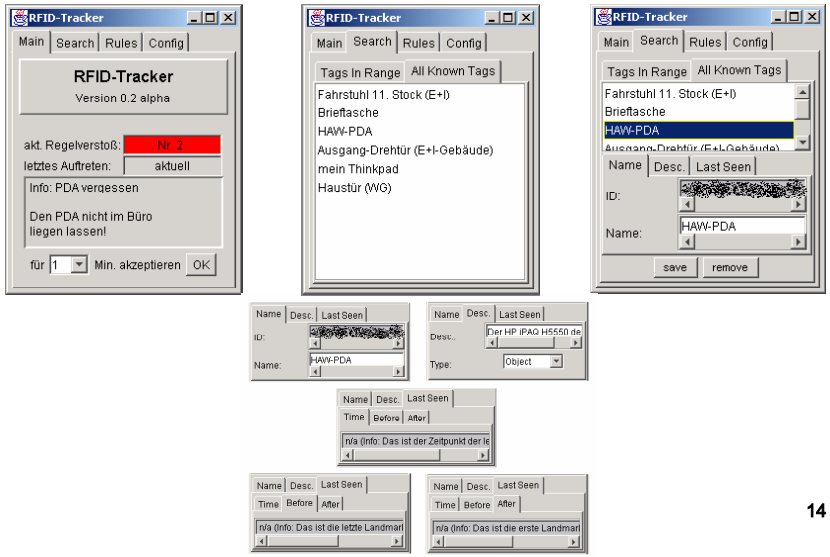
2.) Eine bedarfsfällige Menüführung für den Benutzer durch einen PDA.



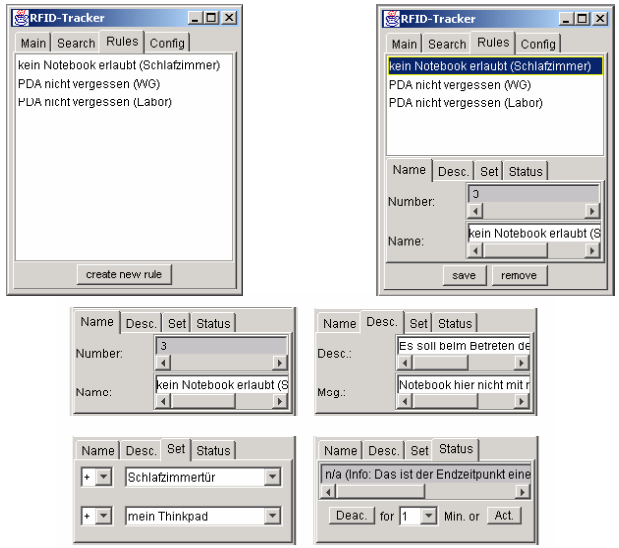


RFID-Configurator

„mobiles RFID-Tracking“



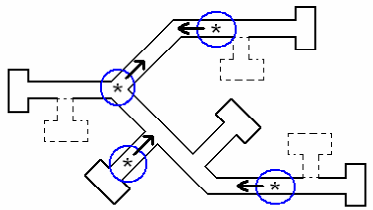
„mobiles RFID-Tracking“



Mehr zum Thema findet man unter: http://users.informatik.haw-hamburg.de/~ubicomp/arbeiten/diplom/stein.pdf

„verteiltes mobiles Tracking“

- Viele mobile Lesegeräte
- Bei Lesegerätbegegnungen werden RFID-Tag-Sichtungen gegenseitig aktualisiert
- Je mehr Lesegeräteträger desto aktueller die Tracking-Daten (alle „Fremdbewegungen“ werden besser erkannt)



*ortsveränderliches RFID-Lesegerät

Antikollisionsstrategien

1.) „Slotted Aloha“

- Mehrere Antwort-Slots mit jeweils Adresslänge
- Jeder Tag in Reichweite wählt sich zufällig einen der Slots aus
- Erkannte Tags werden stummgeschaltet
- Schnell (aber nur bei sehr wenigen Tags in Reichweite)

2.) „Binärer Suchbaum“

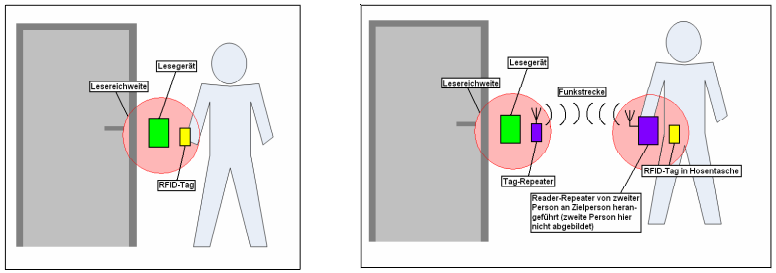
- Bitgenaue Kollisionserkennung
- Adress-Bitmasken
- Erkannte Tags werden stummgeschaltet
- Langsamer (funktioniert aber immer)

Sicherheitsprobleme

1.) Bisher fehlende Anonymität, da Tag-ID = Tag-Adresse

2.) „Feind hört mit“ – Abhören der Kommunikation zwischen Lesegerät und RFID-Tag bei den meisten Systemen möglich, da Kryptographie viel elektrische Energie kostet

3.) Der „Repeater-Angriff“ – Allgemeiner Angriff auf die „Authentifikation durch Besitz“-Verfahren



Mein Angebot an den Ferienclub

- Tracking mit festen Lesegeräten (ggf. auch mobile Lesegeräte)

- Getrackt werden: Gäste, Mitarbeiter, Gegenstände/Inventar

- Mögliche Anfragen an das System:
  1.) Wo ist X?
  2.) Wo war X schon?
  3.) Wer ist alles an Position Y + Radius?
  4.) Wer war schon alles an Position Y + Radius?
  5.) etc. (welche Wünsche und Vorschläge habt ihr?)

- Möchtet Ihr die Informationen direkt per SQL aus der Datenbank holen oder wünscht ihr Euch noch eine andere Schnittstelle?

Mein Zusatz

Ein Mitarbeiter-Unterstützungs-PDA

Für die Animateure:

- Animateur-Unterstützungs-Server erkennt gelangweilte Gäste (z.B. über Trinkverhalten, Verschwinden anderen Gästen aus seiner Umgebung, etc.)
- Automatische Zuordnung welcher Animateur sich kümmern soll (Animateur gerade in der Nähe vom Gast und kennt ihn schon)
- PDA zeigt dem Animateur ein Bild des Gastes, den aktuellen Aufenthaltsort, Interessen des Gastes und in Frage kommende aktuell mögliche Aktivitäten, etc.
- Animateur-PDA ggf. mit Display in der Sonnenbrille und Soundausgabe über Sonnenbrillenbügel

Für die Hausmeister: ???

Mein Zusatz

Die Animateure [P14] [15] [18]
Die bekommen vielleicht besser noch etwas buntere Klamotten…

Die Hausmeister-Crew mit unbefristeten Arbeits-verträgen (wirklich fester Bestandteil der Firma) [P19]

Hausmeister mit Zeitvertrag [P16] [17]

Mein Forderungen

Ich brauche von Euch:

1.) Eine geeignete Datenbank

2.) Ein Kommunikationsnetzwerk auf dem Club-Gelände (Flächendeckend? Wie zuverlässig? Wie vertraulich?)

3.) Wer sucht mir „Langweiler“? Ggf. Informationen aus einem Data-Warehouse ziehen? Auch Interessenprofile brauche ich! Ggf. aus Bewegungsprofilen, „Einkaufsverhalten“ im Club, etc.

What Not To Do

Keine Bezahlung allein durch RFID-Tags!

Auch sonstige (alleinig) durch RFID-authentifizierenden Verfahren unterlassen (siehe Repeater-Angriff) – zumindest bei sicherheitskritische Anwendungen

Datenschutz

Datenschutz muss bereits in der Konzeptphase eingearbeitet werden!

In wieweit „darf“ man bestimmt Informationen sammeln?
(nicht nur im rechtlichen Sinn)

…oder sind wir vielleicht sowieso schon verloren?

Meine düstere Zukunftsvision:
„Distributed-P2P-Video-Surveillance-By-Stupid-Kiddies“
(siehe Tafel)

Literaturhinweise

Wer Interesse bekommen haben sollte, kann dort weiterlesen:

Finkenzeller, Klaus: *RFID-Handbuch* 3. Auflage, ISBN 3446220712, http://www.rfid-handbook.de

Stein, Martin: *Entwicklung eines auf RFID basierenden mobilen Objekt-Tracking-Systems* http://users.informatik.haw-hamburg.de/~ubicomp/arbeiten/diplom/stein.pdf

Hennig, Ladkin, Sieker (RVS Group, Universität Bielefeld): *Privacy Enhancing Technology Concepts for RFID Technology Scrutinised,* http://www.rvs.uni-bielefeld.de/publications/Reports/SPC2005_Privacy_Enhancing_Technology_Concepts_for_RFID_Technology_Scrutinised.pdf

BSI: *Risiken und Chancen des Einsatzes von RFID-Systemen* http://www.bsi.bund.de/fachthem/rfid/RIKCHA.pdf

Langheinrich, Marc: *Die Privatsphäre im Ubiquitous Computing - Datenschutzaspekte der RFID-Technologie* http://www.vs.inf.ethz.ch/publ/papers/langhein2004rfid.pdf

Finke, Thomas und Kelter, Harald (BSI): *Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems* http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf

RFID-Videos

Wenn Interesse besteht, können wir jetzt noch ca. 30 Minuten „Werbevideos“ (accenture Consulting) und einen WDR „Monitor“ Beitrag zu RFID ansehen.

accenture
High performance. Delivered.

monitor

Ende

Danke für die Aufmerksamkeit zu dieser späten Stunde!

RFID

Bild-Quellen:

[P01]: http://www.elektroniknet.de/topics/kommunikation/fachthemen/2003/0021/images/3190908.jpg

[P02]: Finkenzeller, Klaus: RFID-Handbuch 3. Auflage, ISBN 3446220712

[P03]: http://www.ecplanet.com/pic/2004/09/1096340743/nanotransistor.jpg

[P04]: http://www.informatik.fh-muenchen.de/~chipcard/vortraege/vortrag6/Jens/Presentation/img020.GIF

[P05]: http://www.dbcbraincon.de/images/gat_lock.jpg

[P06]: http://www.dbcbraincon.de/images/fun_locks.jpg

[P07]: http://www.warcrimes.org.uk/captain/murder_inc/pics/verichip1.jpg

[P08]: http://www.erenouvelle.com/site/images/verichip2.jpg

[P09]: http://references.transportation.siemens.com/refdb/link_download.jsp?file_name=A19100-V100-B846607.pdf&l=de

[P10]: http://users.informatik.haw-hamburg.de/~ubicomp/arbeiten/diplom/stein.pdf

[P11]: http://www.go-maut.at/GoMedia/Image/de-AT/584_Image_HighRes.jpg

[P12]: http://www.kolinahrsystems.com/rfid/rfid_portal_large.gif

[P13]: http://www.sla.de/images/gate.jpg

[P14]: http://www.microopticalcorp.com/Applications/Images/appLGconsumer.jpg

[P15]: http://www.microopticalcorp.com/Applications/Images/task9.jpg

[P16]: http://www.microopticalcorp.com/Applications/Images/APPWCbig.jpg

RFID

Bild-Quellen:

[P17]: http://www.microopticalcorp.com/Applications/images/SV-3.jpg

[P18]: http://www.shimadzu.co.jp/hmd/images/top_main.jpg

[P19]: http://www.reviewjournal.com/images/bestoflv/1998/photos/startrek-borg.jpg

[EP01]: http://www.informatik.fh-muenchen.de/~chipcard/vortraege/vortrag6/Jens/Abbildung2-4.gif

[NP01]: http://www.nokia.com/BaseProject/Sites/NOKIA_MAIN_18022/CDA/Categories/Business/DocumentCenter/_Content/_Static_Files/rfid_kit_one_pager_v_2_0.pdf

[NP02]: http://www.nokia.com/nokia/0,,55738,00.html