Submission Title: [Guard RFID 433 MHz PHY Proposal]
Date Submitted: [13 September, 2009]
Source: [Dalibor Pokrajac] Company [Guard RFID Solutions]
Address [#8 – 1600 Derwent Way, Delta, BC, V3M 6M5, Canada]
Voice:[604-998-4018], E-Mail:[dalibor.pokrajac@guardrfid.com]
Re: [Response to 802.15.4f Call For Final Proposals]

Contributors: [Dalibor Pokrajac (GuardRFID), Dave Michelson (University of British Columbia), Hongbo Guo, (University of British Columbia)]

Abstract: [Proposal for usage of 433 MHz channel as alternate 802.15.4f PHY and MAC modifications.]

Purpose: [To be considered during 802.15.4f standard development process]

Notice: This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

Release: The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15.
GuardRFID 433 MHz PHY Proposal
Why 433 MHz PHY?

- Avoid busy 2.4GHz channel
  - Thousands and tens of thousands Tags must coexist in limited area
  - Interference with Wi-Fi, Bluetooth, Zigbee, wireless phones, etc.

- Low cost
  - Low energy per bit transmitted / received (increased battery life)
  - Narrow band = low silicon complexity (low cost and power consumption)
  - Low infrastructure deployment cost (no system “tuning” or “calibration”)

- Optimal RF performance
  - Low pathloss and signal attenuation – very good range
  - Optimal data throughput
  - Optimal and adjustable location accuracy

- Seamless Indoor and Outdoor use

- Acceptable frequency band in most regions
  - Not true ISM band worldwide, but close to it

- Majority of RFID / RTLS systems deployed to date are 433 MHz
433 MHz Channel Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency Band</td>
<td>433.05 MHz – 434.79 MHz</td>
</tr>
<tr>
<td>Number of Channels</td>
<td>1</td>
</tr>
<tr>
<td>Channel Bandwidth</td>
<td>540 kHz</td>
</tr>
<tr>
<td>Data Rate</td>
<td>250 kb/s</td>
</tr>
<tr>
<td>Modulation</td>
<td>Minimum Shift Keying (MSK)</td>
</tr>
<tr>
<td>Pathloss</td>
<td>10m = 45dB, 100m = 65dB, 300m = 74dB</td>
</tr>
</tbody>
</table>
Frequency Band

- **Band:**
  - 433.05 MHz - 434.79 MHz
  - 1.74 MHz width

- **Channels:**
  - Single channel centered at 433.92 MHz
  - Potentially 3 channels available at 250 kb/s

- **Channel Bandwidth:** 540 kHz
Modulation

- **Minimum Shift Keying (MSK)**
  - Continuous phase FSK → Reduced non-linear distortion
  - Frequency difference between “1” and “0” = ½ data rate (modulation index is always 0.5)
  - Signals are orthogonal and minimal distance → more compact spectrum
  - Trade-off between Inter Symbol Interference and side-lobe suppression
    - Low ISI (compared to GMSK) but higher side lobes (less efficient use of spectrum)
    - The available 433 MHz channel is wide enough to tolerate this trade-off
Encoding

- Two carrier frequencies (f1 and f2)
- The frequency of one carrier is twice the frequency of the other
- Information bits are separated into even and odd bits – duration of each bit is doubled

**MSK signal rules:**

<table>
<thead>
<tr>
<th>Even Bit</th>
<th>Odd Bit</th>
<th>Output signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Invert f2</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Invert f1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>Adopt f1 without change</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Adopt f2 without change</td>
</tr>
</tbody>
</table>

- Each bit is encoded as a half sinusoid
- Bit to Symbol Mapping: 1:1
Data Rate

- Data rate has impact on
  - PER
  - Communication distance
  - Battery life

<table>
<thead>
<tr>
<th>Data Rate [kbps]</th>
<th>RX Sensitivity Degradation$^1$ [dBm]</th>
<th>Energy consumption per 20 byte PDU$^2$ [µJ]</th>
<th>Energy per Bit [µJ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>0</td>
<td>10,000</td>
<td>62.5</td>
</tr>
<tr>
<td>38.4</td>
<td>9</td>
<td>312</td>
<td>1.95</td>
</tr>
<tr>
<td>250</td>
<td>18</td>
<td>48</td>
<td>0.3</td>
</tr>
<tr>
<td>500</td>
<td>23</td>
<td>24</td>
<td>0.15</td>
</tr>
</tbody>
</table>

$^1$ = RX sensitivity for 1.2 kbps = -110 dBm
$^2$ = +10dBm transmit power, 20 bytes PDU, 3V battery, $I_{TX}$ = 25 mA

- Tradeoff between RX sensitivity, energy consumption, tag density → 250 kb/s as optimal Data Rate
## Link Budget

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Noise power (N) (B=540 kHz)</td>
<td>-116 dBm</td>
</tr>
<tr>
<td>Receiver Noise Figure (NF)</td>
<td>+6 dB</td>
</tr>
<tr>
<td>Receiver Noise Floor (RNF=N+NF)</td>
<td>-110 dBm</td>
</tr>
<tr>
<td>Eb/No</td>
<td>+12 dB</td>
</tr>
<tr>
<td>Signal To Noise Ratio (SNR)</td>
<td>+7.33 dB</td>
</tr>
<tr>
<td>Received Power (Prx=RNF+SNR)</td>
<td>-103 dBm</td>
</tr>
<tr>
<td>Transmit Antenna Gain (Gtx)</td>
<td>-15 dBm</td>
</tr>
<tr>
<td>Receive Antenna Gain (Grx)</td>
<td>0 dBm</td>
</tr>
<tr>
<td>Transmit Power (Ptx)</td>
<td>+10 dBm</td>
</tr>
<tr>
<td>Pathloss (Lfs)</td>
<td>30m</td>
</tr>
<tr>
<td><strong>Fade Margin (FM) (= Ptx – Prx – Lfs + Gtx + Grx)</strong></td>
<td>46 dB</td>
</tr>
</tbody>
</table>
Link Budget – cont’d

- Even with very low efficiency antennas (picture shows a Tag with Gtx = -15 dB) the link budget is still very good allowing for comfortable indoor and outdoor use in RF hostile environments

- High Fade margin is essential to compensate for various losses:
  - Tag attached to metal surface → 10-30 dB
  - Drywall, wooden frame → 6-10 dB
  - Concrete floor → 10-30 dB

- 433 MHz has significantly lower signal attenuation than higher ISM frequencies
Pathgain 433 MHz vs. 2.4 GHz

Data from IEEE 802.15-09-0501-00-004f

- Measurement results in realistic environment show significant advantage of using 433 MHz vs. 2.4 GHz (15-26 dB)
  - Measurement distance: up to 40m;
  - Dashed black line – theoretical 15 dB improvement when frequency is lowered,
  - Solid red line – additional improvement due to lower attenuation through barriers
  - Industrial space: tall and large industrial structures but no walls (LOS/NLOS)
  - Office space: corridor (LOS) and closed rooms (NLOS)

Industrial LOS environment

Office LOS / NLOS environment

Better Better

at each location, the path gain has been averaged over 6 spatial points and across a 20 MHz frequency span
433 MHz Coexistence

- With 802 devices
  - There is no interference with any of existing 802 devices
- Within the band
  - Regulatory limits (e.g. FCC) restrict in-band interference with other 433 MHz devices
  - Tag to Tag interference is mitigated through redundant packet transmissions (Double Pure Aloha), CCA or CSMA
- With Licensed devices
  - This band is ISM band or de-facto ISM band worldwide
  - There is no interference with any of licensed devices
433 MHz Regulatory Compliance

- Countries throughout the world permit usage of the 433 MHz band at various ERP levels and duty cycles

<table>
<thead>
<tr>
<th>Region</th>
<th>Standard</th>
<th>Transmit Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA, Canada</td>
<td>FCC 15.231(e)</td>
<td>Field strength: 4400 μV/m @ 3m</td>
</tr>
<tr>
<td></td>
<td>RSS-210</td>
<td>10 sec blink rate</td>
</tr>
<tr>
<td></td>
<td>FCC15.240</td>
<td>Field Strength: 55,000 μV/m @ 3m (deployment restrictions apply)</td>
</tr>
<tr>
<td>Europe, Africa</td>
<td>ISM Band EN 300 220</td>
<td>Max ERP: &lt;10 mW @ 10% or &lt;1mW @ 100% duty cycle</td>
</tr>
<tr>
<td>China</td>
<td>SRRC Regulation</td>
<td>Max ERP: 10 mW, occupied bandwidth &lt; 400 kHz</td>
</tr>
<tr>
<td>Australia, New Zealand</td>
<td>AS/NZS 4268:2003</td>
<td>Max ERP: 15 mW</td>
</tr>
</tbody>
</table>
Tag Blink Rate

- Estimated requirements:

<table>
<thead>
<tr>
<th>Object</th>
<th>Example</th>
<th>Motion (%)</th>
<th>Static Blink</th>
<th>Dynamic Blink</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>Hospital Patient Assembly Line Worker</td>
<td>100%</td>
<td>n/a</td>
<td>1 - 10 sec</td>
</tr>
<tr>
<td>Mobile Asset</td>
<td>Wheelchair Forklift</td>
<td>70%</td>
<td>10 min</td>
<td>1 - 10 sec</td>
</tr>
<tr>
<td>Semi-Mobile Asset</td>
<td>IV Pump Container</td>
<td>10%</td>
<td>1 hour</td>
<td>10 - 60 sec</td>
</tr>
<tr>
<td>Static Assets</td>
<td>Furniture IT Equipment</td>
<td>1%</td>
<td>6 hours</td>
<td>10 - 60 sec</td>
</tr>
</tbody>
</table>

- Proposed Blink Rates for 433 MHz PHY:
  - Dynamic Blink:
    - 10 sec
    - 60 sec
  - Static Blink:
    - 10 min
    - 60 min

- A Tag could have both Blink Rates (static and dynamic) or only one
Location Mechanism

- RSSI based
  - Weighted Center of Mass Multilateration
  - Received signal is measured and compared to a noise floor
  - Pathloss and fading $\Rightarrow$ signal strength is inversly proportional to distance
  - Multipath compensation through statistical analysis (signal received by multiple nodes)

- No need for system tuning and calibration
  - Low infrastructure deployment cost

- Location is available within few seconds of Tag blink
  - Data is collected from multiple receivers

- Portal detection through alternative technologies (LF, IR, US):
  - Instant portal detection at very low power consumption cost (3-10 $\mu$W for “always on” operation)
  - Accurate Portal to Portal differentiation even when they are near each other
  - Precise room location (exact side of the wall)
Location Accuracy

- If sub 30 cm location accuracy cannot be guaranteed, 3 m accuracy is sufficient for majority of applications
  - Sub 30 cm location accuracy outside lab conditions is very difficult to guaranty at acceptable cost, regardless what technology is used
- Critical question to answer is “on what side of the wall is the Tag?”
  - 30 cm location accuracy cannot answer that question

- RSSI location accuracy is dependant on node density
  - Rule of thumb: Location accuracy is 15 - 20% of node to node distance (Some systems claim this accuracy to be 10% of node distance)
- RSSI achieves sub 3 meter location accuracy
  - Better accuracy is achieved when many nodes receive Tag signal and compute RSSI
  - 433 MHz Tags can afford distant receiver reception due to long communication distance
Location Accuracy

Screen captures from RTLS systems deployed in healthcare facilities (different location accuracy is achieved through different node density and different Tag transmit power)
RFID/RTLS within 802.15.4

- Transmit Only tags for most sensitive applications
  - Many applications do not need 2-way communication or even CCA
- Bidirectional Tags where data storage is needed or high link reliability
  - Traditional 15.4 communication
Bi-Directional Tags

- Compliant to “IEEE Std 802.15.4 – 2006” or later
  - FFD → Tag Reader
  - RFD → Tags
- MAC Frame changes as per pending 15.4e
  - Short MAC Header
- Additional MAC changes as per 15.4f (Blink Frame)

- Beacon Network
  - Applications with relatively small number of Tags
  - Applications where communication reliability is important
- Non-Beacon Network
  - Tag decides when to transmit data (Blink)
  - Acknowledged or unacknowledged, but must be associated
CCA before TX – Channel Access

- “Listen Before Talk” mechanism
- Clear Channel Assessment (CCA) performed before every transmission to avoid collisions
- Back-off mechanism as described in 802.15.4

Number of CCA+BO Slots depends on collision rate
CCA-TX Simulation Results

- Assumptions:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot interval</td>
<td>100 µs</td>
</tr>
<tr>
<td>Data rate (bit interval)</td>
<td>250 kbps (4 µs)</td>
</tr>
<tr>
<td>Tag PDU length</td>
<td>6 slots</td>
</tr>
<tr>
<td>CCA duration (Contention Window)</td>
<td>2 successive slots</td>
</tr>
<tr>
<td>Tag Power consumption in Delay</td>
<td>1.5 µW</td>
</tr>
<tr>
<td>Tag Power consumption in CCA</td>
<td>50 mW</td>
</tr>
<tr>
<td>Tag power consumption in TX</td>
<td>70 mW</td>
</tr>
</tbody>
</table>

- Tag state machine model
### CCA-TX Simulation Results (cont’d)

<table>
<thead>
<tr>
<th>Number of Tags</th>
<th>(BE\text{min}, BE\text{max})</th>
<th>Collision Rate</th>
<th>Power per blink [\mu W]</th>
<th>Total time delay (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>(6,8)</td>
<td>0.39</td>
<td>6.74</td>
<td>0.10</td>
</tr>
<tr>
<td></td>
<td>(9,11)</td>
<td>0.12</td>
<td>5.69</td>
<td>0.31</td>
</tr>
<tr>
<td></td>
<td>(12,14)</td>
<td>0.01</td>
<td>5.30</td>
<td>1.02</td>
</tr>
<tr>
<td>1,000</td>
<td>(6,8)</td>
<td>0.88</td>
<td>8.68</td>
<td>0.28</td>
</tr>
<tr>
<td></td>
<td>(9,11)</td>
<td>0.68</td>
<td>7.97</td>
<td>0.56</td>
</tr>
<tr>
<td></td>
<td>(12,14)</td>
<td>0.07</td>
<td>5.54</td>
<td>2.25</td>
</tr>
<tr>
<td></td>
<td>(15,17)</td>
<td>0.02</td>
<td>5.36</td>
<td>16.9</td>
</tr>
</tbody>
</table>

Note: Simulation results courtesy of Hongbo Guo, University of British Columbia

- **Highlighted** (BE\text{min}, BE\text{max}) looks reasonably good, but…
A flaw in “CCA before TX” principle

- Tag antenna gain is usually significantly lower than Tag Reader antenna gain (10 - 20 dB or even more)

  - 20 dB in link budget equals lots of distance!
  - Tags cannot hear majority of other Tags that Tag Reader can
    - 10 db difference in antenna gain → Tag can hear ~ 25% other Tags
    - 20 db difference in antenna gain → Tag can hear ~ 5% other Tags
  - Energy spent on CCA is largely wasted!
TX Only – Channel Access

- Variation of P-Aloha (“Double P-Aloha”)
- Low protocol efficiency but minimized power consumption and code complexity
- Collision “avoidance”:
  - Tags send redundant, randomized packets to compensate for collisions when Blink periods align
  - Tag timing is based on imperfect time keeping to allow Blink Windows to slide over time and Blinks drift apart
Successful Tag ID Reception Probability of Double P-Aloha

Mrepeat = Number of Packets in a Blink
Ntag = Number of Tags
T blink = Blink period

- $T_{\text{blink}} = 600 \mu s$ (20 byte PDU @ 250 kbps)
- Depending on expected Tag density for particular application, $M_{\text{repeat}}$ and $T_{\text{blink}}$ should vary (defined by Tag class)

### Graphs

- **Tblink = 10s**
  - $M_{\text{repeat}} = 3$

- **Tblink = 60s**
  - $M_{\text{repeat}} = 1$
PPDU

- **Small change from classic 15.4**
  - Add option to use 1 or 2 byte SFD

<table>
<thead>
<tr>
<th>4 Octets</th>
<th>1 / 2 Octet</th>
<th>1 Octet</th>
<th>Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preamble</td>
<td>SFD</td>
<td>Length</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>Synchronization Header</td>
<td>PHY Header</td>
<td>PSDU</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PHY Payload (MAC Frame)</td>
</tr>
</tbody>
</table>

- **Bit Synchronization**
  - Preamble Field
  - Alternate sequence of “1”s and “0”s

- **Byte Synchronization**
  - Start of Frame Delimiter (SFD)
  - 1 byte SFD format: “11100101”
  - 2 byte SFD format: “1111011100110001”
MAC Frame Changes

General 15.4 MAC Frame format

<table>
<thead>
<tr>
<th>2 Octets</th>
<th>1</th>
<th>0/2</th>
<th>0/2/8</th>
<th>0/2</th>
<th>0/2/8</th>
<th>0/5/6/10</th>
<th>Variable</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>Sequence Number</td>
<td>Dest. PAN ID</td>
<td>Dest. Address</td>
<td>Source PAN ID</td>
<td>Source Address</td>
<td>Security Header</td>
<td>Payload</td>
<td>CRC</td>
</tr>
</tbody>
</table>

Blink Frame format (General MAC Frame with “muted” fields)

<table>
<thead>
<tr>
<th>2 Octets</th>
<th>1</th>
<th>2</th>
<th>0/2/8</th>
<th>Variable</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>Sequence Number</td>
<td>Dest. PAN ID</td>
<td>Source Address</td>
<td>Payload</td>
<td>CRC</td>
</tr>
</tbody>
</table>

Optional Fields outside IEEE control

<table>
<thead>
<tr>
<th>1 Octet</th>
<th>1</th>
<th>Variable</th>
<th>Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Class</td>
<td>Device Type</td>
<td>Alternative ID</td>
<td>Sensor Data</td>
</tr>
</tbody>
</table>

- Changes to 15.4 MAC
  - New frame – Blink Frame
  - Source Address interpretation change (0 Octets $\rightarrow$ Address specified in Payload)
Proposed Frame Changes

- **Frame Control** → Add “Blink” frame type
  - 000 = Beacon
  - 001 = Data
  - 010 = Acknowledgement
  - 011 = Command
  - 100 = 1 Octet MHR
  - 101 = CSL Wakeup
  - 110 = Secure Acknowledgement
  - **111 = Blink**

- **Addressing**
  - **0 bit**: Payload addressing
  - **16 bit**: Dynamic addressing for Tags with 2-way communication
  - **64 bit**: Full EUI-64 address

- **Payload (not defined by IEEE):**
  - Device Class, Status, Alternate ID, Sensor data (includes alternate location methods: LF, IR, ultrasound, …)
Blink Frame Options

**0-bit Addressing Blink Frame format**

- Minimal message size, no security, no IEEE addressing
- Source Address (defined by industry association) is specified in Payload field
- Frame Control Field could be 1 octet (Short Frame Control as per 4e)

<table>
<thead>
<tr>
<th>2 Octets</th>
<th>1</th>
<th>Variable</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>Sequence Number</td>
<td>Payload</td>
<td>CRC</td>
</tr>
</tbody>
</table>

**64-bit Addressing Blink Frame format**

- Normal 15.4 addressing
- Payload may or may not be included

<table>
<thead>
<tr>
<th>2 Octets</th>
<th>1</th>
<th>2</th>
<th>8</th>
<th>Variable</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>Sequence Number</td>
<td>Source PAN ID</td>
<td>Source Address</td>
<td>Payload</td>
<td>CRC</td>
</tr>
</tbody>
</table>
Addressing Scheme

• **64-bit address (EUI-64)**
  – Useful, unique and simple addressing mechanism for many Tag applications
  – Unnecessarily long for other applications which are extremely sensitive to air time and power consumption
  – Some applications and industry associations require their own addressing scheme and can’t use EUI-64

• **16-bit address doesn’t satisfy needs of large scale Tag deployments.**
  – Can be used for some Tag applications which use classic 15.4 communication

• **0-bit address (payload addressing)**
  – Allows addressing through address specified in payload
  – Allows generation of short and efficient frame
  – Can be controlled by industry association built on top of 15.4f
Energy per PPDU (Blink Message)

- **0-bit Addressing**
  - Payload: 7 Bytes
  - Total PPDU length: 18 byte
  - Energy at 250kbps (0.3 µJ/bit) : 43.2 [µJ]

<table>
<thead>
<tr>
<th>4 Octets</th>
<th>1</th>
<th>1</th>
<th>2</th>
<th>1</th>
<th>9</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preamble</td>
<td>SFD</td>
<td>Length</td>
<td>Frame Control</td>
<td>Sequence Number</td>
<td>Payload</td>
<td>CRC</td>
</tr>
</tbody>
</table>

- **64-bit Addressing (EUI-64)**
  - Payload: 3 Bytes
  - Total PPDU length: 24 byte
  - Energy at 250kbps (0.3 µJ/bit) : 57.6 [µJ]

<table>
<thead>
<tr>
<th>4 Octets</th>
<th>1</th>
<th>1</th>
<th>2</th>
<th>1</th>
<th>2</th>
<th>8</th>
<th>3</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preamble</td>
<td>SFD</td>
<td>Length</td>
<td>Frame Control</td>
<td>Seq. Number</td>
<td>Source PAN ID</td>
<td>Source Address</td>
<td>Payload</td>
<td>CRC</td>
</tr>
</tbody>
</table>
Thank You!