

# ZigBee IEEE 802.15.4 PHY Layer

Nicolas Billeau, Post-Doc.  
Hassan Aboushady, Associate Professor

## Outline

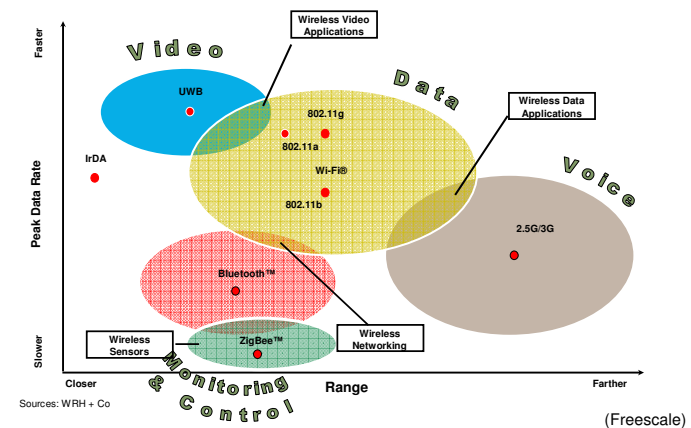
- ZigBee: Applications and Perspective.
- ZigBee Standard.
- IEEE 802.15.4 PHY Layer.

## ZigBee

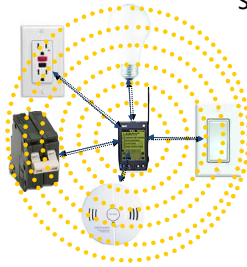
*ZigBee for applications with modest transmission data requirements, and demanding secure communication.*

- Named after Zig-zag movements of bees when pollinating
- **low-power** = long life (+2 y.) with small batteries.
- **low-cost and low-area** = widely deployed in wireless control and monitoring applications.
- **wireless mesh networking** = high reliability and larger range (+65000 nodes) = **Wireless Sensors Networks (WSN)**.
- **vs Bluetooth** = simpler, less expensive and more network capabilities.

## Where Does ZigBee Fit ?

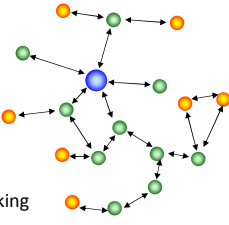


## IEEE 802.15.4 Applications



### Sensors & Controls:

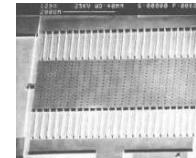
- Home Automation
- Industrial Automation
- Remote Metering
- Automotive Networks
- Interactive Toys
- Active RFID/ asset tracking
- Medical



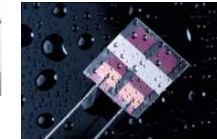
Heterogenous devices communicate through the same protocols.

(ZigBee Alliance)

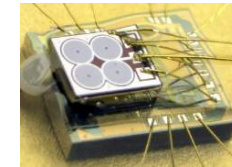
## Sensors



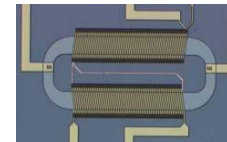
Accelerometer



Humidity

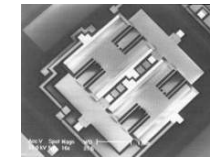


Pressure sensor



Magnetometer

Temperature  
Force  
Chemical  
Bio  
...



Gyroscope

(CEA LETI)

## ZigBee: Building Automation

- Advance Transformer
  - Wireless lighting control
    - Dimmable ballasts
    - Light switches anywhere
    - Customizable lighting schemes
    - Energy savings on bright days
    - Building Management System BMS (DALI)
  - Extendable networks
    - Additional sensors
    - Other networks



(ZigBee Alliance)

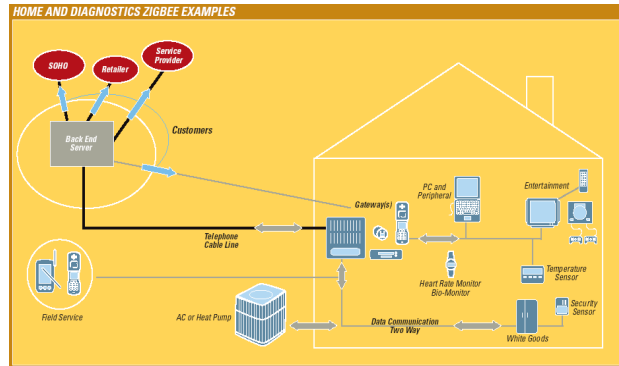
## ZigBee: Asset Management

- Within each container, sensors form a mesh network.
- Multiple containers in a ship form a mesh to report sensor data
- Increased security through on-truck and on-ship tamper detection
- Faster container processing. Manifest data and sensor data are known before ship docks at port.



(ZigBee Alliance)

## ZigBee: Home RF



(Freescale)

N. Belleau and H. Aboushady

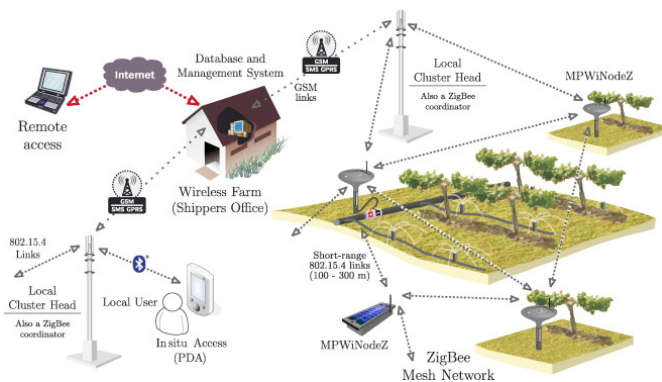
## ZigBee: Agriculture



(Journal of Computers and Electronics in Agriculture, Elsevier)

N. Belleau and H. Aboushady

## ZigBee: Agriculture



(Journal of Computers and Electronics in Agriculture, Elsevier)

N. Belleau and H. Aboushady

## ZigBee Perspective

- 2007: **7 millions** units shipped.
- 2012: **292 millions** units shipped (much higher ?).
- Bluetooth:
  - 2007: **800 millions** units shipped.
  - 2012: **1850 millions** units shipped.

(In-Stat previsions)

### Wireless Sensor Network:

- R&D: 1.3 billions \$ in 2012.
- Science Found.: #400 projects in 2008.
- EU funding: 1 billion \$ 2008/2012.

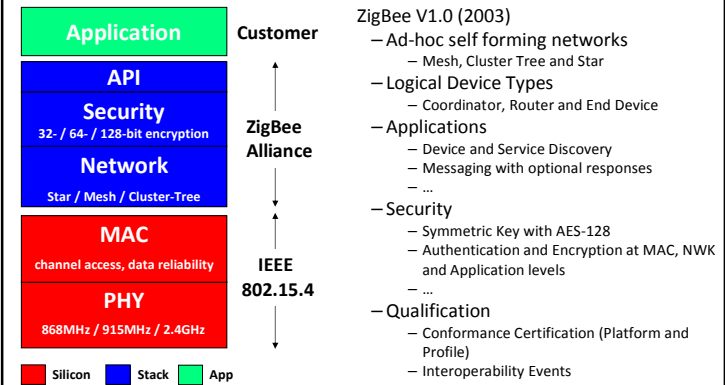
(ON World report)

N. Belleau and H. Aboushady

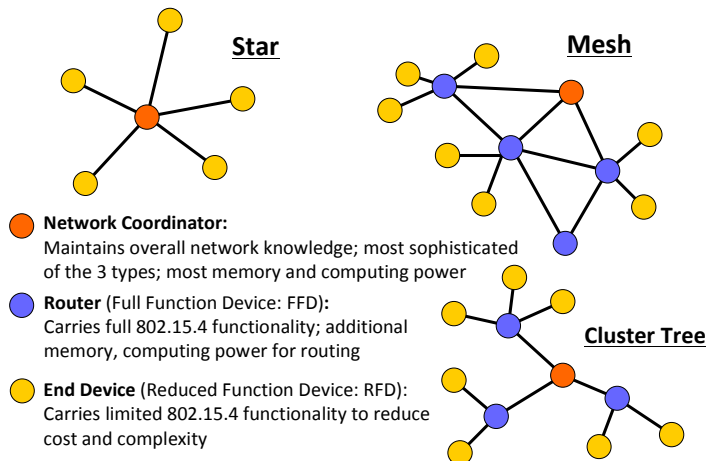
## Outline

- ZigBee: Applications and Perspective.
- ZigBee Standard.
- IEEE 802.15.4 PHY Layer.

## ZigBee Features Set



## ZigBee Network Topologies



## ZigBee Nodes Communication

Based on **IEEE 802.15.4** standard:

- Transmission Range of 30-100+ Meters
- Channel Access is via CSMA-CA or optional time slotting.
- Message acknowledgement or an optional beacon structure.
- Multi-level security.
- 3 bands, 27 channels specified:
  - 2.4 GHz: 16 channels, 250 kbps
  - 868.3 MHz : 1 channel, 20 kbps
  - 902-928 MHz: 10 channels, 40 kbps
- Works well for
  - Long battery life, selectable latency for controllers, sensors, remote monitoring and portable electronics

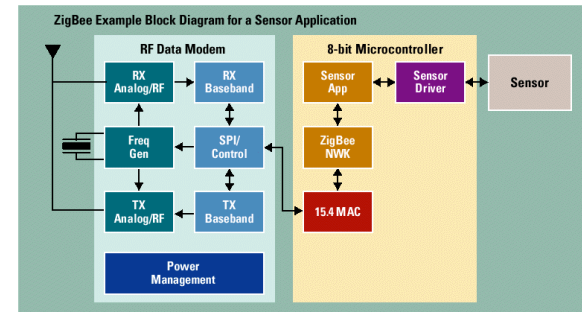
## 802.15.4 Channel Access Mechanisms

- **CSMA-CA** (Carrier Sense Multiple Access-Collision Avoidance):
  - performs a clear channel assessment (CCA):
    - measures the spectral energy in the frequency channel of interest (Energy Detection).
    - or detects the type of the occupying signal (Carrier Sense).
  - if no channel available, wait for a random time and retry.
  - waits for ack. to verify packet reception at other end.
- **BEACON-Enabled Networking**
  - Coordinator dedicates a specific time slot to a particular device (Guaranteed Time Slot: GTS).
  - Beacon is a message with specific format sent by the coordinator to synchronize the nodes in the network.
  - Dedicated bandwidth and low latency
  - Wake-up only for synchronization

N. Beilleau and H. Aboushady

IEMC 17

## Integration of IEEE 802.15.4 / ZigBee



3 types of devices (Coordinator, FFD, RFD) can be implemented with this architecture and powered by a AAA battery:

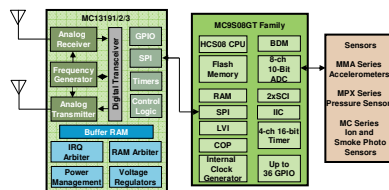
- Full protocol stack < 32 k
- Simple node-only stack ≈ 4k
- Coordinators require extra RAM (node device database, transaction table, pairing table)

N. Beilleau and H. Aboushady

IEMC 18

## Freescal 802.15.14 Radio Example

- Key Features
  - IEEE® 802.15.4 Compliant
    - 2.4GHz
    - 16 selectable channels
    - 250Kbps Data Rate
    - 250Kbps 0-QPSK DSSS
  - Multiple Power Saving Modes
    - Hibernate 2.3uA
    - Doze 35uA
    - Idle 500uA
  - RF Data Modem
    - Up to 7 GPIO
    - SPI Interface to Micro
    - Internal Timer comparators (reduce MCU resources)
    - -16.6dBm to +3.6dBm output power
      - Software selectable
      - On-chip regulator
    - Up to -92 Rx sensitivity at 1% PER



N. Beilleau and H. Aboushady

IEMC 19

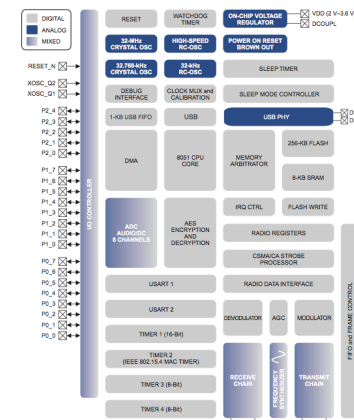
## TI CC2531: SoC ZigBee/802.15.4

### Features:

- IEEE 802.15.4 PHY/MAC
- ZigBee Stack
- USB controller

### Performance:

- Power Cons. = 40 mA
- RX Sensitivity = -97 dBm
- TX Power = 4.5 dBm
- surface = 6mm x 6mm



N. Beilleau and H. Aboushady

IEMC 20

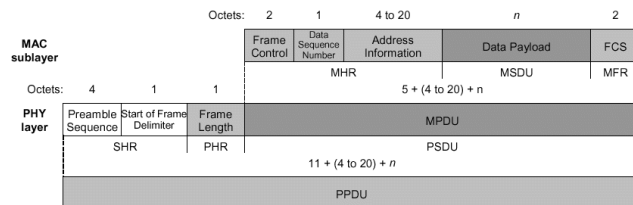
## Outline

- ZigBee: Applications and Perspective.
- ZigBee Standard.
- IEEE 802.15.4 PHY Layer.

## IEEE 802.15.4 PHY Layer

- 3 bands, 27 channels specified:
  - 2.4 GHz (ISM/Worldwide) : 16 channels, 250 kbps
  - 868.3 MHz (ISM/Europe) : 1 channel, 20 kbps
  - 902-928 MHz(ISM/Americas): 10 channels, 40 kbps
- Channels spacing: 5 MHz
- Coding: Direct Sequence Spread Spectrum
- Modulation: Offset-QPSK
- Tx Maximum Output Power > -3 dBm (adj. 30 dB)
- Rx Sensitivity < -85 dBm for a PER of 1%

## PHY Layer Data Frame format

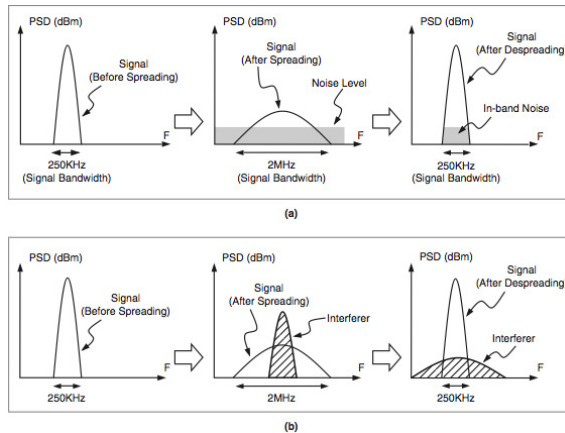


- Data Rate = 250 kbps for 2.4 GHz ISM band.
- Preamble sequence (32 binary 0) used for receiver timing recovery.
- SFD indicates end of the synchronization field.
- Frame length indicates the size of the PSDU.
- Average size of PPDU = 22 bytes = 176 bits.
- PER=1% => BER=5.7e-5

## Direct Sequence Spread Spectrum

- Improves the receiver sensitivity level, increases the jamming resistance, and reduces the effect of the multipath.
- 1 chips sequence/symbol (4 bits) => 16 chips sequences.
- minimize the similarity of each sequence to the other 15 sequences (quasi-orthogonals = low cross-correlation).
- sequences of 32 chips @ 2 Mcps => signal spectrum spread on a larger band then modulation performance based on it.
- de-spreading at receiver concentrates signal energy on a smaller frequency band to increase the final SNR.
- Processing Gain =  $10 \log_{10}(2M/250k) \approx 9$  dB

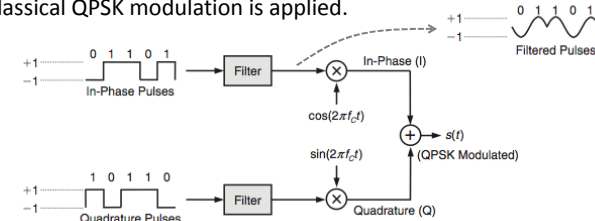
## Direct Sequence Spread Spectrum



(Farahani, ZigBee Wireless Network and Transceiver)

## Offset Quadrature Phase Shift Keying

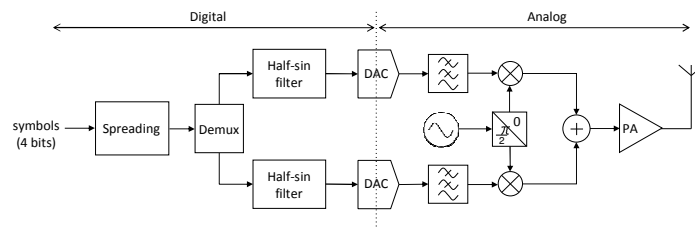
- Q chips are delayed of a Tchip period from I chips.
- chips are processed by a half-sin filter.
- classical QPSK modulation is applied.



- equivalent to an MSK modulation with only phase transitions of  $\pi/2$  and spectrum with a lower and wider main lobe.
- performance are equivalent to a QPSK modulation.

(Farahani, ZigBee Wireless Network and Transceiver)

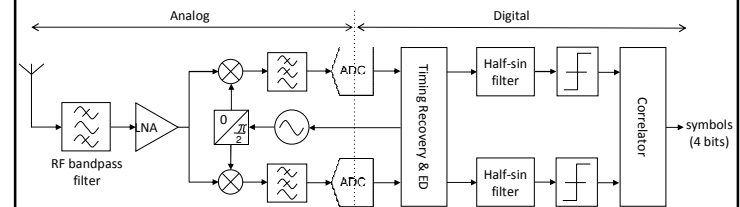
## IEEE 802.15.4 Transmitter



- Several types of transmitter (direct conversion, IF conversion, PLL).
- Direct conversion is simple, low cost and adapted for integration.
- Leakage between LO and PA is an issue.

N. Beilleau and H. Aboushady

## IEEE 802.15.4 Receiver



- Leakage between LO and LNA is an issue.
- Flicker Noise and DC offset can lead to have a complex analog part.
- 8 symbols for Timing Recovery.

N. Beilleau and H. Aboushady

## References

1. ZigBee Alliance, <http://www.zigbee.org>
2. SystemC-AMS, <http://www.systemc-ams.org>
3. S. Farahani, "ZigBee Wireless Networks and Transceivers", Newnes Edition.
4. R.M. Koteng, "Evaluation of SDR-implementation of IEEE 802.15.4 Physical Layer", Master Thesis, Norwegian University of Science and Technology.
5. Seo et al, "System Design Considerations for a ZigBee RF Receiver with Regard to Coexistence with Wireless Devices in the 2.4 GHz ISM-band", KSII Transactions on Internet and Info. Systems, 2008.
6. J.C. Rudell, "An Integrated GSM/DECT Receiver: Design Specifications", BWRC.
7. Chipcon, "CC2420, 2.4 GHz IEEE 802.15.4/ZigBee-ready RF Transceiver", Datasheet.
8. Texas Instrument, "A USB Enabled System-On-Chip Solution for 2.4-GHz IEEE 802.15.4 and ZigBee Applications", Datasheet.

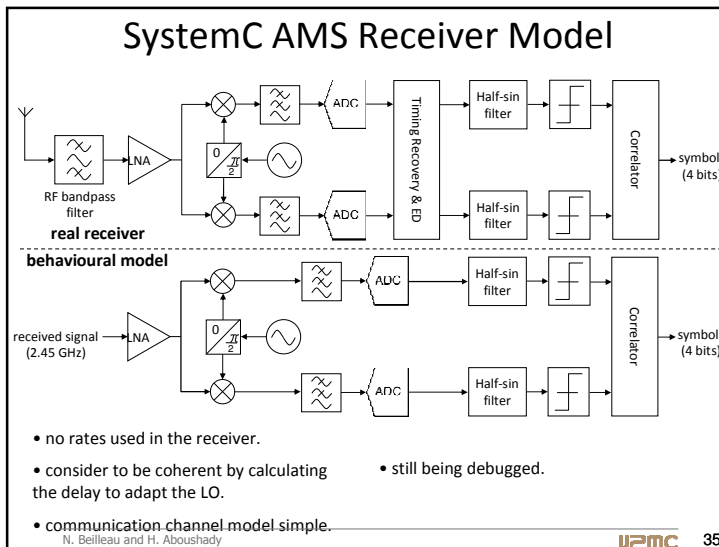
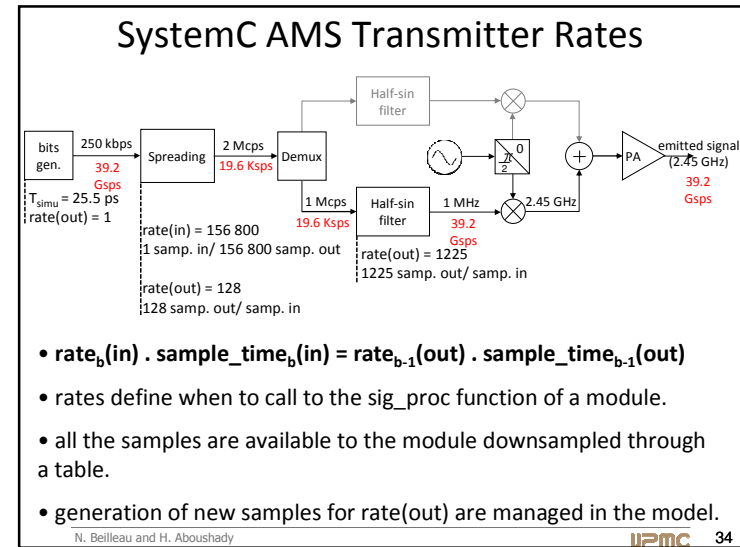
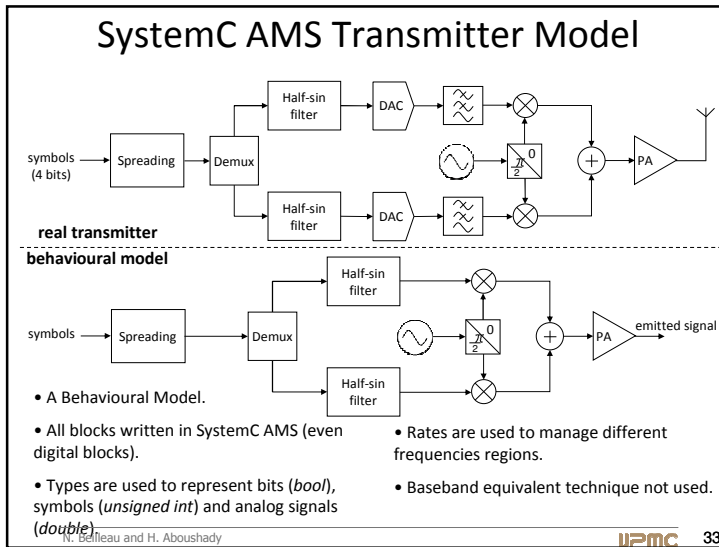
Thank you for your attention

## Backup

## Outline

- ZigBee: Applications and Perspective.
- ZigBee Standard.
- IEEE 802.15.4 PHY Layer.





### Simulators Comparison

- just thoughts on the 3 tools I used to do the same model.
- nothing quantitative.

	MATLAB	Simulink	SystemC AMS
Model Writing	model based on matrices: needs to manage all the data.	the most intuitive and easy to use	like Matlab, no graphic representation to make it intuitive and code writing.
Simulation Speed	Matlab scripts are limited by the memory management	needs to work on it to have a « fast » simulation	comparable to Latex: more efforts but gives almost the best results at the first run !

N. Belleau and H. Aboushady I2PMC 36

## ZigBee: Overview

- **Specifications Managed by the ZigBee Alliance**
  - Global consortium of OEMs, IC vendors & tech companies
  - Specify device, network and service discovery / pairing
- **Defining Star, Mesh & Cluster-Tree Networks**
  - Allows users to balance system cost, reliability & battery life
- **Defining Security Management**
  - Extends 32-, 64- & 128-bit AES encryption of 802.15.4
- **Defining Application Profiles & Brand Compliance**
  - Ensures product & application interoperability (e.g., AMR & DSM)

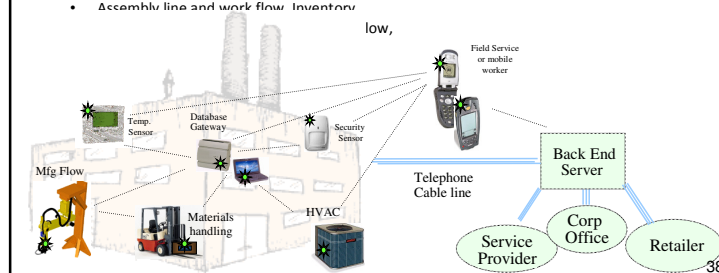
37

## Industrial/Commercial Spaces

- Warehouses, Fleet management, Factory, Supermarkets, Office complexes
- Gas/Water/Electric meter, HVAC
- Smoke, CO, H<sub>2</sub>O detector
- Refrigeration case or appliance
- Equipment management services & Preventative maintenance
- Security services
- Lighting control
- Assembly line and work flow

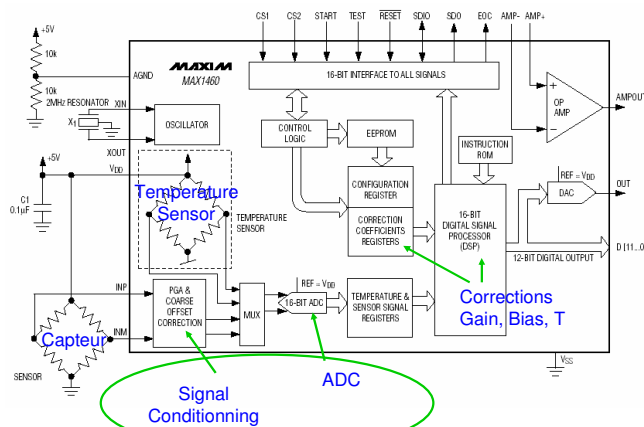
Energy, diagnostics, e-Business services

- **Gateway or Field Service links to sensors & equipment**
  - Monitored to suggest PM, product updates, status changes
- **Nodes link to PC for database storage**
  - PC Modem calls retailer, Service Provider, or Corp headquarters
  - Corp headquarters remotely monitors assets, billing, energy management



38

## Sensor Interfaces



(CEA LETI)

H. Aboushady

ASTECAS Meeting 17/11/2011

Confidential

IAPMC 39

## Wireless Networking Standards

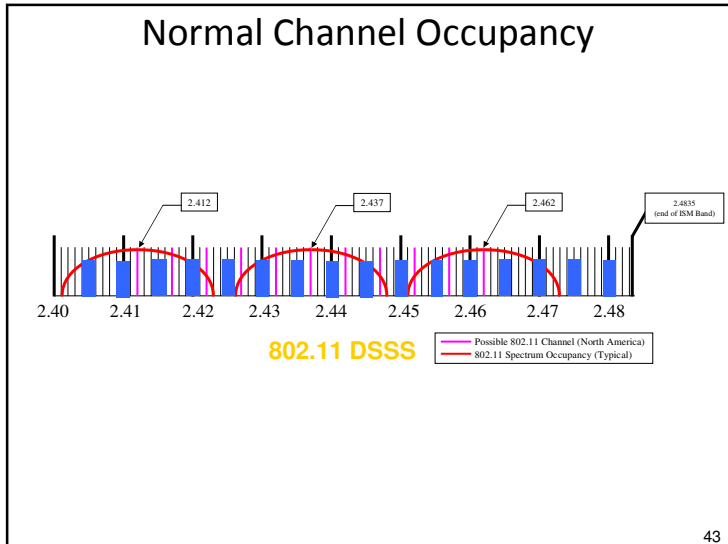
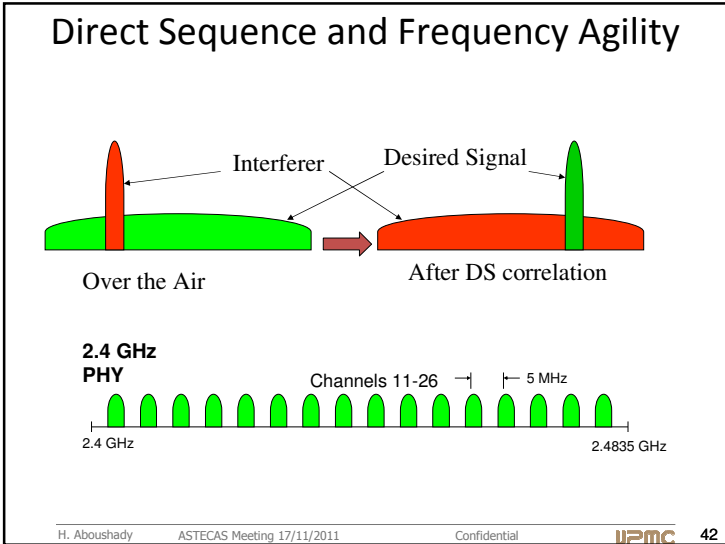
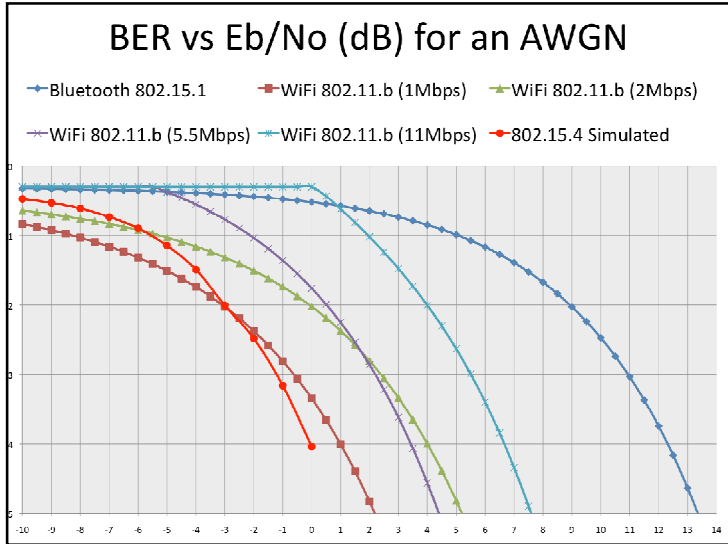
Market Name	GPRS/GSM	Wi-Fi™	Bluetooth™	ZigBee™
Standard	1xRTT/CDMA	802.11b	802.15.1	802.15.4
Application Focus	Wide Area Voice & Data	Web, Email, Video	Cable Replacement	Monitoring & Control
System Resources	16MB+	1MB+	250KB+	4KB - 32KB
Battery Life (days)	1-7	.5 - 5	1 - 7	100 - 1,000+
Network Size	1	32	7	255 / 65,000
Bandwidth (KB/s)	64 - 128+	11,000+	720	20 - 250
Transmission Range (meters)	1,000+	1 - 100	1 - 10+	1 - 100+
Success Metrics	Reach, Quality	Speed, Flexibility	Cost, Convenience	Reliability, Power, Cost

H. Aboushady

ASTECAS Meeting 17/11/2011

Confidential

IAPMC 40



- ### 15.4 Protocol Built for the Mission
- 15.4 Protocol was developed for very different reasons than Bluetooth
    - 802.15.4
      - Very low duty cycle, very long *primary* battery life applications as well as mains-powered
      - Static and dynamic mesh, cluster tree and star network structures with potentially a very large number (>>65534) of client units, low latency available as required
      - Ability to remain quiescent for long periods of time without communicating to the network
    - Bluetooth
      - Moderate duty cycle, secondary battery operation where battery lasts about the same as master unit
      - Wire replacement for consumer devices that need moderate data rates with very high QoS and very low, guaranteed latency
      - Quasi-static star network structure with up to 7 clients (and ability to participate in more than one network simultaneously)
      - Generally used in applications where either power is cycled (headsets, cellphones) or mains-powered (printers, car kits)
  - Protocol differences can lead to tremendous optimizations in power consumption

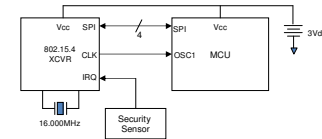
## 15.4/ZigBee and Bluetooth

- Instantaneous Power Consumption
  - 15.4 Transceivers are "similar" to Bluetooth Transceivers
    - 802.15.4
      - O-QPSK with shaping
      - Max data rate 250kbps over the air
      - 2Mchips/s over the air Direct Sequence Spread Spectrum (62.5ksp\*32 spread)
      - 92 dBm sensitivity nominal
      - 40ppm xtal
    - Bluetooth
      - FSK
      - Max data rate 720kbps over the air
      - 1Msp/s over the air Frequency Hop Spread Spectrum (79 channels @ 1600 hps)
      - 83 to -84 dBm sensitivity nominal
      - 20ppm xtal
- Instantaneous power consumption will be similar for the raw transceivers without protocol
- Bluetooth's FHSS makes it impractical to create extended networks without large synchronization cost

45

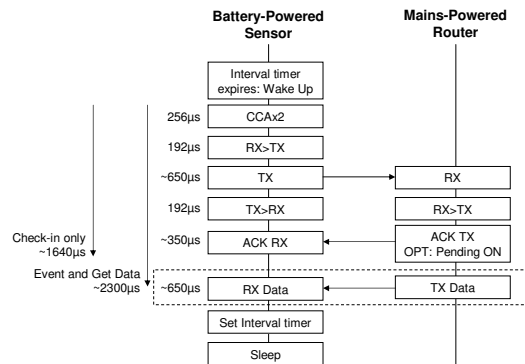
## Peel-n'-Stick Security Sensors

- Battery Operation
  - 2 AA Alkaline or 1 Li-AA cell
- 802.15.4/ZigBee Mode
  - Non-beacon network environment
- Sensor process
  - RC Oscillator waking up MCU and doing network check-in at some interval
    - Many security systems have between ~10 second and ~15 minute requirement
  - On a sensor event, device immediately awakens and reports in to network



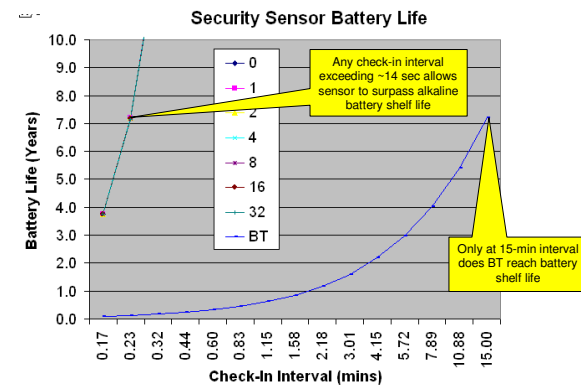
46

## Security Sensor Timing



47

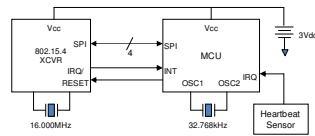
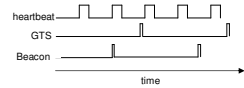
## 802.15.4 Security Sensor



48

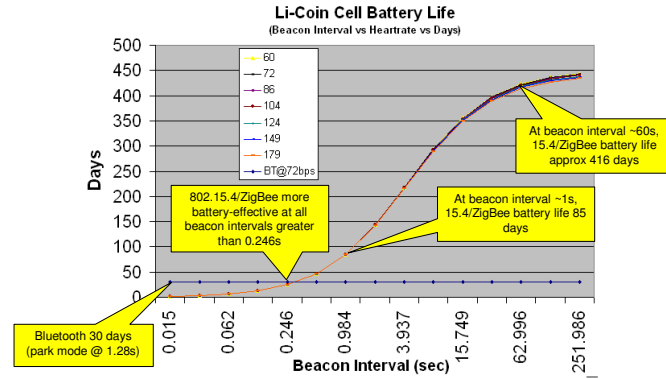
## Body-Worn Medical Sensors

- Heartbeat Sensor
  - Battery-operated using CR2032 Li-Coin cell
- 802.15.4/ZigBee Mode
  - Network environment using Guaranteed Time Slot (GTS)
  - Network beacons occurring either every
    - 960ms or 61.44s (closest values to 1 and 60 s)
- Sensor has two ongoing processes
  - Heartbeat time logging
  - Transmit heartrate and other information (8 bytes total)
    - Instantaneous and average heart rate
    - Body temperature and battery voltage



49

## 802.15.4/ZigBee vs Bluetooth



50