Project: IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)

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]

GuardRFID 433 MHz PHY Proposal

Why 433 MHz PHY?

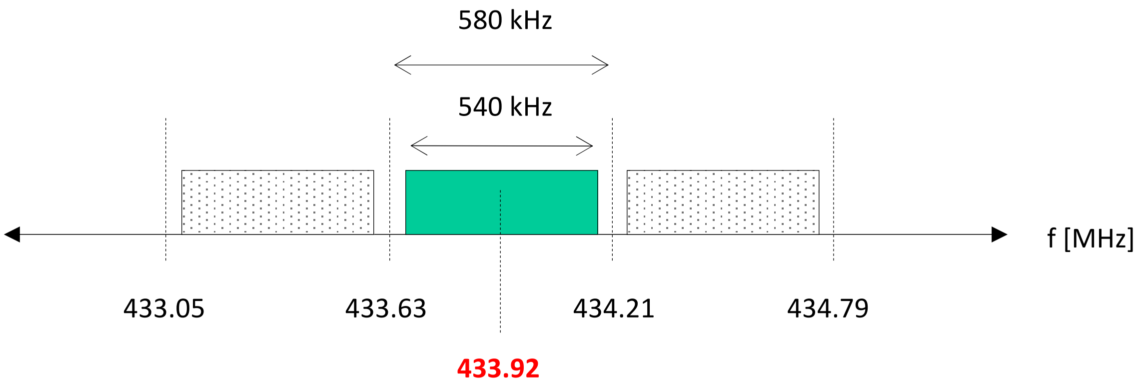
- Avoid busy 2.4GHz channel
  - Thousands and tens of thousands Tags must coexist in limited area
  - Interference with Wi-Fi, Bluetooth, Zigbee, wireless phones, etc.
- Low cost
  - Low energy per bit transmitted / received (increased battery life)
  - Narrow band = low silicon complexity (low cost 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

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

Frequency Band

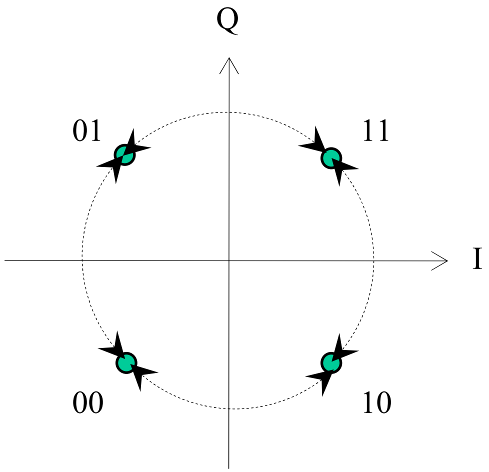
- Band:
  - 433.05 MHz - 434.79 MHz
  - 1.74MHz width
- Channels:
  - Single channel centered at 433.92 MHz
  - Potentially 3 channels available at 250 kb/s

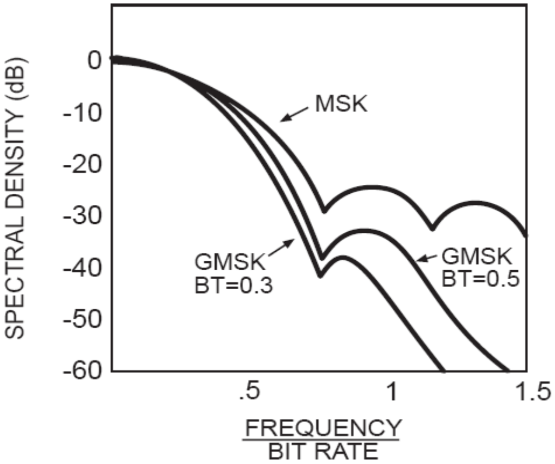


- Channel Bandwidth: 540 kHz

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



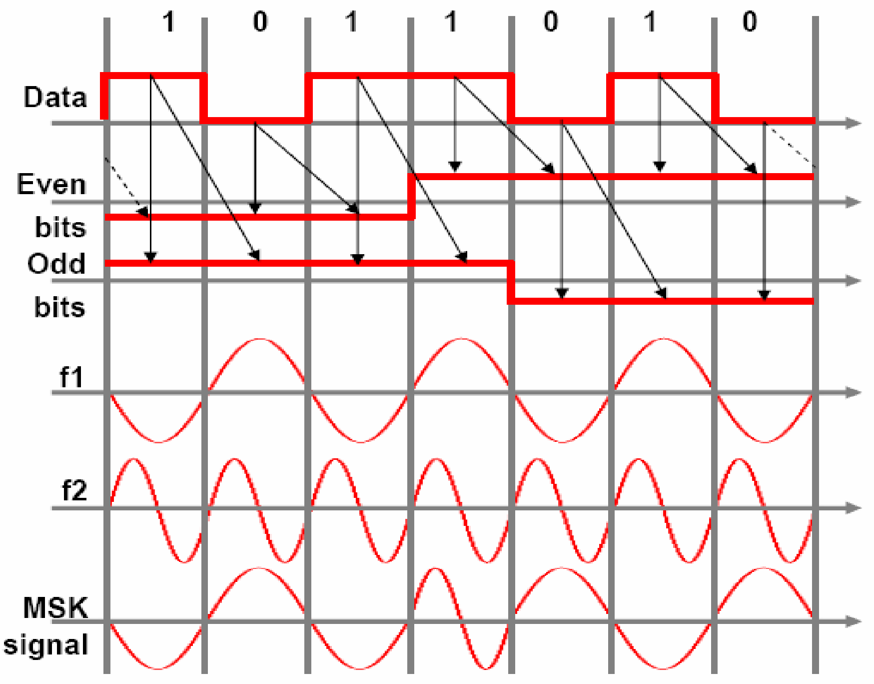


Encoding

- 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:

Even Bit	**Odd Bit**	Output signal
0	0	Invert f2
1	0	Invert f1
0	1	Adopt f1 without change
1	1	Adopt f2 without change



- 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

Data Rate [kbps]	RX Sensitivity Degradation[1] [dBm]	Energy consumption per 20 byte PDU[2] [μJ]	Energy per Bit [μJ]
1.2	0	10,000	62.5
38.4	9	312	1.95
250	18	48	0.3
500	23	24	0.15

[1] = RX sensitivity for 1.2 kbps = -110 dBm

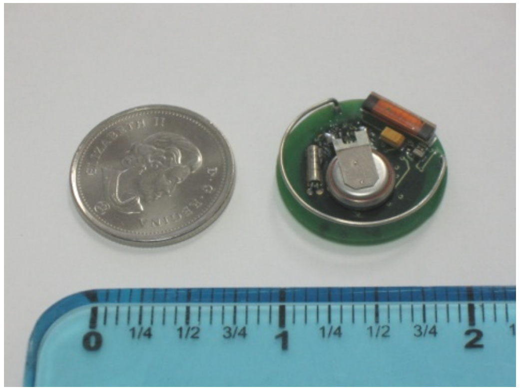
[2] = +10dBm transmit power, 20 bytes PDU, 3V battery, I_{TX} = 25 mA

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

Link Budget

Parameter	Value		
Noise power (N) (B=540 kHz)	-116 dBm		
Receiver Noise Figure (NF)	+6 dB		
Receiver Noise Floor (RNF=N+NF)	-110 dBm		
Eb/No	+12 dB		
Signal To Noise Ratio (SNR)	+7.33 dB		
Received Power (Prx=RNF+SNR)	-103 dBm		
Transmit Antenna Gain (Gtx)	-15 dBm		
Receive Antenna Gain (Grx)	0 dBm		
Transmit Power (Ptx)	+10 dBm		
	30m	100m	300m
Pathloss (Lfs)	54 dB	65 dB	74 dB
Fade Margin (FM) (= Ptx – Prx – Lfs + Gtx + Grx)	46 dB	35 dB	26 dB

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

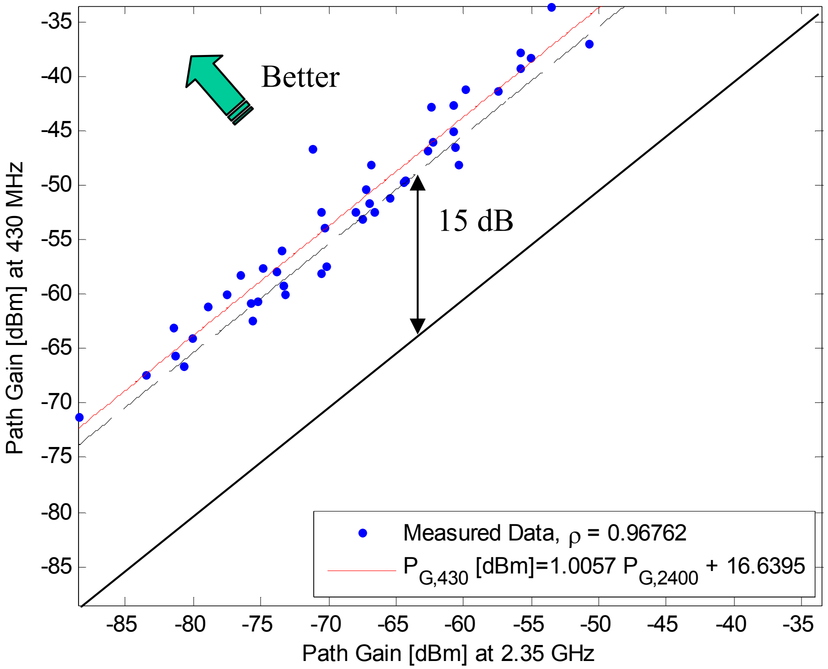
- 433 MHz has significantly lower signal attenuation than higher ISM frequencies

Pathgain 433 MHz vs. 2.4 GHz

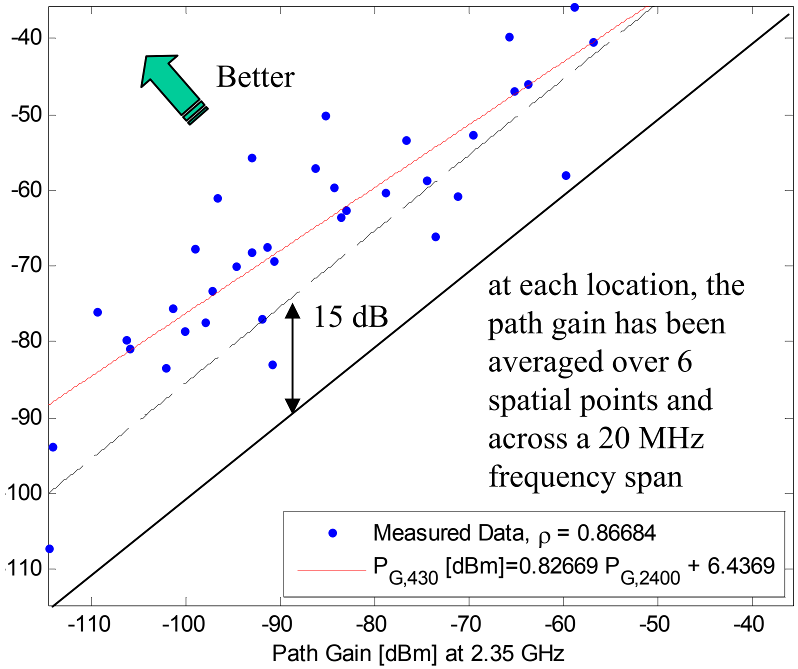
Data from IEEE 802.15-09-0501-00-004f

- 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



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

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

Tag Blink Rate

- Estimated requirements:

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

- 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 → 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 µW for “always on” operation)
  - Accurate Portal to Portal differentiation even when they are near each other
  - Precise room location (exact side of the wall)

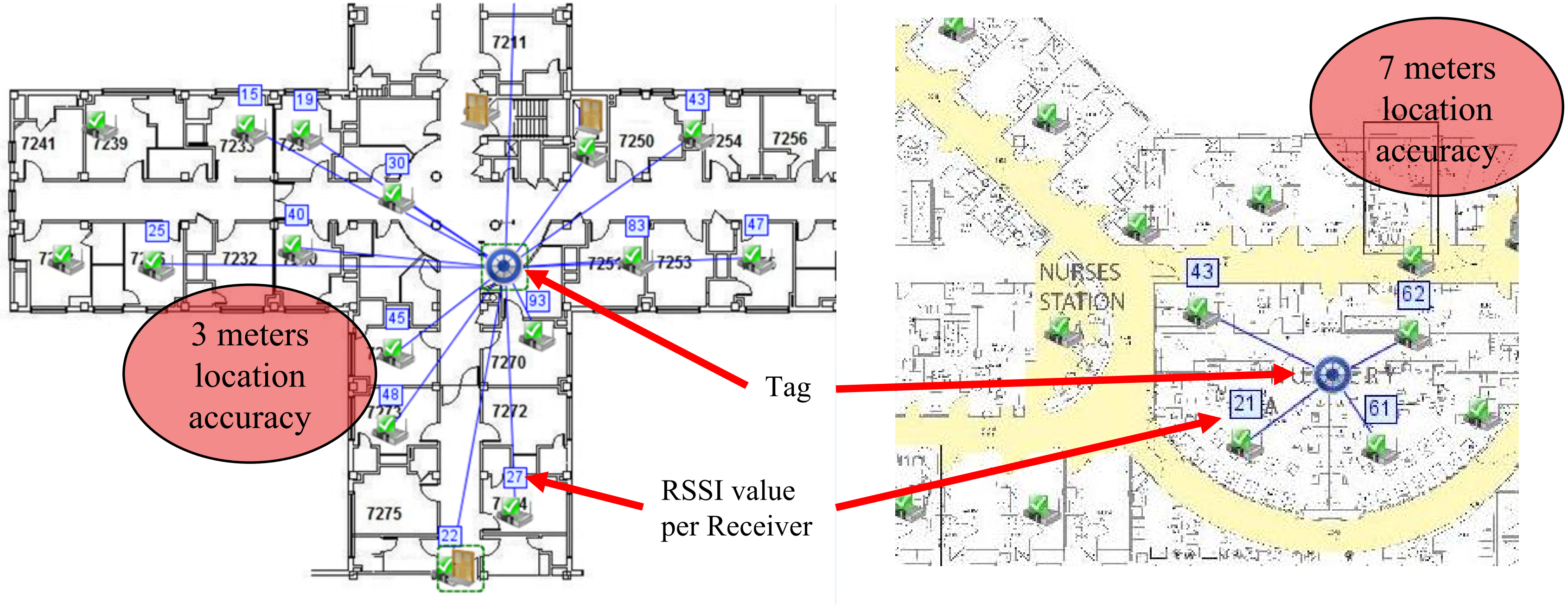
Location Accuracy

- 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)



3 meters location accuracy

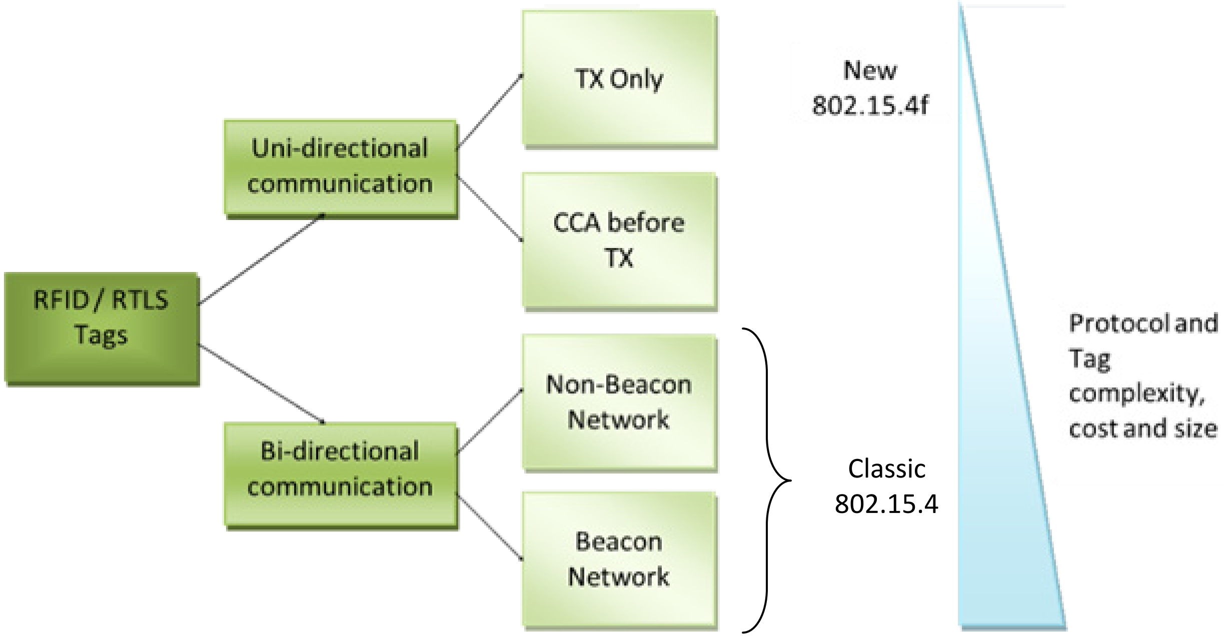
7 meters location accuracy

Tag

RSSI value per Receiver

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



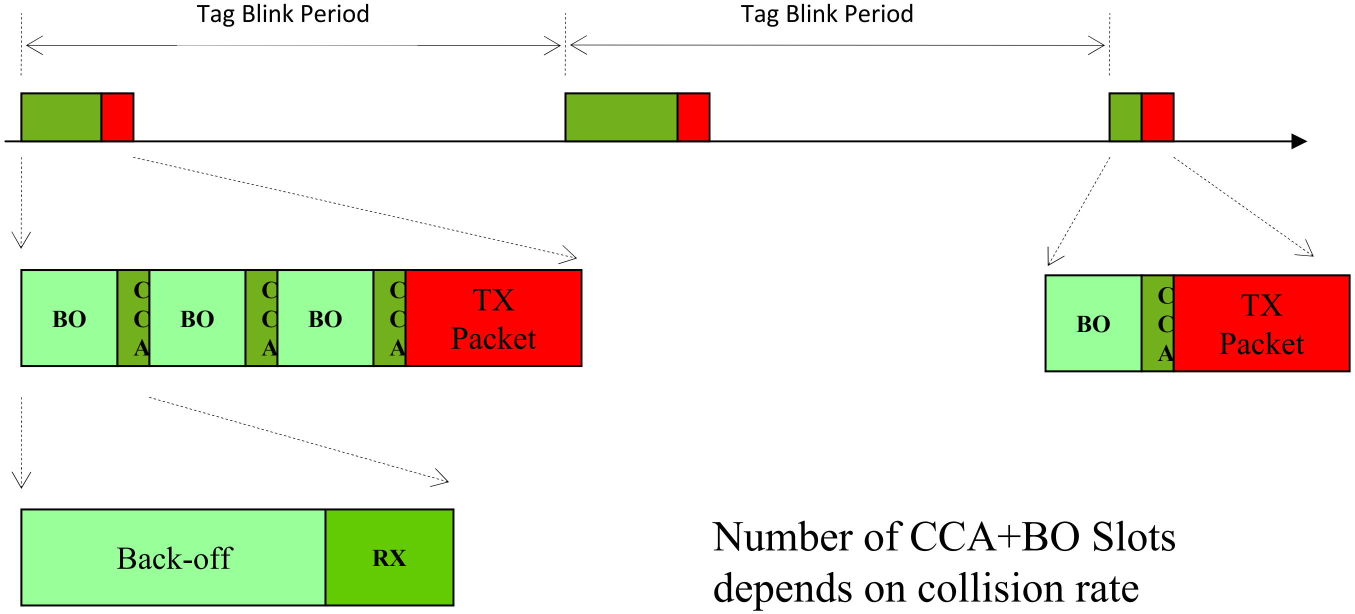
Bi-Directional Tags

- 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 Aaccess

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



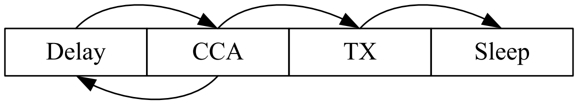
Number of CCA+BO Slots depends on collision rate

CCA-TX Simulation Results

- Assumptions:

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

  - Tag state machine model



CCA-TX Simulation Results (cont'd)

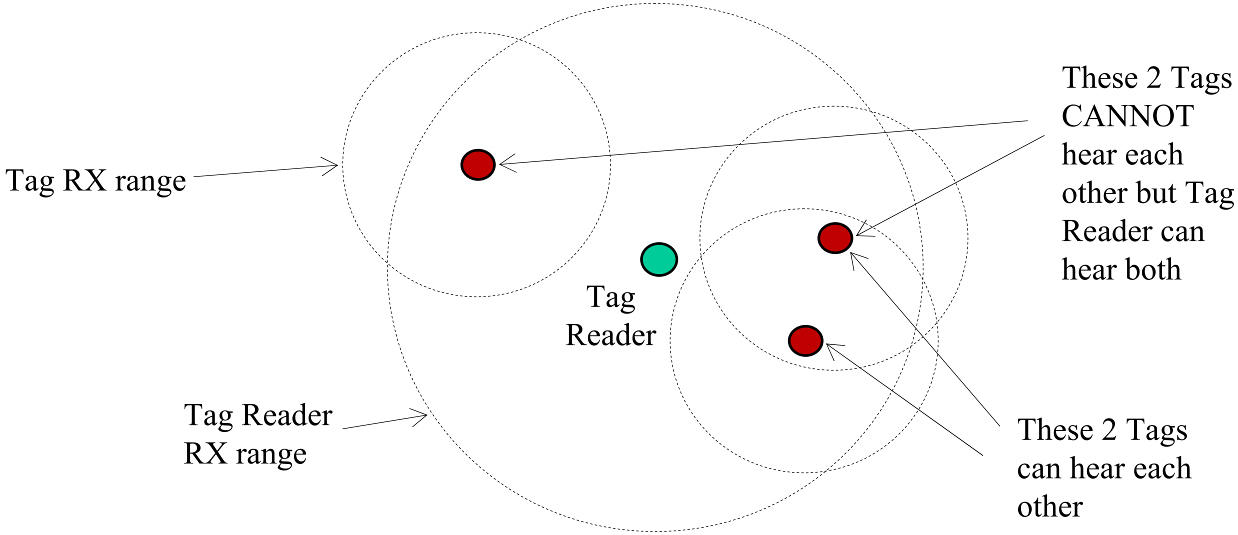
Number of Tags	(BEmin, BEmax)	Collision Rate	Power per blink [µW]	Total time delay (seconds)
100	(6,8)	0.39	6.74	0.10
	(9,11)	0.12	5.69	0.31
	(12,14)	0.01	5.30	1.02
1,000	(6,8)	0.88	8.68	0.28
	(9,11)	0.68	7.97	0.56
	(12,14)	0.07	5.54	2.25
	(15,17)	0.02	5.36	16.9

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

- Highlighted (Be_{min}, Be_{max}) looks reasonably good, but…

A flaw in “CCA before TX” principle

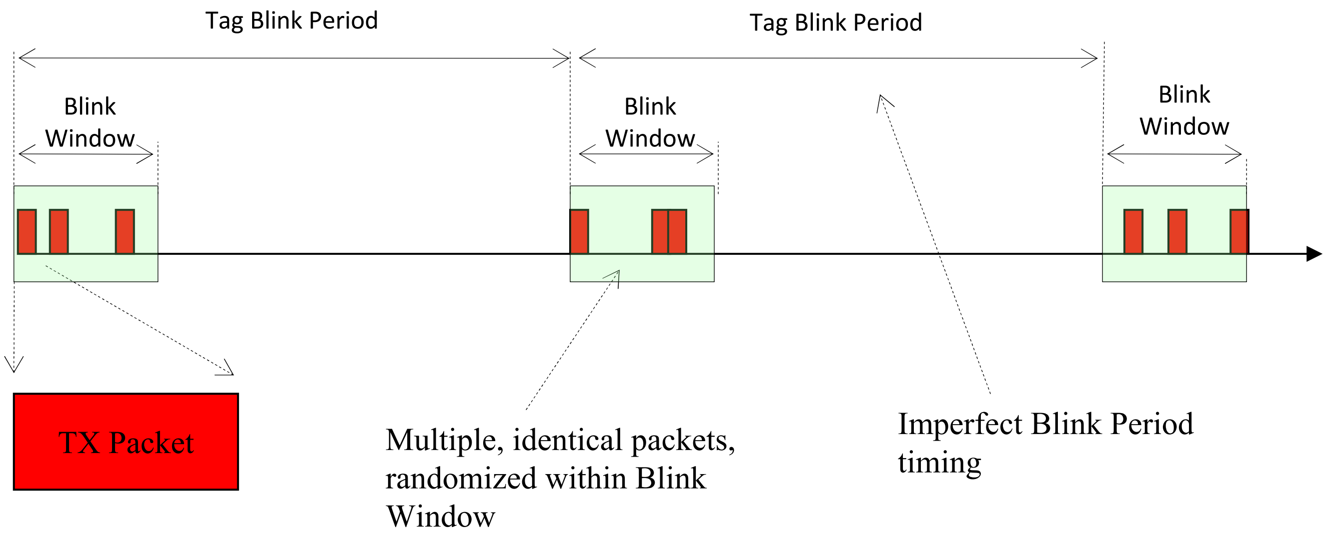
- Tag antenna gain is usually significantly lower than Tag Reader antenna gain (10 - 20 dB or even more)



- 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



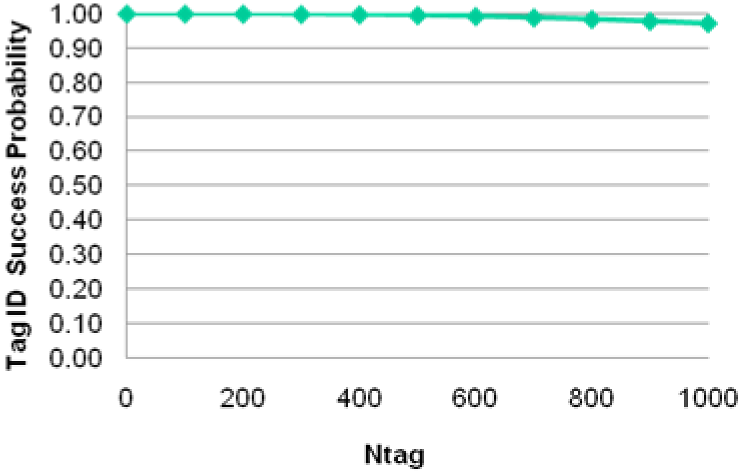
Multiple, identical packets, randomized within Blink Window

Imperfect Blink Period timing

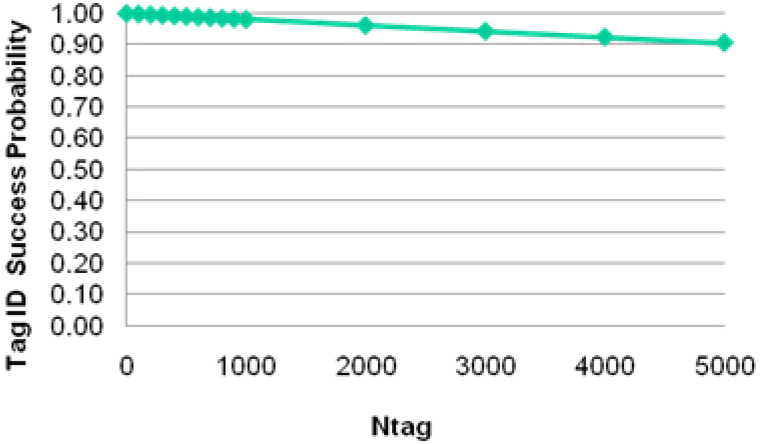
Successful Tag ID Reception Probability of Double P-Aloha

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

Tblink = 10s
Mrepeat = 3



Tblink = 60s
Mrepeat = 1



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

PPDU

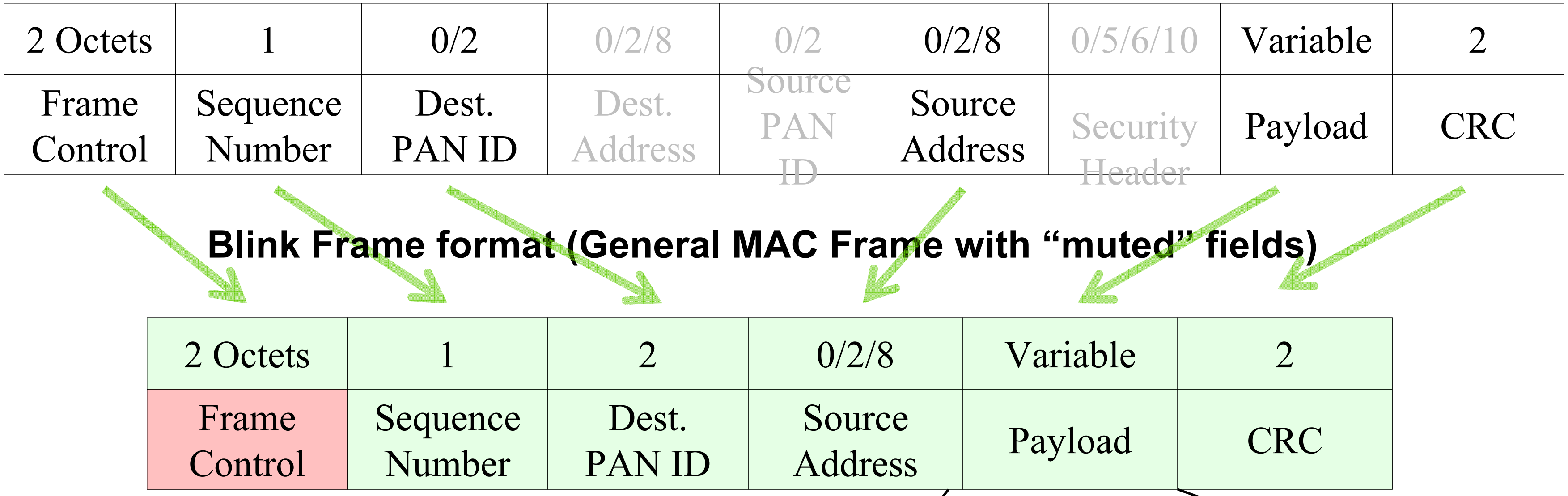
- Small change from classic 15.4
  - Add option to use 1 or 2 byte SFD

4 Octets	1 / **2** Octet	1 Octet		Variable
Preamble	SFD	Length	R	PSDU
Synchronization Header		PHY Header		PHY Payload (MAC Frame)

- 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



2 Octets	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10	Variable	2
Frame Control	Sequence Number	Dest. PAN ID	Dest. Address	Source PAN ID	Source Address	Security Header	Payload	CRC

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

2 Octets	1	2	0/2/8	Variable	2
Frame Control	Sequence Number	Dest. PAN ID	Source Address	Payload	CRC

Optional Fields outside IEEE control

1 Octet	1	Variable	Variable
Device Class	Device Type	Alternative ID	Sensor Data

- Changes to 15.4 MAC
  - New frame – Blink Frame
  - Source Address interpretation change (0 Octets → 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**

New 4e frames

- 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

2 Octets	1	Variable	2
Frame Control	Sequence Number	Payload	CRC

- 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)

64-bit Addressing Blink Frame format

2 Octets	1	2	8	Variable	2
Frame Control	Sequence Number	Source PAN ID	Source Address	Payload	CRC

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

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]

1 Octet	1	1	4
Device Class	Device Type	Tag Status	Tag ID

4 Octets	1	1	2	1	9	2
Preamble	SFD	Length	Frame Control	Sequence Number	Payload	CRC

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

1 Octet	1	1
Device Class	Device Type	Tag Status

4 Octets	1	1	2	1	2	8	3	2
Preamble	SFD	Length	Frame Control	Seq. Number	Source PAN ID	Source Address	Payload	CRC

Thank You!