ZigBee™ Alliance

Wireless Control That Simply Works

Designing a ZigBee Network

ESS 2006, Birmingham

David Egan

Ember Corporation

ember

ZigBee™ Alliance

Contents: Typical Network Design Issues

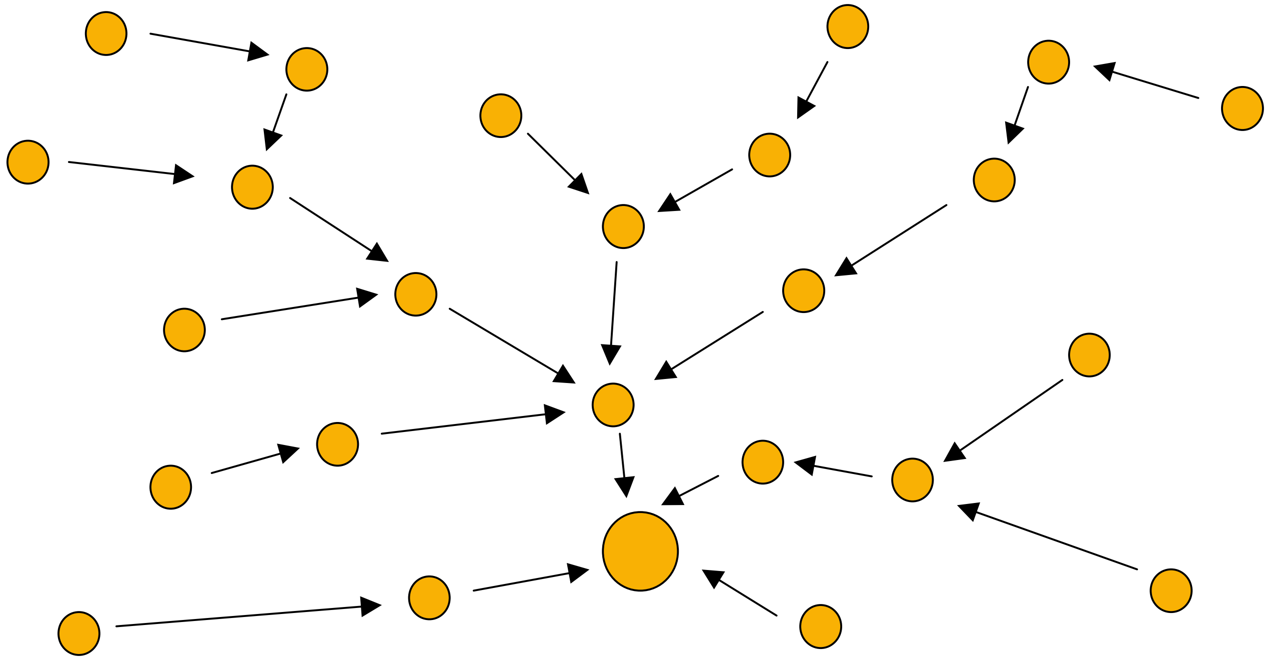
- Traffic Patterns in different applications
  - Bandwidth, Latency, Reliability
  - Data Throughput in a ZigBee network
- Handling Interference with 802.11
  - Interference Detection and Channel Change
- Asymmetric Links
- Choosing Single Chip vs Dual-chip Solutions

ZigBee™ Alliance

Traffic Requirements of Applications

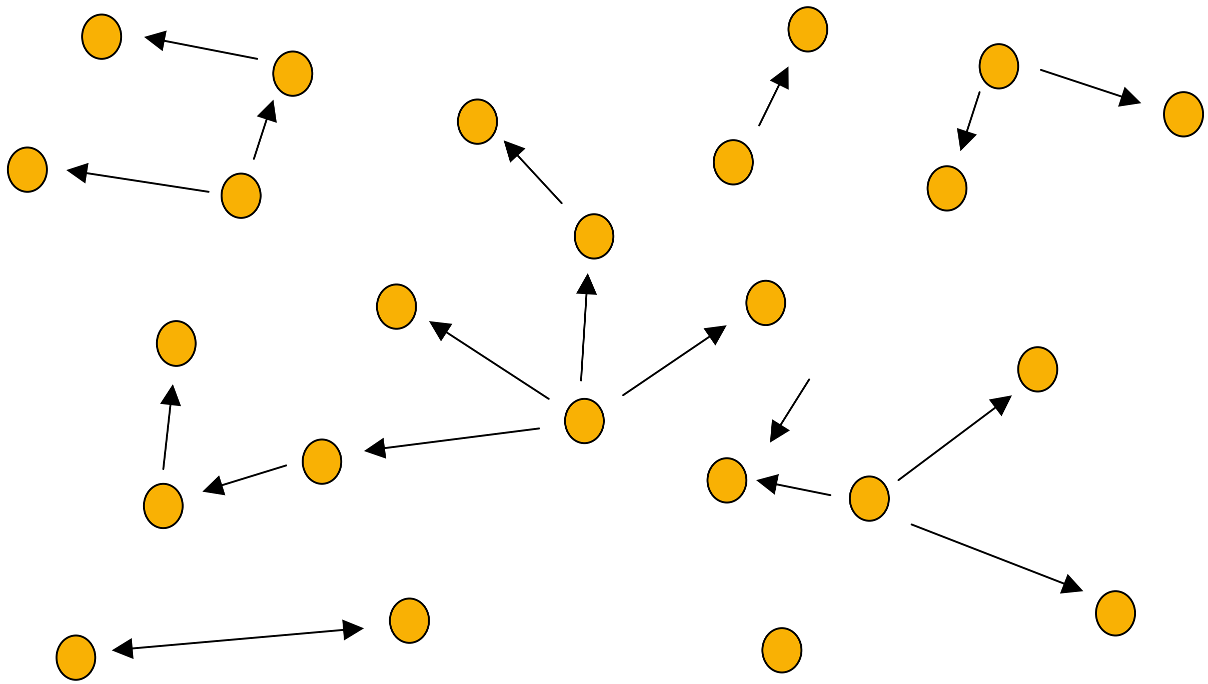
- Bandwidth
  - Estimate message sizes, frequency
  - Identify high bandwidth nodes
  - Be conservative – ensure a margin. Actual throughput can vary with number of hops, security, retries, from 46kbps to 15kbps.
- Latency
  - Estimate minimum latencies
  - Estimate path lengths
  - Conservative approximation: 10-15ms/hop in quiet networks
- Reliability
  - Depends on latency, traffic
  - High latencies and low traffic mean high reliability is easy

Network Patterns: Sensor



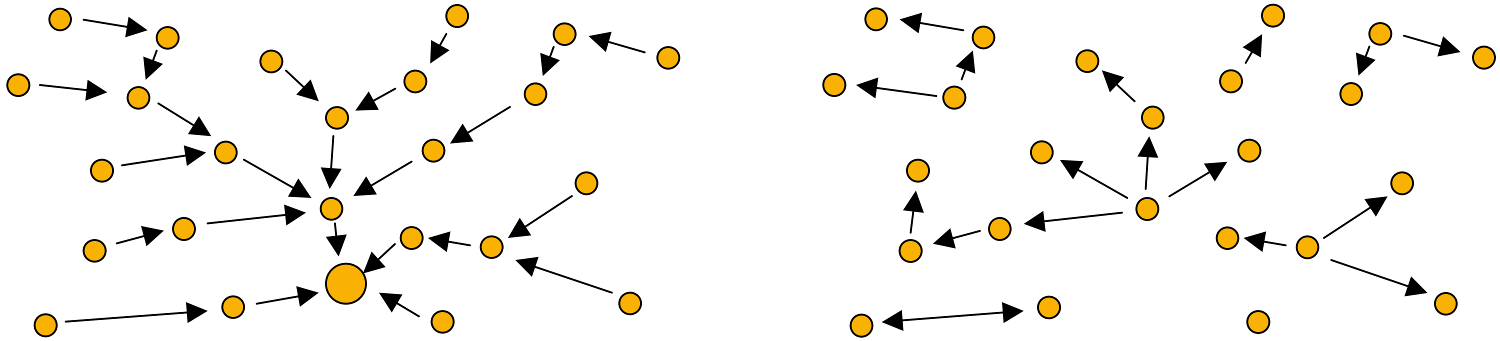
- Most data flows in to central “gateway” device
- Occasional data flows from gateway device to outlying devices
- Data almost never flows between adjacent devices

Network Patterns: Control



- May be no central “gateway” node
- Data often flows from a local control node to a nearby actuator node
- Data almost never flows long distances across the network

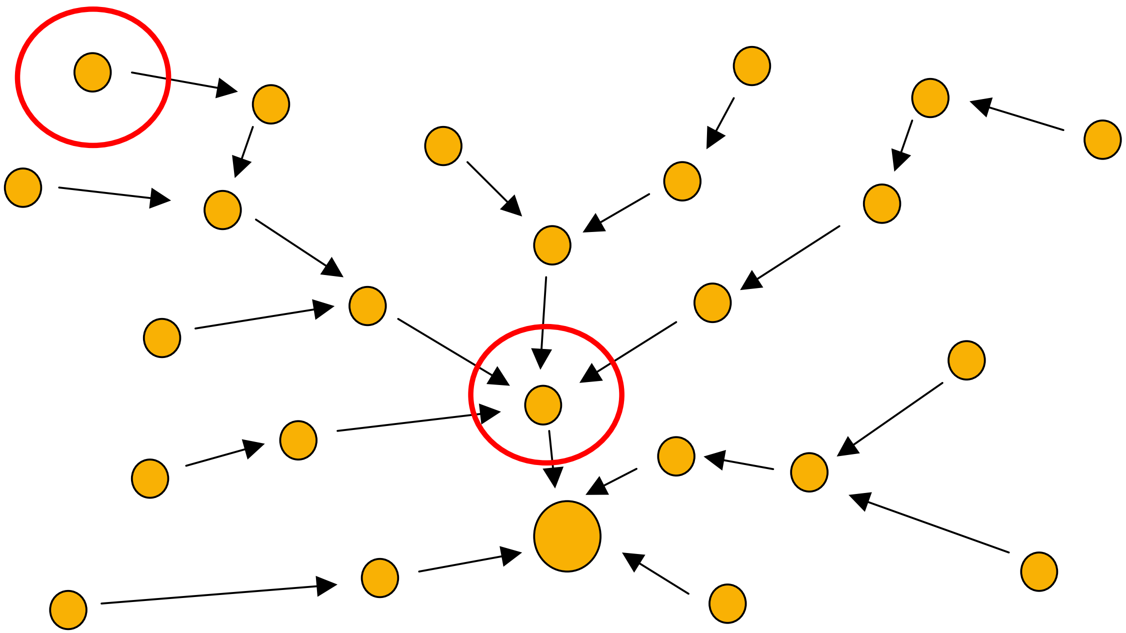
Network Patterns: Lessons



- The same physical topology results in very different results for bandwidth usage, latency
- The networks experience different failure modes
- Networks may be a combination of the two

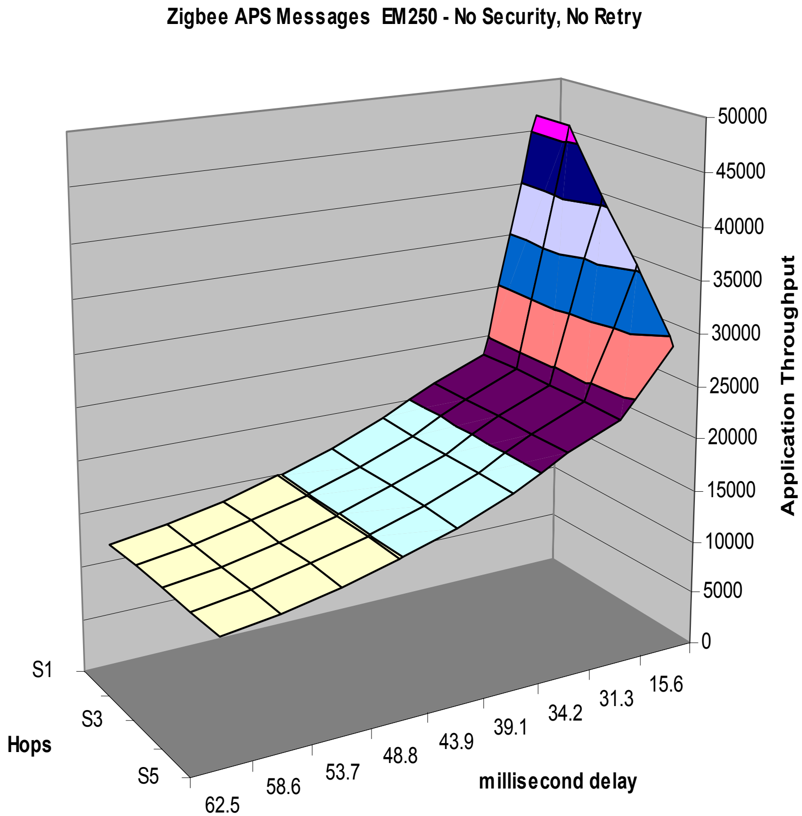
ZigBee™ Alliance

Bandwidth and Topology



- Even identical devices may experience different loading!
- Bandwidth must be estimated as the maximum *total* passing through a device: NB: leave a margin!

Typical Throughput – APS Messages

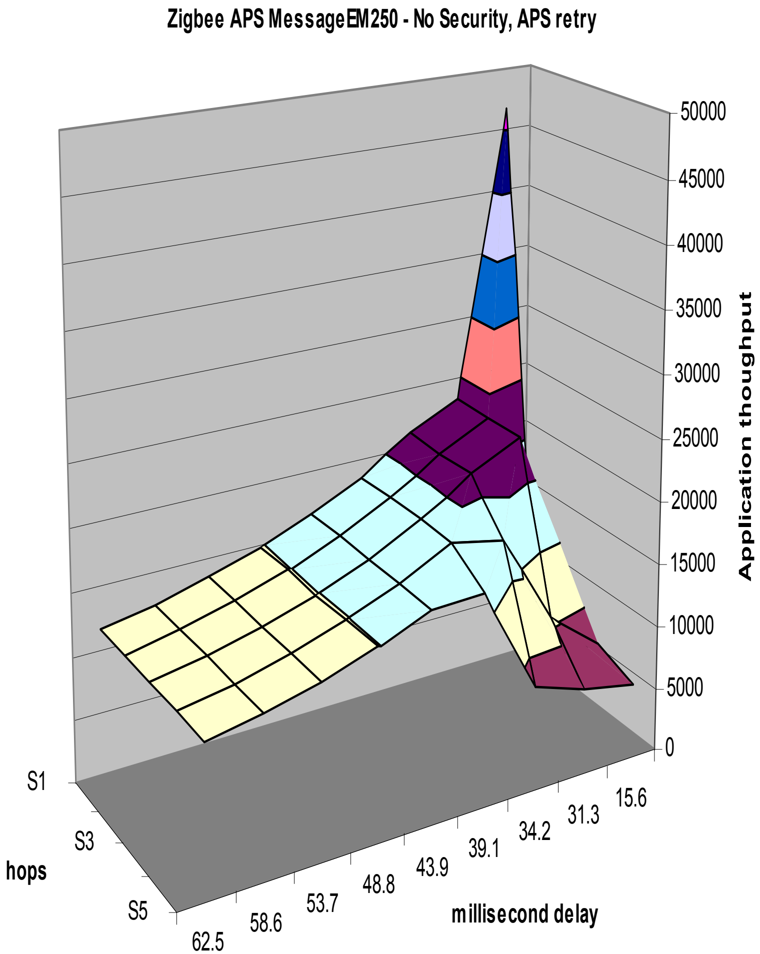


Throughput –
Data is for 91 byte payload
Highest throughput at single hop smallest interpacket delay
Peaks at 46 kbps for application throughput

Performance drops after 2 hops due to packet loss
Even at 5 hops, performance is higher than 25 kbps

Note: Throughput is based on expected throughput given the interpacket spacing and adjusted based on percent of successful packets from the test

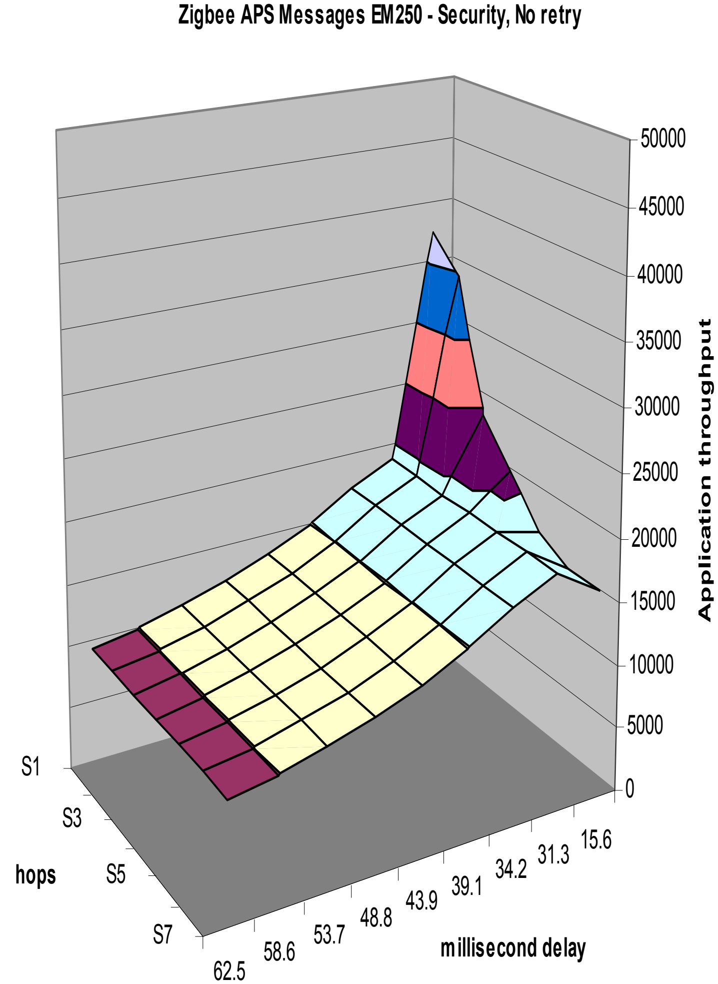
Typical Throughput – Adding APS Reply



Throughput –
Data is for 91 byte payload
Highest throughput at single hop with smallest interpacket delay
Peak remains at 46 kbps for application throughput

Performance drops quickly as reply consumes additional bandwidth
There is a throughput penalty for knowing if message was delivered

Typical Throughput – Adding Security



Throughput –
Data is for 73 byte payload (reduced maximum payload due to security)
Highest throughput at single hop smallest interpacket delay
Peaks at 37 kbps for application throughput

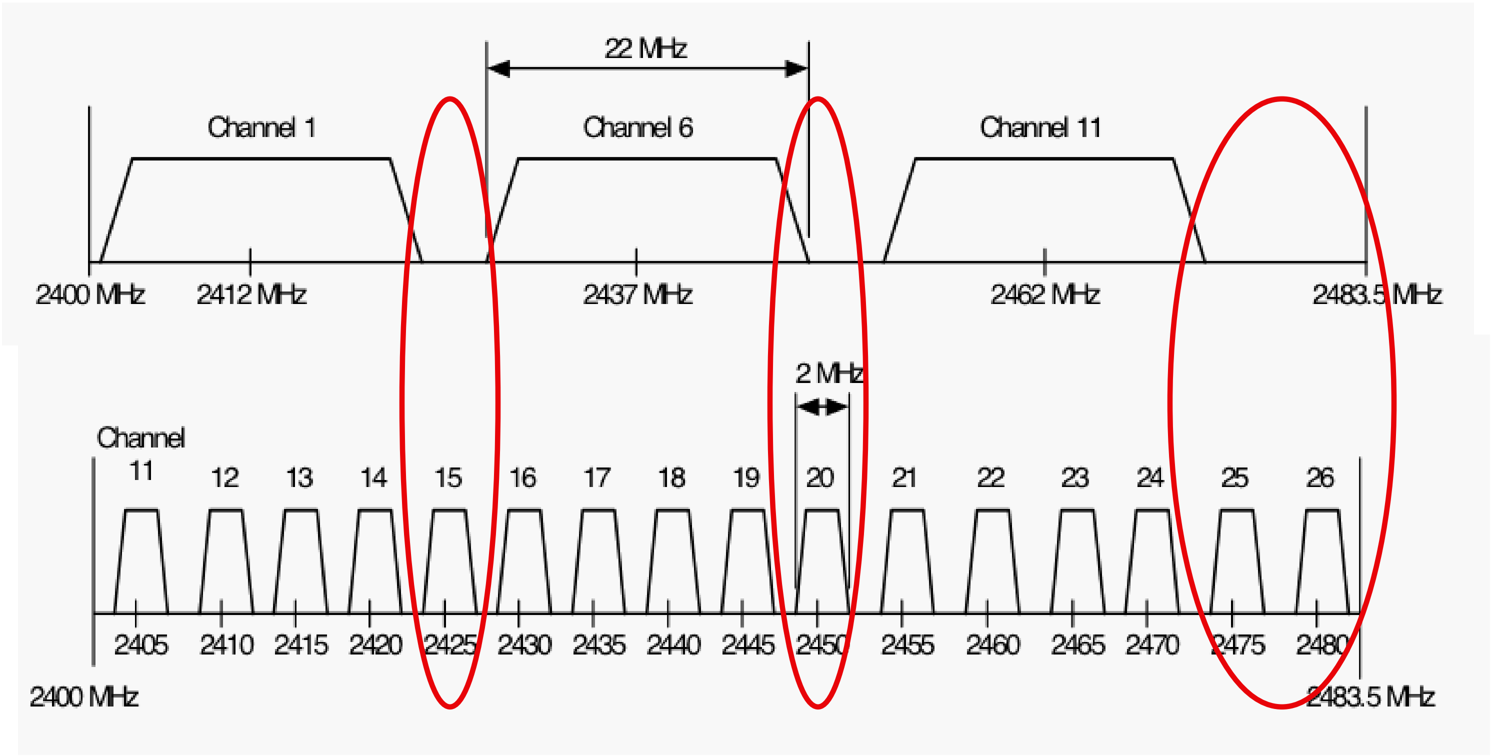
Smaller max payload decreases maximum throughput
Performance drops after 2 hops due to packet loss
Even at 7 hops, performance is higher than 15 kbps

15.4/.11 Channel Allocation - US

US

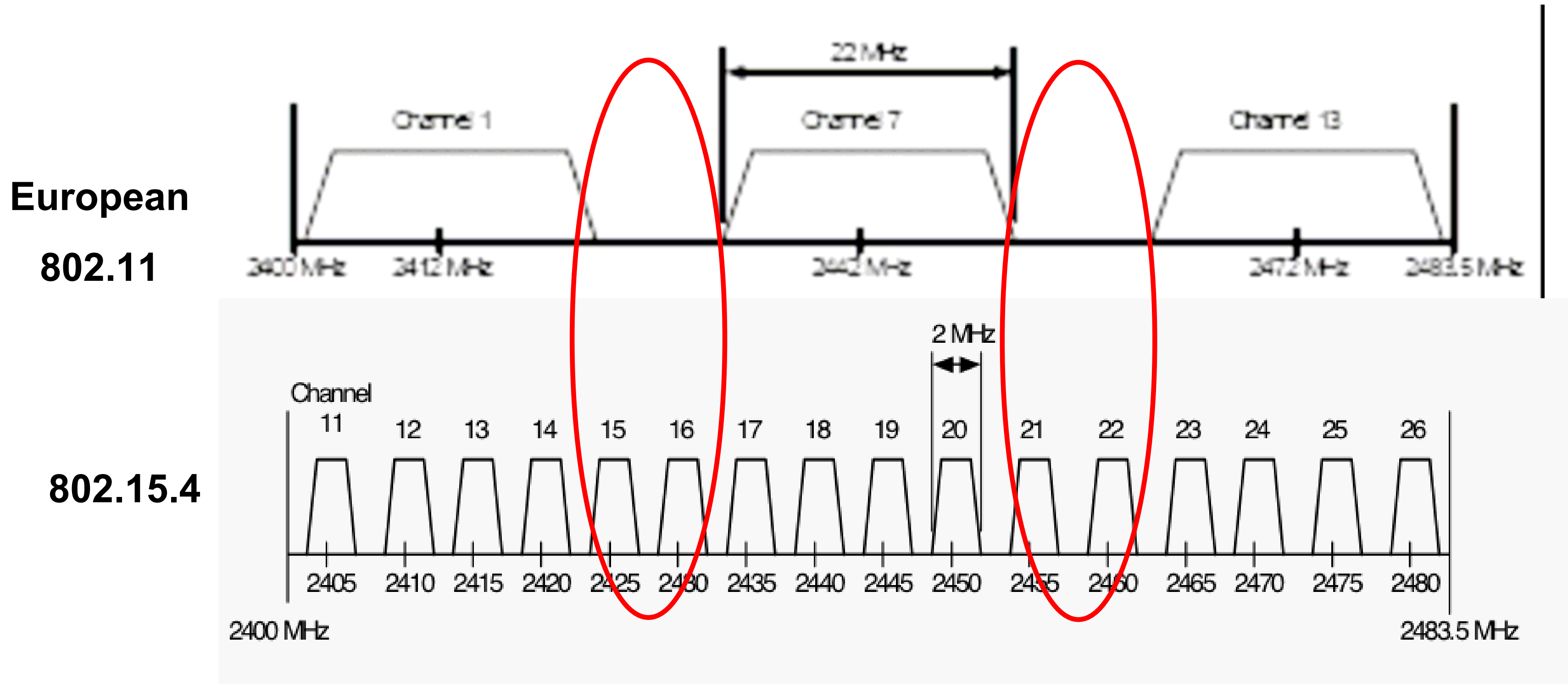
802.11

802.15.4



- Some 15.4 channels are better than others even in a fully populated .11 network – 11, 15, 20, 25 and 26 best in US.
- Doesn't help in unmanaged .11 networks

15.4/.11 Channel Allocation - Europe



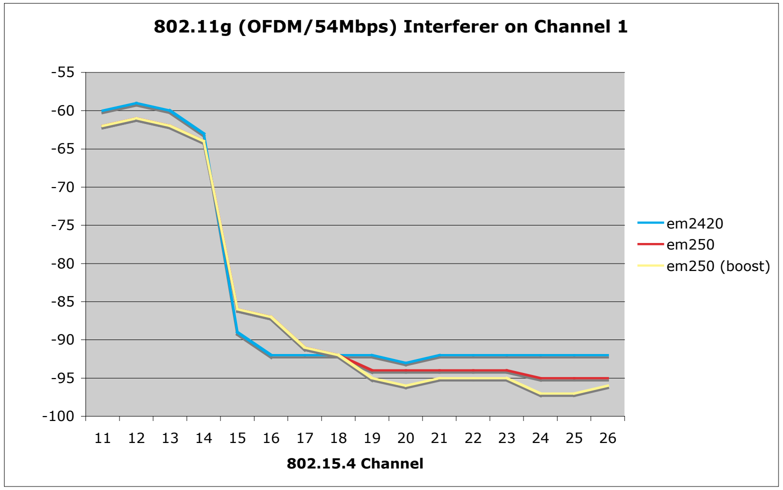
- Some 15.4 channels are better than others even in a fully populated .11 network: 15, 16, 21, 22 in Europe
- Doesn't help in unmanaged .11 networks

ZigBee™ Alliance

Avoiding 802.11 Interference

- 4 Main Objectives
  - Start with the best link budget possible for your application
    - Maximize output power
    - Get the best performing receiver you can
  - Maximise distance from 802.11 interference to ZigBee devices
  - Maximise frequency separation between 802.11 and ZigBee networks
  - Ensure you have enough time-separated retries - if no NWK retries present, make sure your application retries (APS or self-created)

Getting the Best Link Margin



- There are two main factors in getting the best link margin
  - TX Power
  - Receiver sensitivity/immunity to interference
- TX Power - battery life, cost, and design complexity - on-chip vs off-chip PA
- Receiver - performance tradeoffs are built in by vendor - can be tough to extract from datasheets
- Antenna - a factor if you also control the 802.11 radio

Maximising Frequency Separation

- The best technique by far for protecting against 802.11 interference appears to be maximizing the frequency separation of the ZigBee and 802.11 channels
- Two main techniques
  - Active deployment/installation control of both ZigBee and 802.11 channels
    - Offers the best flexibility for maximizing ZigBee and 802.11 density
    - May be possible in some buildings
  - Automatic channel selection
    - At network start, automatically detect and avoid 802.11
    - During operation, move the network if needed

ZigBee™ Alliance

Dealing with Interference: Detection

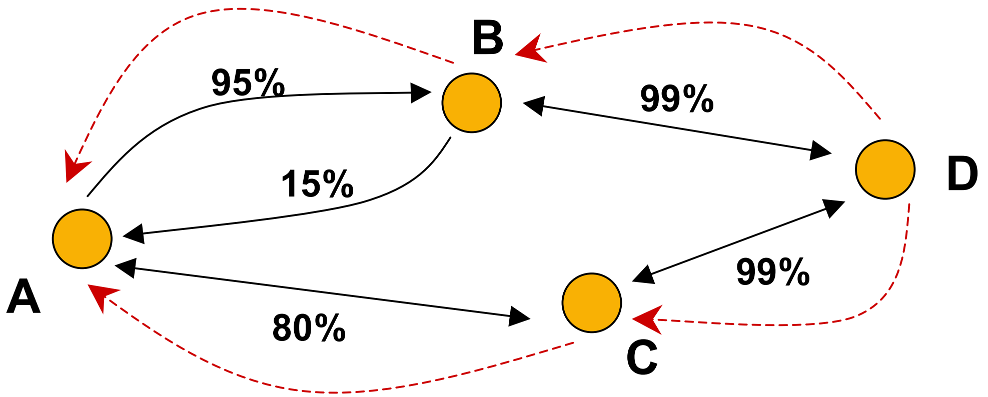
- Detect interference by tracking the reporting behavior of devices
- Low LQI / High RSSI on inbound messages may assist decision
- In a large network, multiple devices need to be involved in the detection – may be interferers on different channels in different areas of a building.
- Intelligent selection of initial network channel can help avoid problems.
  - Channels 11, 26 are at the extremes of the 2.4GHz range.
  - Channels 15, 16, 21, 22 sit between the non-overlapping European 802.11 channels (not guaranteed!).

ZigBee™ Alliance

Dealing with Interference: Channel Change

- Sensor-type networks can use the gateway device to broadcast a channel change; other devices must automatically rejoin in this case. Devices that don't hear the broadcast must search for the new network channel.
- Control-type networks with an application-required central node can allow that node to control the change.
- Other networks must devise a method for deciding to change the channel : must avoid multiple-network problems.
- Pre-selection of a subset of 802.15.4 channels makes finding the network on a new channel easier.

Asymmetric Links



- Asymmetric links are common in real deployments
- Important that only symmetric links are used when performing route discovery, ensuring the best bi-directional link is established
- Typically this is handled by the network stack.

ZigBee™ Alliance

Single Chip ZigBee vs Dual Chip ZigBee

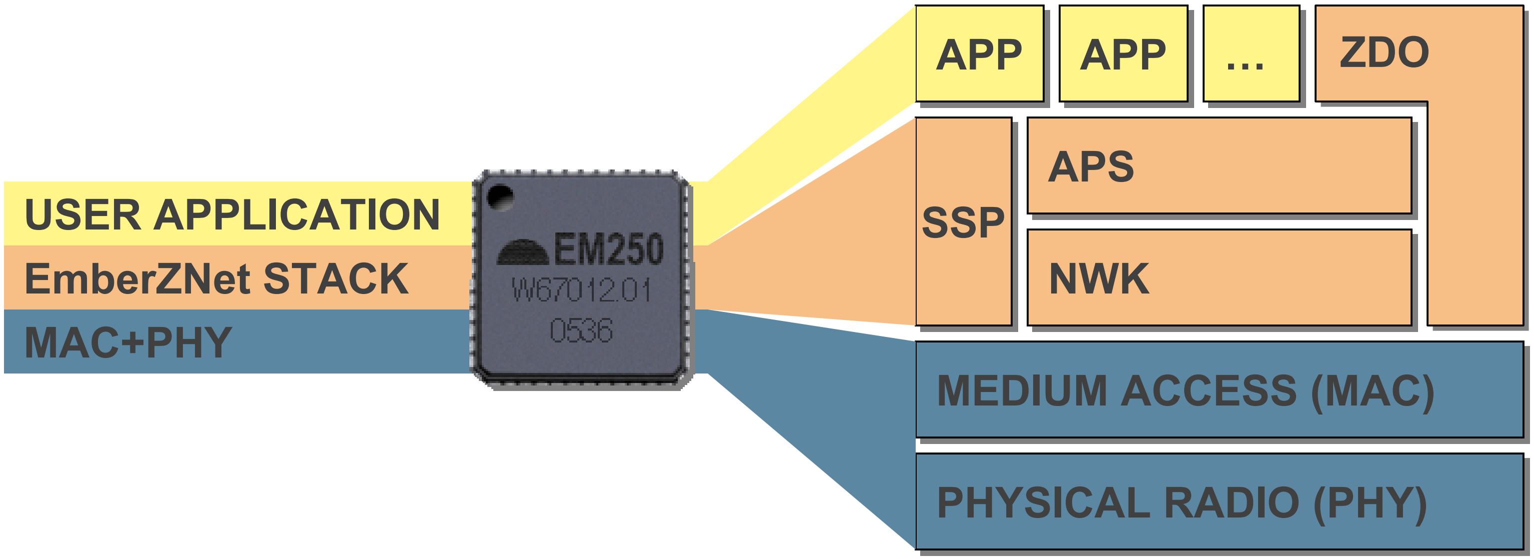
Single Chip

- Lowest BOM cost
- Lowest Power Consumption for battery operated devices such as light switches, temperature sensors etc.
- Smallest pcb footprint
- Ideal for new battery-operated products, especially sensors, remote controls, switches.

Dual Chip

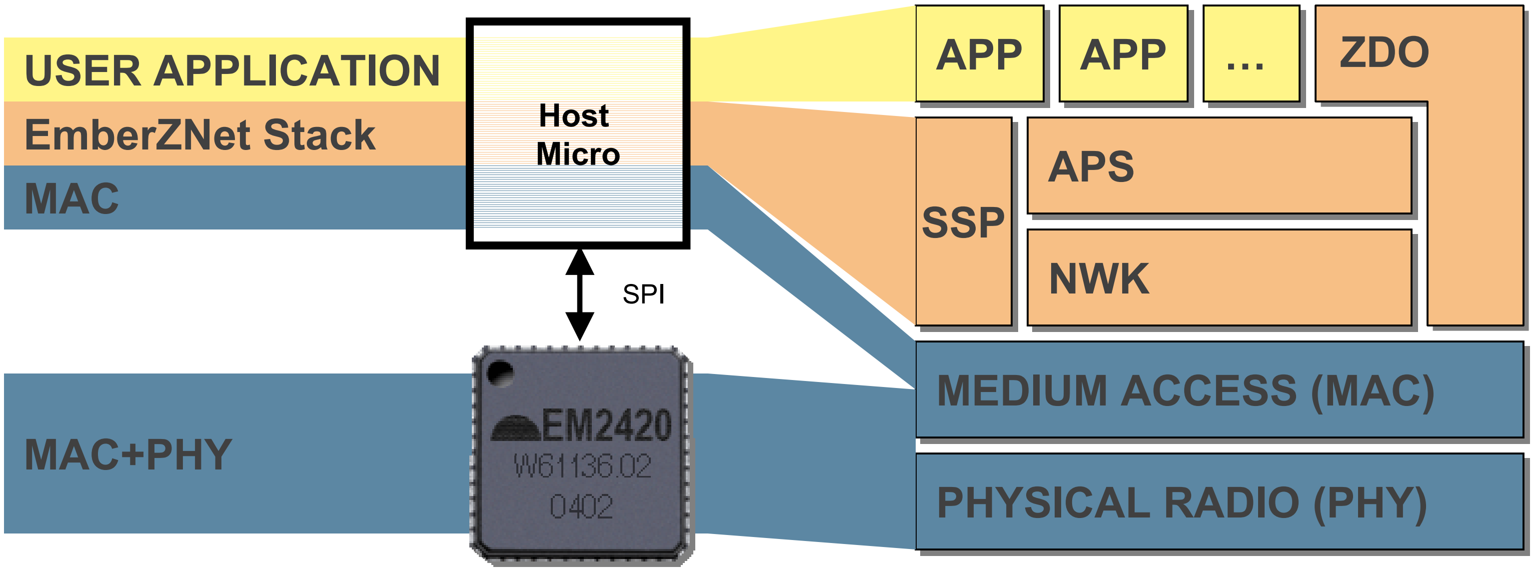
- Existing Product may already contain a microcontroller. Retrofit easier than redesign.
- Gateway device may require more resources than single chip can provide.
- Engineering team may not want to take on another micro, tools etc.

Single Chip ZigBee



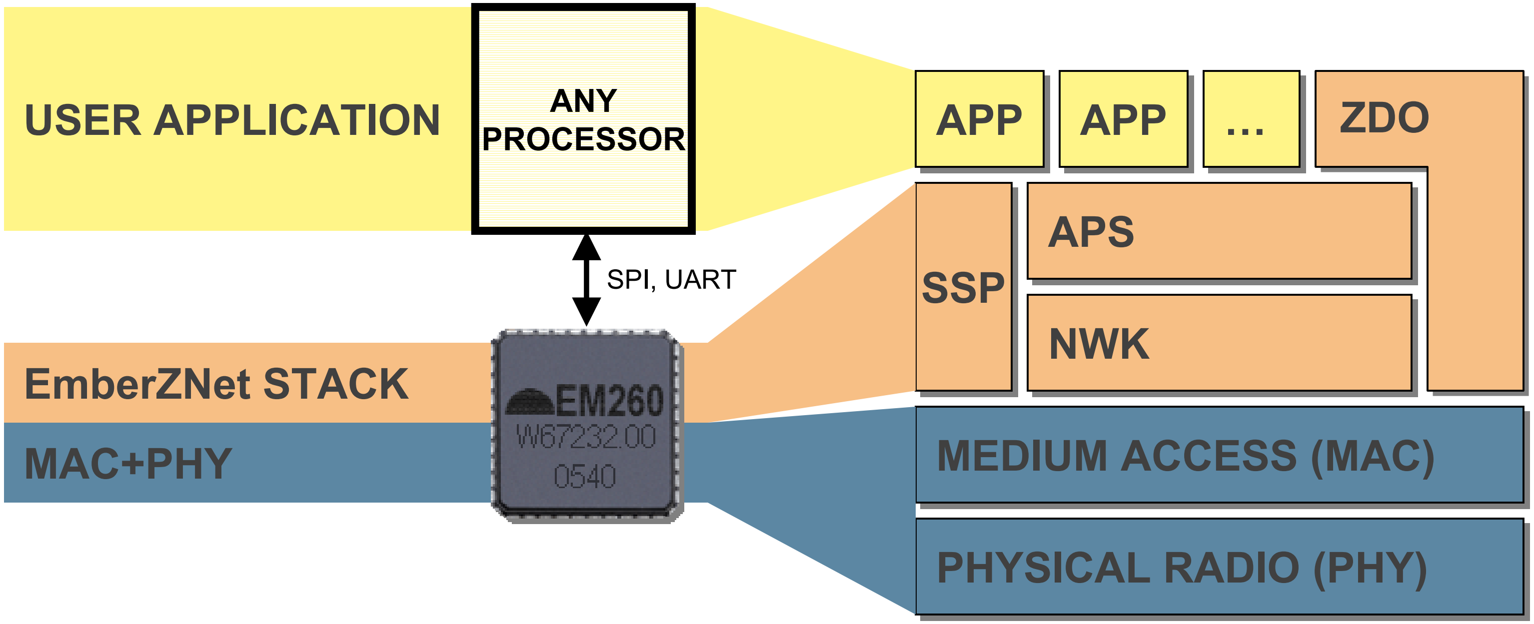
- IEEE 802.15.4 compliant radio AND a microcontroller in a single chip.
  - => No external micro required.
- Low passive component count for lower BOM cost.
- Small pcb footprint

Dual Chip ZigBee / uC + RF Transceiver



- IEEE 802.15.4 compliant Physical (PHY) and Medium Access (MAC) layers in RF Transceiver.
- ZigBee Stack and Application runs on the host micro, communicating with the RF Transceiver via high speed (SPI) serial line.
- Processor support may be limited due to the work required to port a full ZIgBee stack.

ZigBee Network Processor



- ZigBee Networking Stack runs on ZigBee Network Processor
- Applications run on a host processor communicating with the Network Processor via high-speed serial port.
- Ideal for Gateway Applications and Retrofit of ZigBee to existing products.

Any Questions?