Low power sniffing techniques used in 13.56MHz RFID reader systems

Using TRF7960 and MSP430F2370

Johannes Sturz

Juergen Mayer-Zintel
HF RFID reader sniffing techniques

- **Scope - Problem description**
  - Application example

- **13.56MHz RFID system overview**
  - ISO standard / RF regulation
  - Typ. System components

- **Potential sniffing solutions**
  - Mechanical, optical
  - Ceramic Resonator approach
  - Capacitive Sensor
  - TRF796x RSSI check

- **Proposed solution – best cost/pwr. budget**
  - Principle / basic idea / limitation
  - Schematic
  - MSP430 Software
  - Power consumption estimation

- **Summary, outlook, further improvements**
HF RFID reader sniffing techniques

• Scope

  – Many 13.56MHz RFID reader terminals are battery powered
  – Battery size and capacity as small as possible (cost).
  – Typ. 3.6V supply voltage.
  – Use affordable battery technology.
  – No additional components.
  – Polling intervals up to max. 1s
  – ISO 15693 and ISO 14443A/B Cards
  – Most critical applications:
    Car2Go, Door Lock, “car toll reader”

Ultra low power HF RFID card sniffer needed!
HF RFID reader sniffing techniques

- 13.56MHz RFID system overview – RF regulation

Spectrum mask for the European HF RFID frequency band 6.78MHz and 13.56MHz

Carrier accuracy @13.56MHz ±7kHz (~500ppm)
HF RFID reader sniffing techniques

- 13.56MHz RFID system overview – ISO standards

**ISO 15693 / ISO18000-3** – HF-I Product Line – *Vicinity cards*
  - Most widespread HF card – no/very limited security.

**ISO 14443A** – Wireless Payment/Secure – *Proximity cards*
  - Defines the physical layer and some communications layer.

**ISO 14443B** – Wireless Payment/Secure – *Proximity cards*
  - Defines the physical layer and some communications layer.

**Felica (ISO 14443C)** – Near Filed Communication – *Proximity cards*
  - Reader manufacturer will need licensing agreement with Sony.

**NFC (ongoing)** – Near Filed Communication – *Proximity cards*
  - Defines the physical layer and some communications layer.
HF RFID reader sniffing techniques

- 13.56MHz RFID system overview

A battery-less tag gets its energy from the radio waves generated by the reader’s antenna.

**Downlink** (Reader ➔ Inlay)

- ASK Modulation
- Pulse Position Coding
- Datarate 1.6 or 26 kbits/sec

*TI Proprietary Information – Selective Disclosure*
HF RFID reader sniffing techniques

• 13.56MHz RFID system overview

Downlink uses ASK Modulation

ISO 15693 Inlays operate with 100% or 10% modulation; using 10% modulation lowers the spurious emissions.
HF RFID reader sniffing techniques

- 13.56MHz RFID system overview

Communication from Inlay to Reader

**Uplink** (Inlay → Reader)
- FSK or ASK modulation
- (Load-modulation)
- Manchester coding
- Datarate 6 or 26 kbits/sec

"TI Proprietary Information – Selective Disclosure"
HF RFID reader sniffing techniques

• 13.56MHz RFID system overview

Communication from Inlay to Reader

– ASK @423.7kHz sub-carrier
  
or

– FSK with 423.7kHz / 484.2kHz

Digital Bits

Manchester Bits

RF Bits FSK

RF Bits ASK
HF RFID reader sniffing techniques
• 13.56MHz RFID system overview

A 13.56MHz RF-Field on its own, does not automatically generate a response from the Inlay.

– The Inlay only sends back a signal if:
  • the inlay is in the reading field of a reader’s antenna
  • the complete downlink protocol has been understood
  • the inlay keeps within the RF-Field while sending back information

– The inlay can be seen as a slave, whilst the reader is the master.

Note:
Because all ISO inlays work the same way, different technologies can be used simultaneously without interference problems between the inlays
HF RFID reader sniffing techniques

- RFID card sniffing solutions

Decision Criteria

- Mechanical design
  - Design flexibility / degree of freedom
  - Mechanical robustness

- Cost
  - production
  - Installation
  - Maintenance free → battery lifetime

- User friendly
- Protection against vandalism / fraud
- World wide usage / no country specific designs
HF RFID reader sniffing techniques

- RFID card sniffing solutions

**Mechanical / Optical**

A card slot is equipped with a mechanical switch or a light barrier; acting as a “mechanical sensor” to trigger the RFID card reader.

**Pro**
- Very low power
- Familiar handling (magnetic card)

**Con**
- Mechanics required
  - Form factor limitations
  - Reliability / robustness
- Not for harsh environment
- Limited protection against vandalism / fraud
HF RFID reader sniffing techniques

• RFID card sniffing solutions

Resonator approach

The reader is equipped with an additional resonator osc. and sensor antenna. The μC generates a short 13.56MHz power burst (20…200μs) and detects the antenna damping.

Pro
- Low power
- No mechanics required
  • Form factor limitations
  • Reliability / robustness
  • Protection against vandalism / fraud

Con
- Additional electrical components required
  • 2 Antennas (RFID / Card sniffer) or switch (high voltage)
  • 2nd low pwr., fast run-in osc.
- Regulation → frequency accuracy
- Detection Distance
HF RFID reader sniffing techniques

• RFID card sniffing solutions

Capacitive proximity Sensor

The reader antenna also comprises areas used for a capacitive sensor. Capacitive proximity sensors sense "target" objects (RFID cards) due to their ability to be electrically charged. Since even non-conductors can hold charges, this means that just about any object can be detected with this type of sensor.

The reader sends an inventory command each time the sensor detects any change.

Pro
– Flexible SW solution
– Detection range
– Good protection against vandalism
– For all card types
  • ISO-15693 and ISO-14443A/B
  • NFC / Felica

Con
– Many additional components
– High power consumption
– Detector is measuring E-Field, 13.56MHz card is using H-Field
  → false wake-up
HF RFID reader sniffing techniques

• RFID card sniffing solutions

TRF796x RSSI check

The reader issues an Inventory Requ. cmd.; with each cmd. The RSSI value is transmitted to the µC. Dependent on the RSSI value, additional commands are issued.

Pro
– No additional components
– Flexible SW solution
– Good detection range
– For all card types
  • ISO-15693 and ISO-14443A/B
  • NFC / Felica

Con
– High power consumption
  • Long Run-in times → TRF7960
  • High peak current
– Detection resolution
**HF RFID reader sniffing techniques**

• RFID card sniffing solutions

**Proposed solution – Principle & Basic Idea 1/2**

• Initialize the Reader system
  – TRF7960 initialization of the voltage regulators
  – MSP430 initialization → use high frequency Osc. @ 13.56MHz to shorten system run in times.

• Generate a short 13.56MHz TX power pulse (10 … 15μs) through the TRF7960 reader antenna. Use shielded (magnetic) antenna to desensitize the reader against parasitic E-Field damping.

• Sense the damping of the reader antenna circuit → with / without card.

• Rectify the antenna voltage, store it and measure the decay timing after the TX_off.
Use slope A/D technique on MSP430 to measure the $C_1$ charge voltage.

Dependent of the decay timing, initialize the system for a “card_read” or go back to stand-by.
HF RFID reader sniffing techniques

- RFID card sniffing solutions

Proposed solution – schematic
HF RFID reader sniffing techniques

- RFID card sniffing solutions

Proposed solution – System measurement

TX pulse = 15μs

RF (divided, C7/C8)
DEMOD (no card)
DEMOD (card distance = 0cm)
Comp. OUT (card distance = 0cm)
Comp. OUT (card distance = 5cm)
Comp. OUT (no card)

Delta Pulse Length (Bx – Ax)
Voltage difference
HF RFID reader sniffing techniques

- RFID card sniffing solutions

Proposed solution – Power consumption MSP/TRF 1/5

- Phase 1
  - Standby: MSP430 / TRF7060

- Phase 2
  - 13.56MHz Osc. Startup
  - MSP430 initialization
  - TRF7960 programming
  \[ \rightarrow 2\text{msec.} \]

- Phase 3
  - TRF7960 regulator start-up \[ \rightarrow 800\mu\text{sec.} \]

- Phase 4
  - 13.56MHz TX on \[ \rightarrow 15\mu\text{sec.} \]

- Phase 5
  - Comparator count \[ \rightarrow 2...10\mu\text{sec} \]

- Phase 6
  - MSP430 calculation/Status change \[ \rightarrow 5\mu\text{sec} \]
HF RFID reader sniffing techniques

- RFID card sniffing solutions

Proposed solution - Power consumption card read 2/5

Power consumption per 500ms Card polling interval @3.3V

<table>
<thead>
<tr>
<th>Description</th>
<th>Time</th>
<th>Average Current TRF7960</th>
<th>Average Current MSP430</th>
<th>Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1 Standby MSP430/TRF (only RC Osc. Running)</td>
<td>500ms</td>
<td>&lt;1μA</td>
<td>&lt;1μA</td>
<td>1 μAs</td>
</tr>
<tr>
<td>Polling sequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phase 2 13.56MHZ Osc. Start up / MSP430 init. /</td>
<td>2msec.</td>
<td>1.5mA</td>
<td>1mA</td>
<td>5 μAs</td>
</tr>
<tr>
<td>TRF7960 programming</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phase 3 TRF7960 regulator start-up</td>
<td>800 μsec</td>
<td>3.5mA</td>
<td>1mA</td>
<td>3.6 μAs</td>
</tr>
<tr>
<td>Phase 4 13.56MHz TX_ON @ TRF7960 (half power)</td>
<td>15 μsec</td>
<td>60mA</td>
<td>1mA</td>
<td>0.9 μAs</td>
</tr>
<tr>
<td>Phase 5 MSP430 Comparator count</td>
<td>&lt;10μsec</td>
<td>&lt;1μA</td>
<td>1mA</td>
<td>0.01 μAs</td>
</tr>
<tr>
<td>Phase 6 MSP430 calculation / status change</td>
<td>5μsec</td>
<td>&lt;1μA</td>
<td>1.5mA</td>
<td>0.08 μAs</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td>9.59 μAs</td>
</tr>
</tbody>
</table>

Each ISO-15693 card polling requires about 9.6 μAs @3.3V
HF RFID reader sniffing techniques

- RFID card sniffing solutions

**Proposed solution - Power consumption card read 3/5**

**Power consumption per Card read @3.3V**

<table>
<thead>
<tr>
<th>Description</th>
<th>Time (μsec)</th>
<th>Average Current</th>
<th>Energy (μAs)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>TRF7960</td>
<td>MSP430</td>
</tr>
<tr>
<td>Inventory Request Command</td>
<td>1510.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOF</td>
<td>75.52</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EOF</td>
<td>37.76</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag wait time for response</td>
<td>323.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag response (with UID)</td>
<td>3624.96</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional Wait Time</td>
<td>309.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmit Next Slot Command</td>
<td>37.76</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>5918.90</td>
<td>68mA</td>
<td>1.5mA</td>
</tr>
</tbody>
</table>

TRF7960 energy consumption per ISO-15693 card read ≈ 415μAs.
**HF RFID reader sniffing techniques**

- RFID card sniffing solutions

**Proposed solution - Power consumption summary 4/5**

Power consumption stand-by (0.5s interval; MSP and TRF) → 1μAs

Power consumption per polling Interval (3ms, MSP and TRF) → 9.6μAs

Power consumption per UID Card read (6ms, MSP and TRF) → 415μAs
HF RFID reader sniffing techniques

- RFID card sniffing solutions

**Proposed solution - Power consumption summary 5/5**

- Assumptions
  - Supply 3.3V
  - typ. Battery capacity 2500mAh
  - self discharge < 4% per year (linear)
  - Polling interval 500ms
  - 1x ISO-15693 card read per hour (includes false wake-up and power consumption due to additional ISO-15693 commands).

- Energy consumption per hour (7200 x polling & 1 x card read):
  - Stand-by = 7.2mAs
  - Polling = 69.1mAs
  - Card read = 0.415mAs
  - Total: 76.715mAs = 21.3μAh

- Energy consumption per year (8760h):
  - IOS -15693 reader ➔ 187mAh
  - Battery self discharge ➔ 100mAh
  - Total: 287mAh

- Total Battery lifetime
  - Assuming a linear battery self discharge over the lifetime.
  - > 8.7 years
## HF RFID reader sniffing techniques

### Summary

<table>
<thead>
<tr>
<th></th>
<th>Mechanical Design</th>
<th>Cost</th>
<th>Power consumption</th>
<th>Misc. Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mechanical/Optical</strong></td>
<td>- Form factor limitation</td>
<td>- Reasonable</td>
<td>- Extreme low power consumption</td>
<td>- Potential reliability issues due to mechanical parts.</td>
</tr>
<tr>
<td></td>
<td>- Not for harsh environment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- No/Limited protection against vandalism/fraud</td>
<td>=&gt; mechanical design/components may generate additional cost.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resonator approach</strong></td>
<td>- No special mechanics required</td>
<td>- Additional components required</td>
<td>- Low power consumption due to fast run in of the resonator.</td>
<td>- Local RF regulation needs to be checked. - Potential detection range issue.</td>
</tr>
<tr>
<td></td>
<td>- Good protection against vandalism/fraud</td>
<td>=&gt; PA / Antenna Switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Capacitive proximity Sensor</strong></td>
<td>- No special mechanics required</td>
<td>- Quite expensive as several additional components required</td>
<td>- Reasonable power consumption due to additional cap. sensor device</td>
<td>- Several additional components - Sensor measures E-Field; Card is using H-Field. =&gt; This may result in fault wake-ups.</td>
</tr>
<tr>
<td></td>
<td>- Good protection against vandalism/fraud</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TRF796x RSSI check</strong></td>
<td>- No special mechanics required</td>
<td>- No additional components/ cost</td>
<td>- Quite high due to long system run-in times to measure the RSSI. - High pek current</td>
<td>- Very flexible SW solution - Good and accurate detection range. - No additional read cycle required</td>
</tr>
<tr>
<td></td>
<td>- Good protection against vandalism/fraud</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TRF/MSP H-Field sensor</strong></td>
<td>- No special mechanics required</td>
<td>- Reasonable as only a few additional components are required</td>
<td>- Low power consumption due to well timed run in procedure.</td>
<td>- Flexible SW solution - Good and accurate detection range. - pure H-filed sensing possible</td>
</tr>
<tr>
<td></td>
<td>- Good protection against vandalism/fraud</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
HF RFID reader sniffing techniques

• Summary and further improvements

– Ultra Low power, high resolution 13.56MHz ISO-15693 Card sniffer supporting a battery lifetime up to 8.7 years @ 2500mAh/3.3V

– Flexible solution, completely SW controlled e.g. sensing range can be adjusted by using different supply and power (Half/Full) settings.

– Optimize detection range and timings which may further reduce the system power consumption.

– Extend to ISO14443A/B card read by connecting to TRF7960 RX_IN2 PIN => matching required.
HF RFID reader sniffing techniques

Thank you for your attention