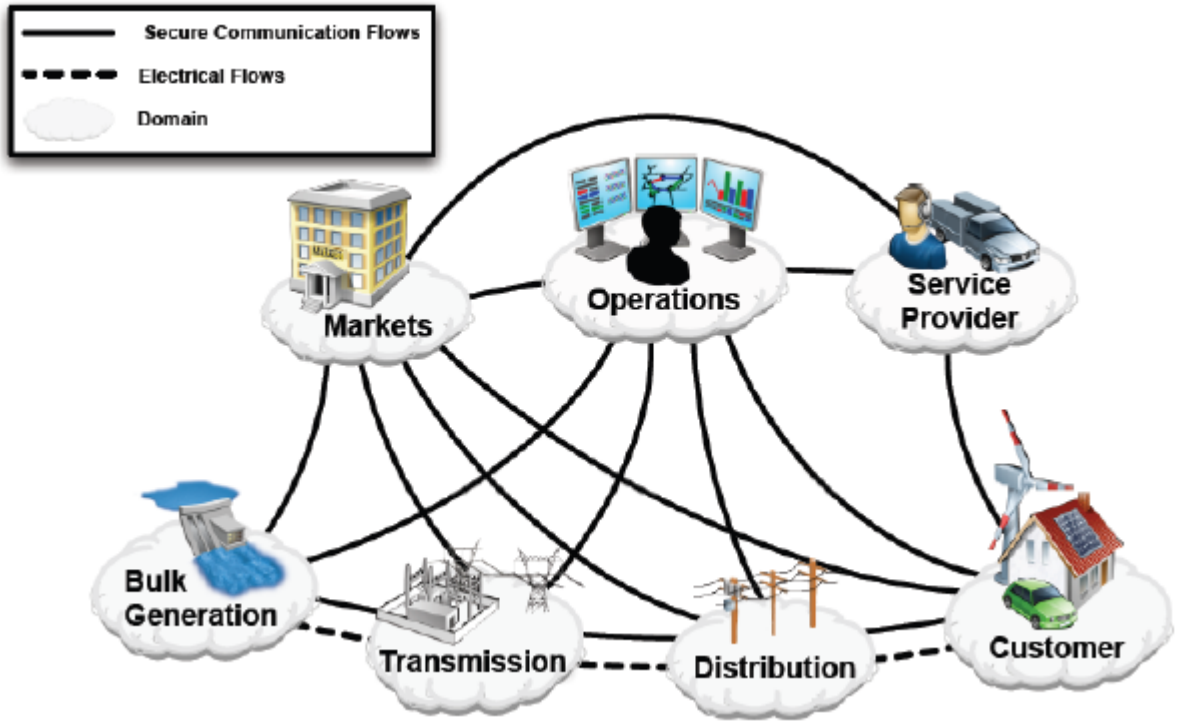
Topic 3: Smart Grid Communications

Department of Electrical & Computer Engineering
Texas Tech University

Spring 2012

NIST Conceptual Reference Model for Smart Grid

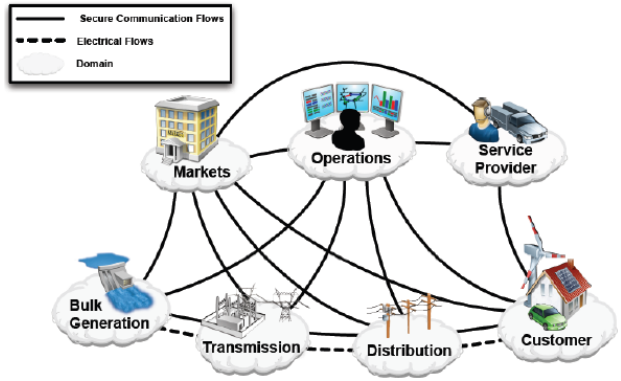
- Interactions across 7 Smart Grid Domains:



- Each domain involves its own *actors* and *applications*.

NIST Conceptual Reference Model for Smart Grid

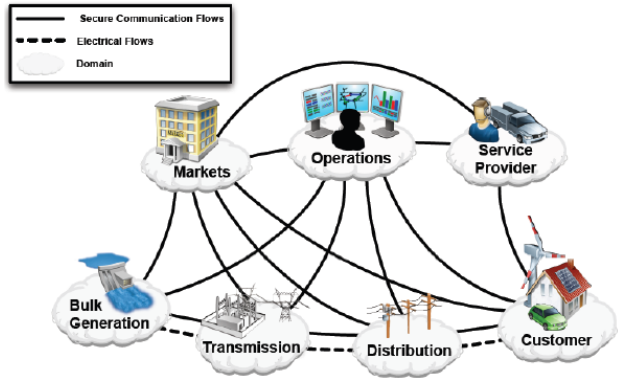
- Consumers:
  - The end users of electricity.
  - May also generate/store electricity.
  - Traditionally: Residential, Commercial, and Industrial.



- Market:
  - Participants in wholesale market: day-ahead, hour-ahead,...
  - Involves prediction, bidding, auctions, …

NIST Conceptual Reference Model for Smart Grid

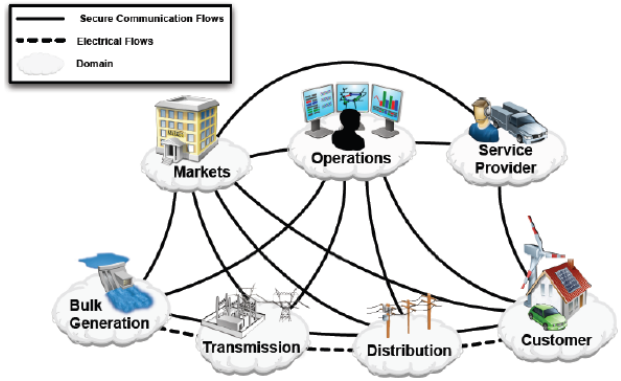
- Service Providers:
  - Organizations providing service to:
    - Both utilities and consumers.
  - ISPs, Cell Phone Companies, Aggregators,…



- Operations:
  - Independent System Operators (ISOs)
  - Regional Transmission Organization (RTOs)

NIST Conceptual Reference Model for Smart Grid

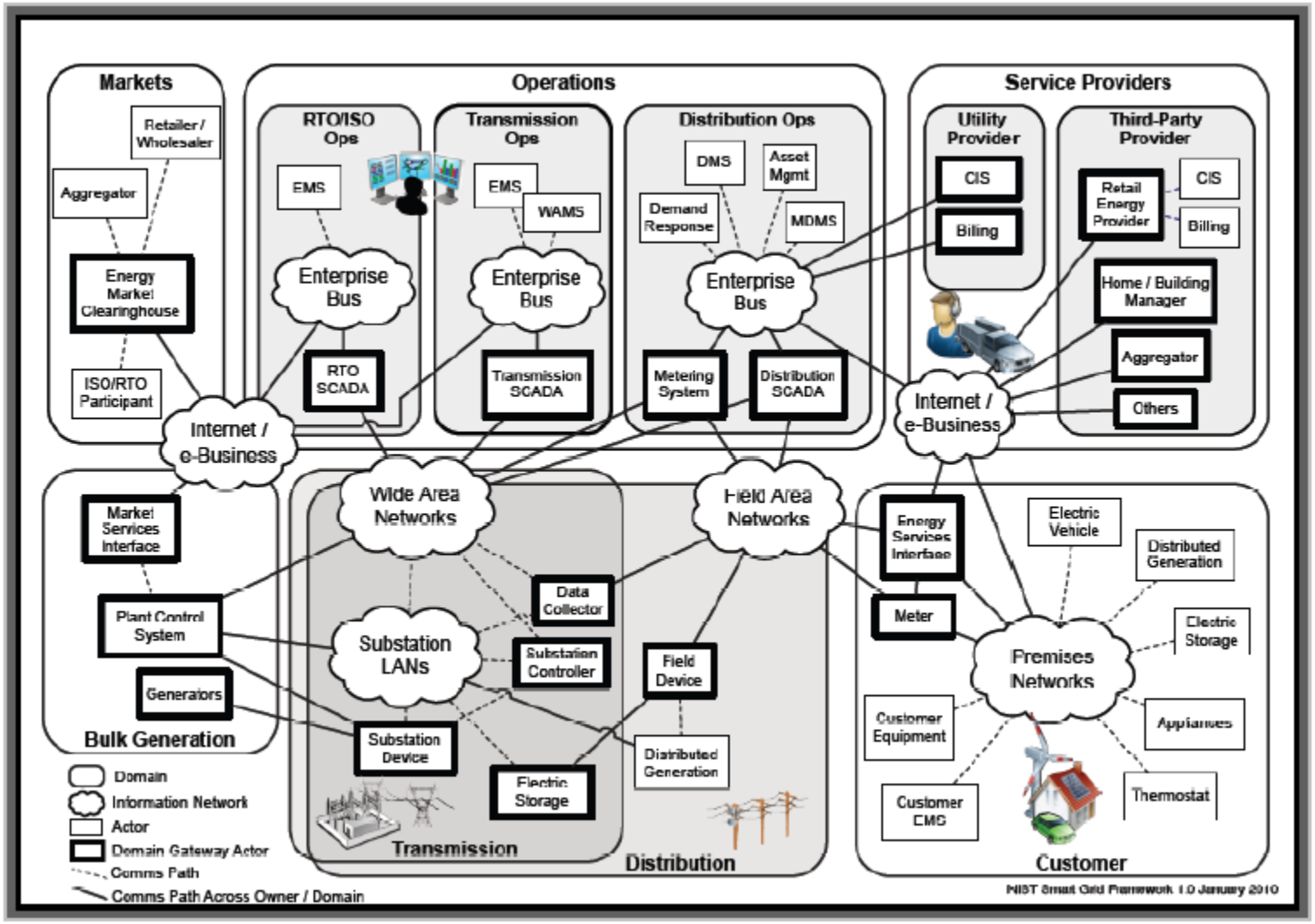
- Bulk Generation:
  - Major Power Plants.



- Transmission:
  - Carriers of bulk electricity over long distances.

- Distribution:
  - Distribution of electricity to (and from!) consumers.

NIST Model for Smart Grid Information Network



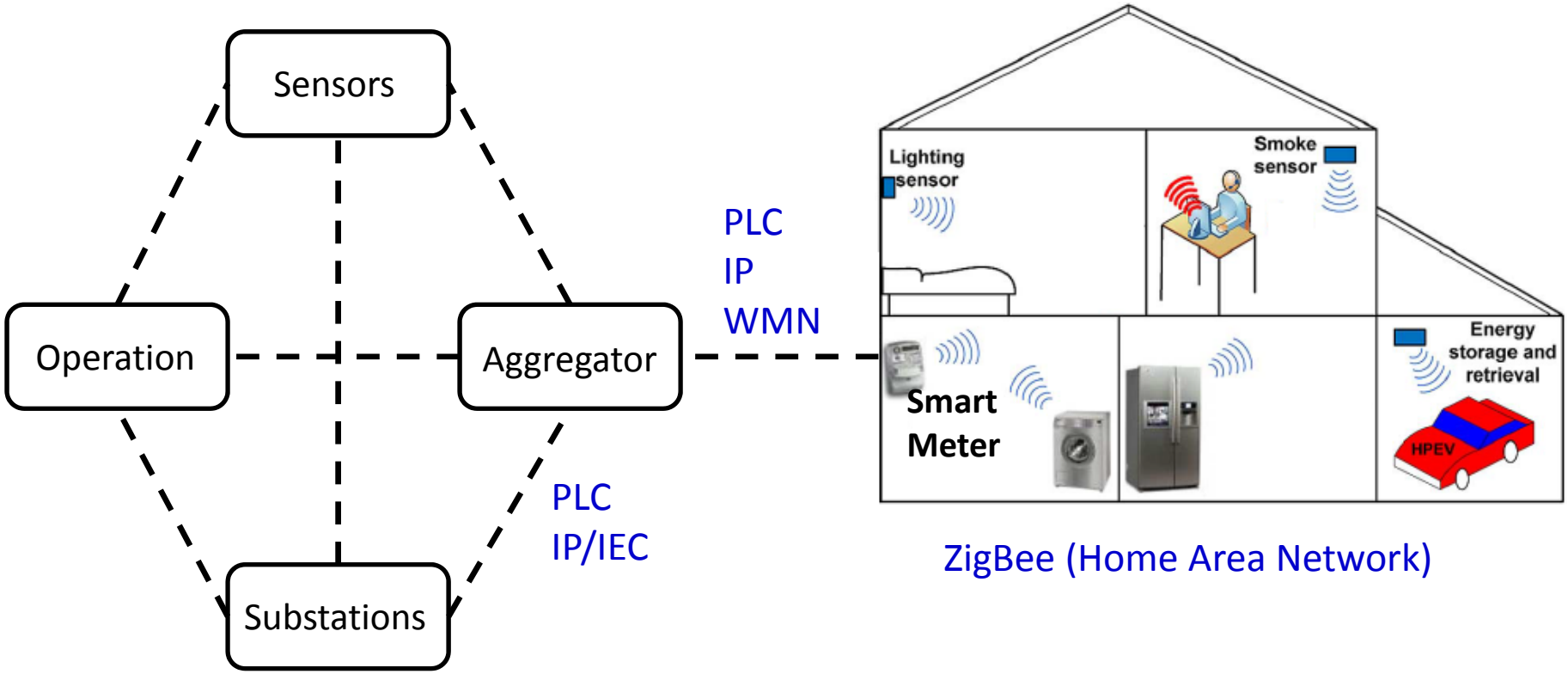
MDMS: Meter Data Management System,
CIS: Customer Information System
EMS: Energy Management System

Smart Grid Communications

- There are two questions to answer:
  - How can different smart grid entities exchange messages?
  - What kind of messages (and why) should they exchange?
- Our focus in Topic 3 is on the first question.
- We want to learn which communication technologies may help.

Smart Grid Communications

- In particular, we cover these communications technologies:



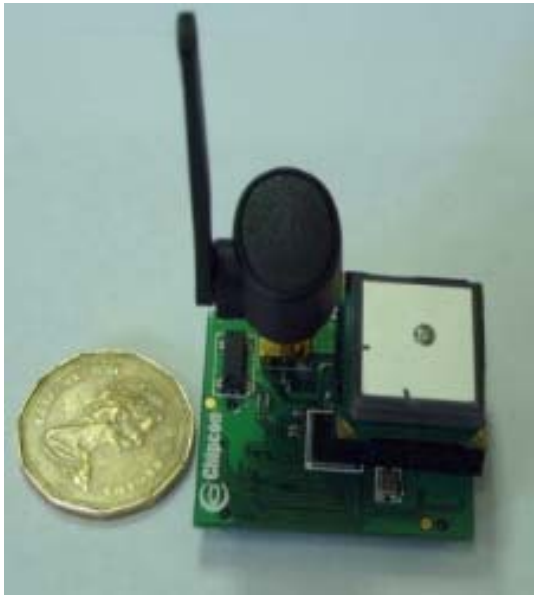
ZigBee (Home Area Network)

ZigBee

ZigBee Overview

- ZigBee is a working group to promote IEEE 802.15.4 standard.
  - High level communication
  - Small, low-cost, low-power devices

MPR2400 Micaz ZigBee Wireless Sensor Node



www.wsncanada.ca

ZigBee Overview

- IEEE 802.15 is for Wireless Personal Area Networking (WPAN)
  - 802.15.1: Bluetooth
  - 802.15.2: Co-existence (e.g., with WLAN)
  - 802.15.3: High Rate WPAN via Ultra wideband (UWB)
  - 802.15.4: Low Rate

    Low Power Consumption

    Long Battery Life

    Inexpensive!

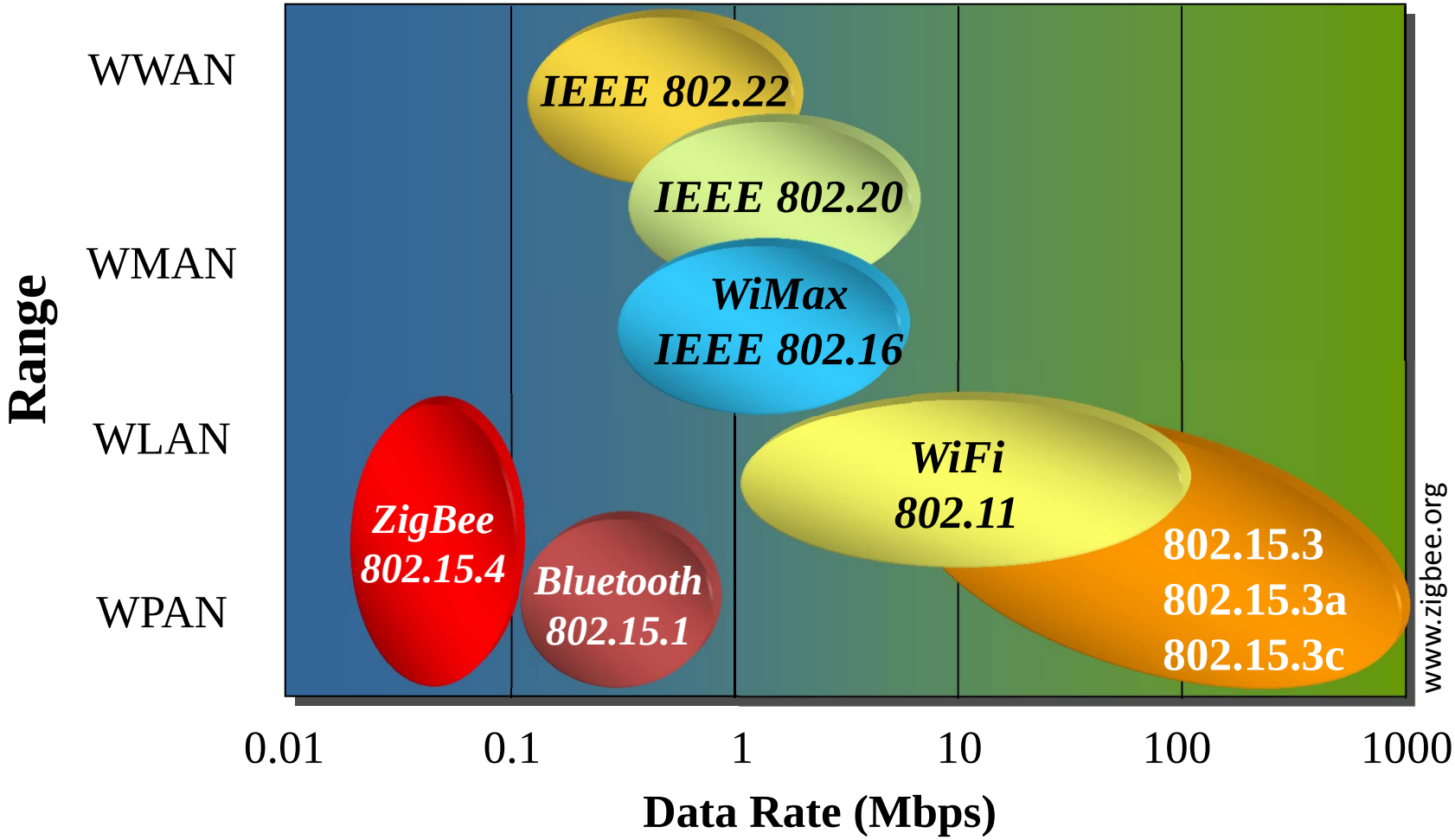
ZigBee Overview

- WPAN vs WLAN/WiFi and WMAN/WiMax

	802.16 WiMAX	802.11 WiFi	802.15 WPAN
Frequency	*2 – 11GHz*	*2.4GHz*	*Varies*
Range	*31 miles*	*100 Meters*	*10 Meters*
Data Rates	*70 Mbps*	*11 - 110Mbps*	*20k – 55Mbps*
Nodes	*Thousands*	*Dozens*	*Dozens*

* Data for 802.16a and 802.11a

ZigBee Overview



ZigBee Overview

- Simpler and Less Expensive than Bluetooth
  - Cost: One fourth of Bluetooth
  - Complexity:
    - Complex ZigBee Nodes: 10% Code of a Bluetooth node
    - Simple ZigBee Nodes: 2% Code of a Bluetooth node

ZigBee Applications

- A wireless mouse that works for years without new batteries!

- Key Application Areas:
  - Building / Home
  - Energy
  - Health
  - Telecommunications

ZigBee Applications in Smart Grid

- Key Application:
  - Smart Meter Communications with Smart Appliances
- Smart Appliances:
  - Washer, Dryer, Dish Washer, Fridge
  - Air Conditioning
  - Pumps and Water Heaters
  - PHEVs

Topic 3: How ZigBee Works

Topic 4: Applications in DR

ZigBee Alliance

- Defining Network, Security, and Application Software
- Assuring Interpretability
- Market Awareness
- Managing / Evolving Standards

Membership: $3500

www.zigbee.org

ZigBee Alliance

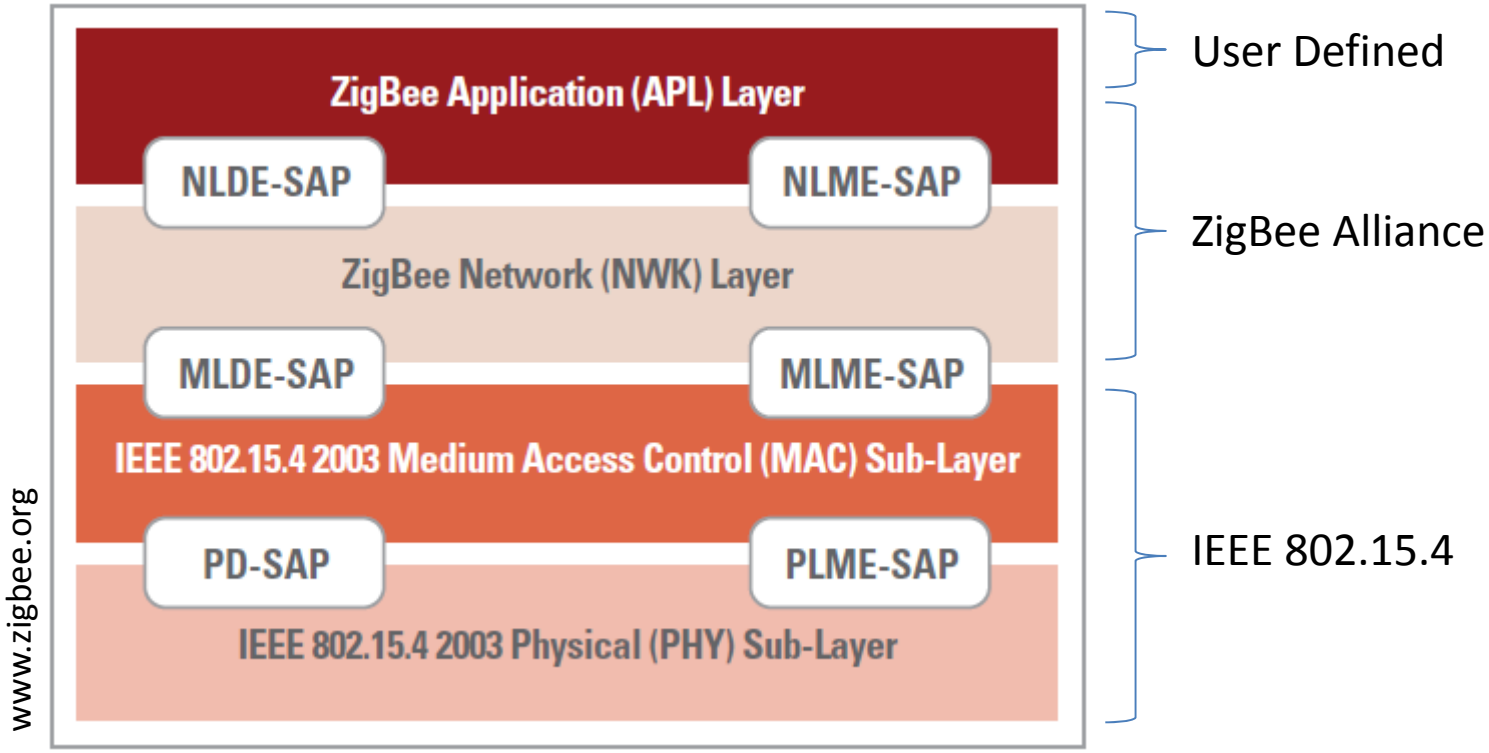
Scenario	ZigBee Membership Required	
	Yes	No
Company creating/designing products for sale	☑	
Company offering services or reselling products		☑
Installer		☑
Reseller/Retailer		☑
User		☑
Architect, Designers, Builder, Owner		☑
Contractor designing products for ZigBee member		☑
Manufacturer		☑
Design House		☑

www.zigbee.org

* Zigbee is an OPEN Global Standard

ZigBee Protocol Stack

- There are four layers in ZigBee Protocol Stack:



[DE: Data Entity, ME: Management Entity, SAP: Service Access Point]

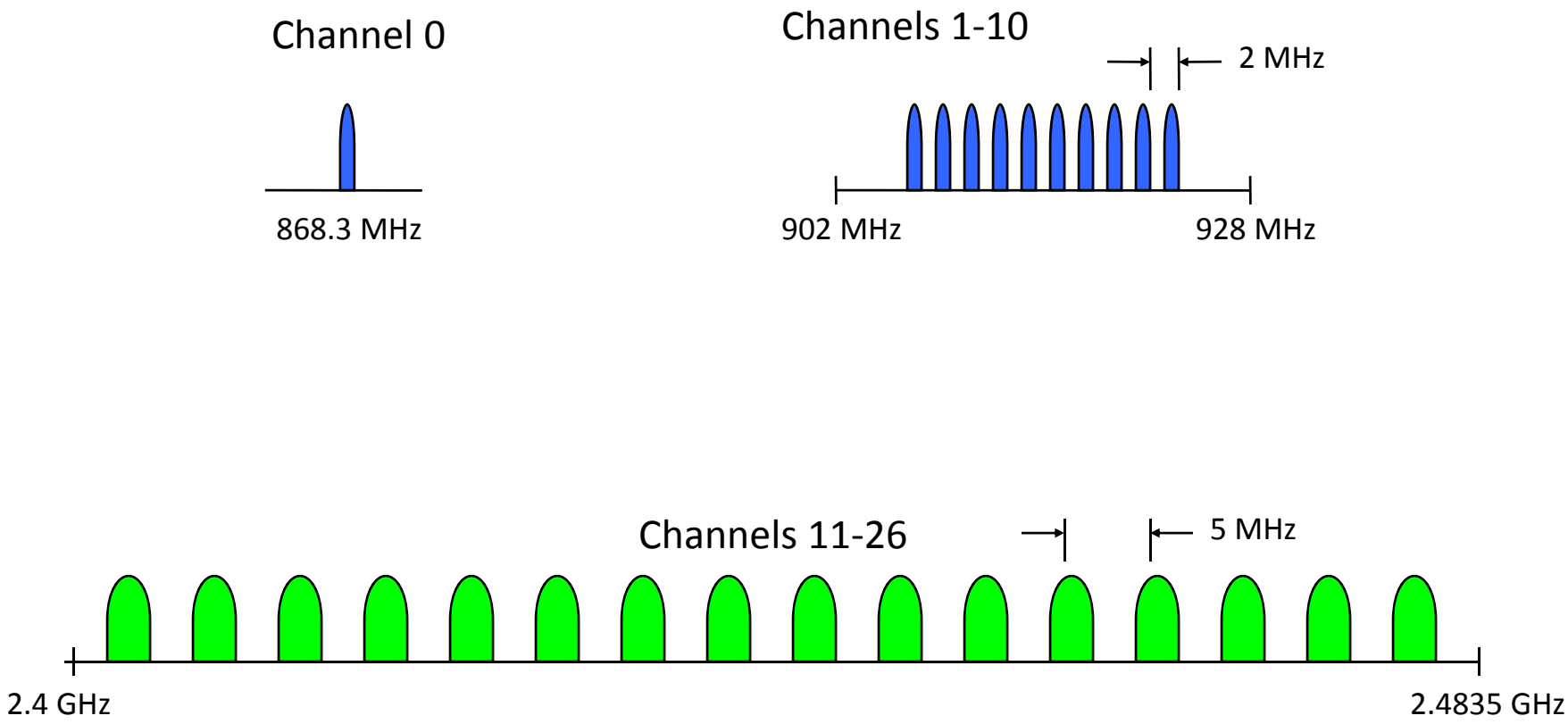
ZigBee Protocol Stack

- ZigBee devices may use different frequency bands:

PHY	Frequency Band	Channel Numbering	Bit Rate
868 MHz	*868 – 870 MHz*	*0*	*20 kb/s*
915 MHz	*902 – 928 MHz*	*1 - 10*	*40 kb/s*
2.4 GHz	*2.4 – 2.4835 GHz*	*11 - 26*	*250 kb/s*

ZigBee Wireless Channels

- Frequency channels used by ZigBee devices:



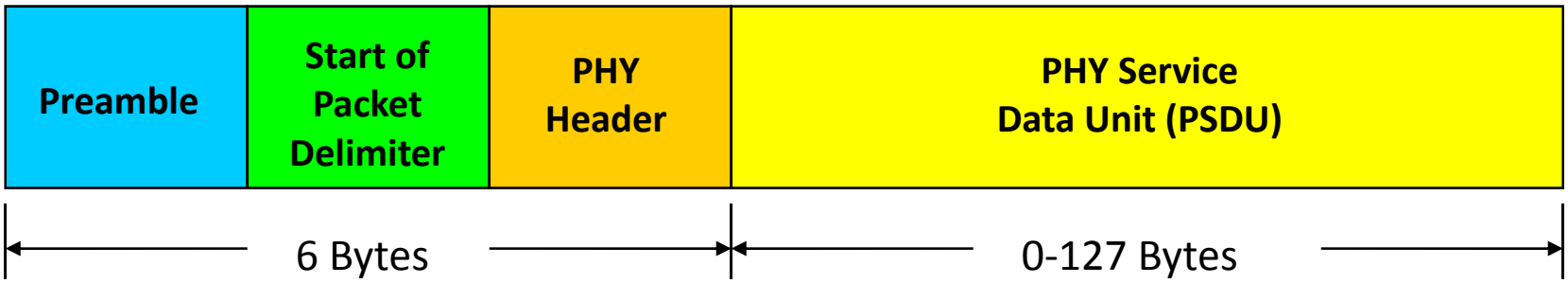
ZigBee Wireless Channels

- ZigBee may co-exist with other technologies at certain bands.

- Some of the features for co-existence:
  - Carrier Sense Multiple Access (CSMA) (Q: Remember?)
  - End-to-end ACK and Retransmission
  - Built-in Channel Scanning / Find Available Channels

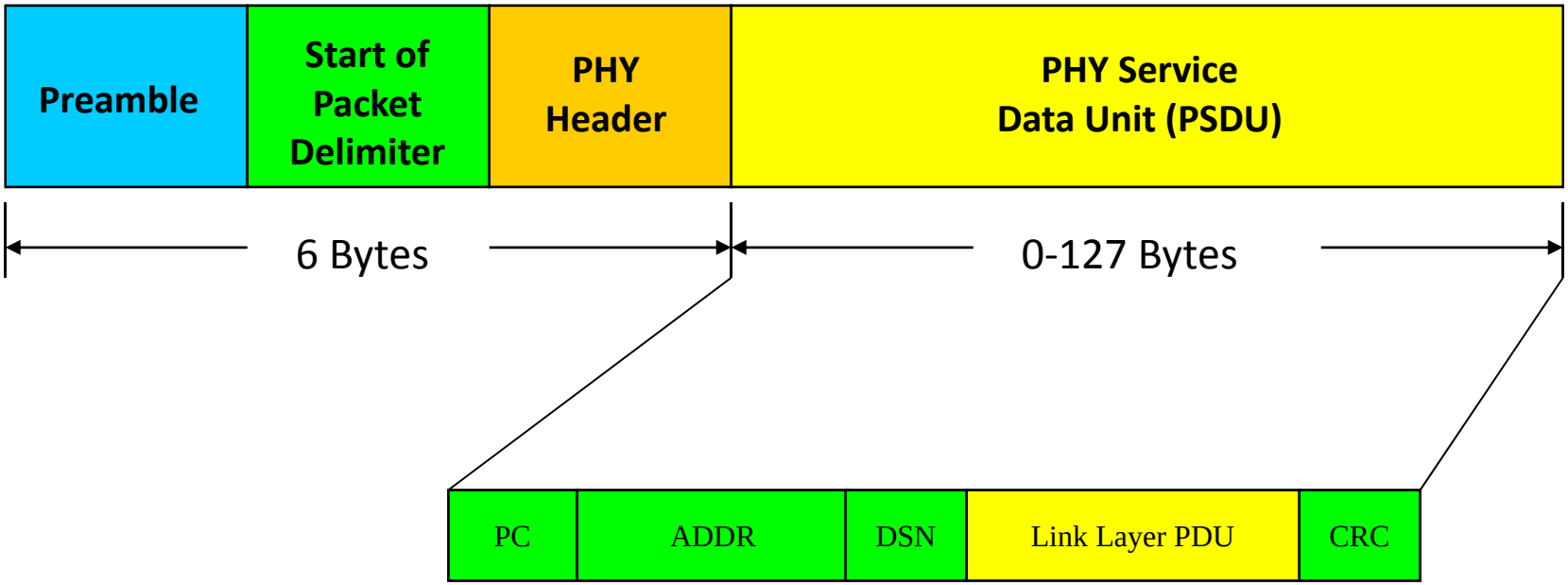
ZigBee Packet Structure

- Packet Fields [specified by IEEE 802.15.4]:
  - Preamble: 32 bits for synchronization (Q: Remember?)
  - Start of Packet Delimiter: 8 bits
  - PHY Header: 8 bits / indicates PSDU length, etc.
  - PSDU: 0 to 127 bytes of data



ZigBee Packet Structure

- Inside PSDU:



PC: Addressing Mode Flags
ADDR: Address
DSN: Data Sequence Number
CRC: Cyclic Redundancy Check

ZigBee Device Addressing

- All Devices Have Address:
  - Two-bytes: We can have up to 65,536 nodes (Q: Why?)
  - Addressing Modes:
    - Star
    - Peer-to-Peer
    - Cluster Tree

Addressing Modes Depend on the Network Topology.

[We will see more on topologies…]

ZigBee Device Classes

- ZigBee has two main Device Classes:
  - Full Function Device (FFD)
  - Reduced Function Device (RFD)

- **FFD**:
  - Available in any topology
  - Can become a network coordinator
  - Talks to any other device

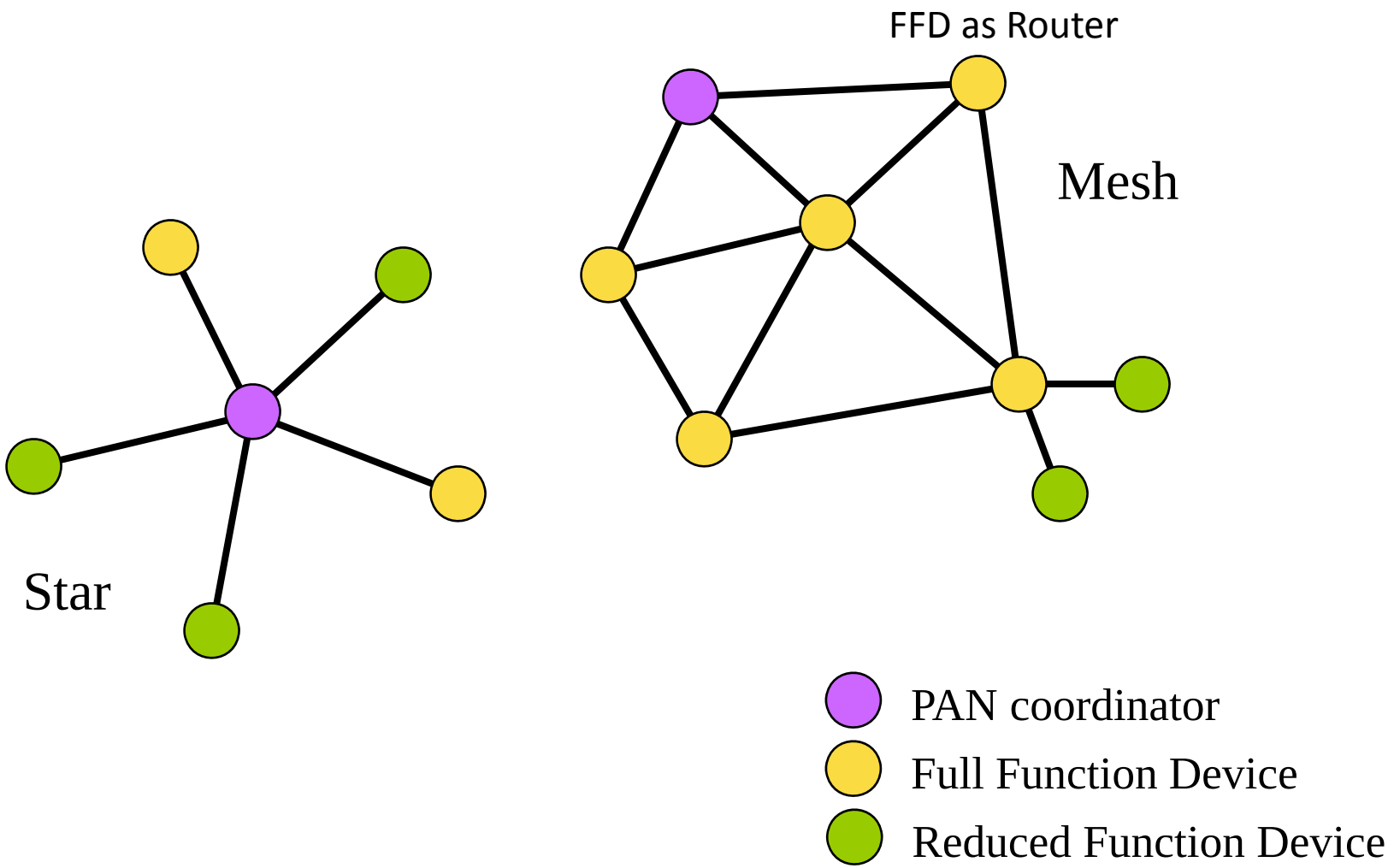
ZigBee Device Classes

- **RFD**:
  - Limited to star topology
  - Cannot become a network coordinator
  - Talks to only a network coordinator
  - Simpler Implementation
  - Less power consumption

ZigBee Device Classes

- Each ZigBee network has one network coordinator.
  - It initiates network formation.
  - We need at least one Full Function Device. (Q: Why?)
- Other devices can be either FFD or RFD.
  - FFDs that are not network coordinator act as routers.
  - Recall that RFDs only talk to the network coordinator.

ZigBee Network Topologies



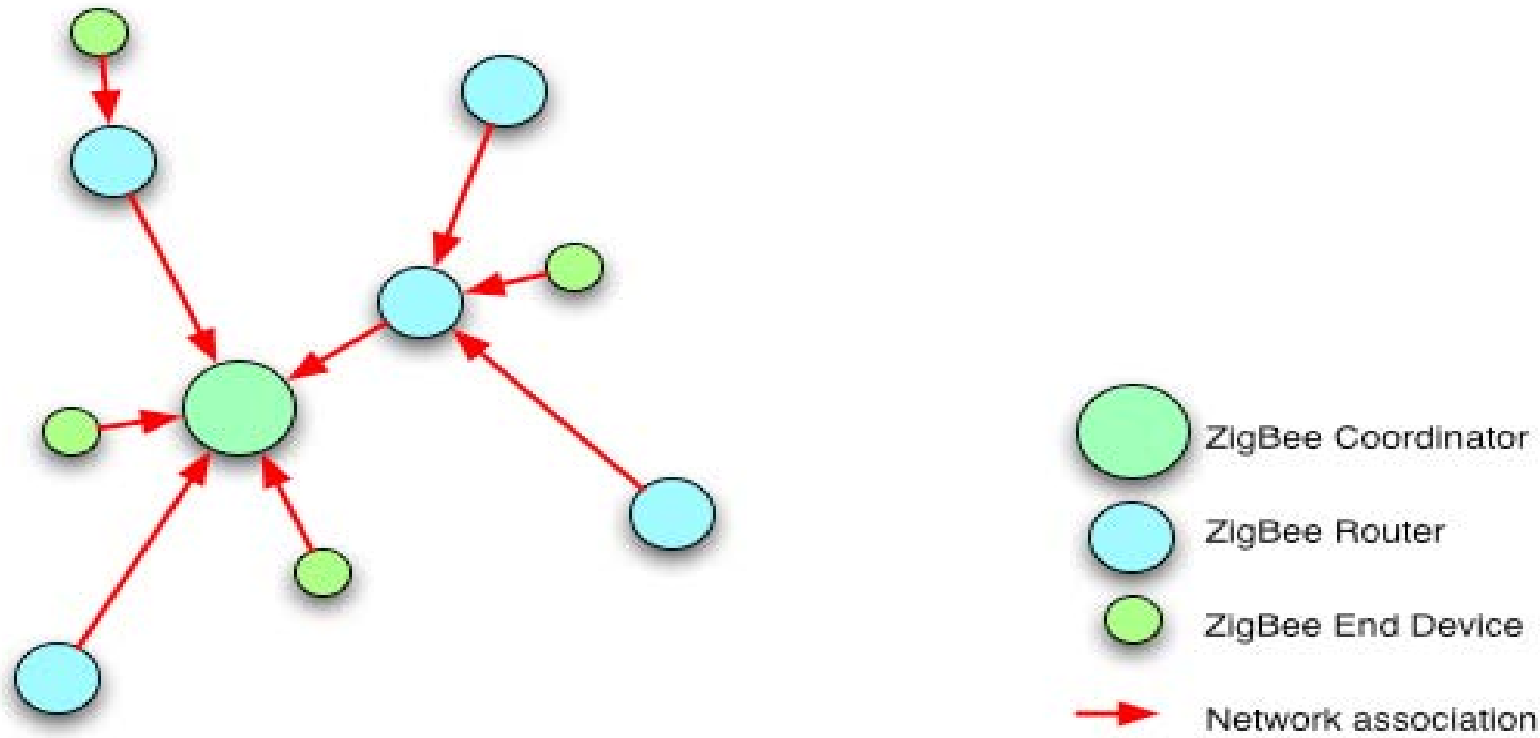
Q: Can we build a mesh topology with RFDs only?

ZigBee Network Topologies

Network Coordinator initiates the network formation.

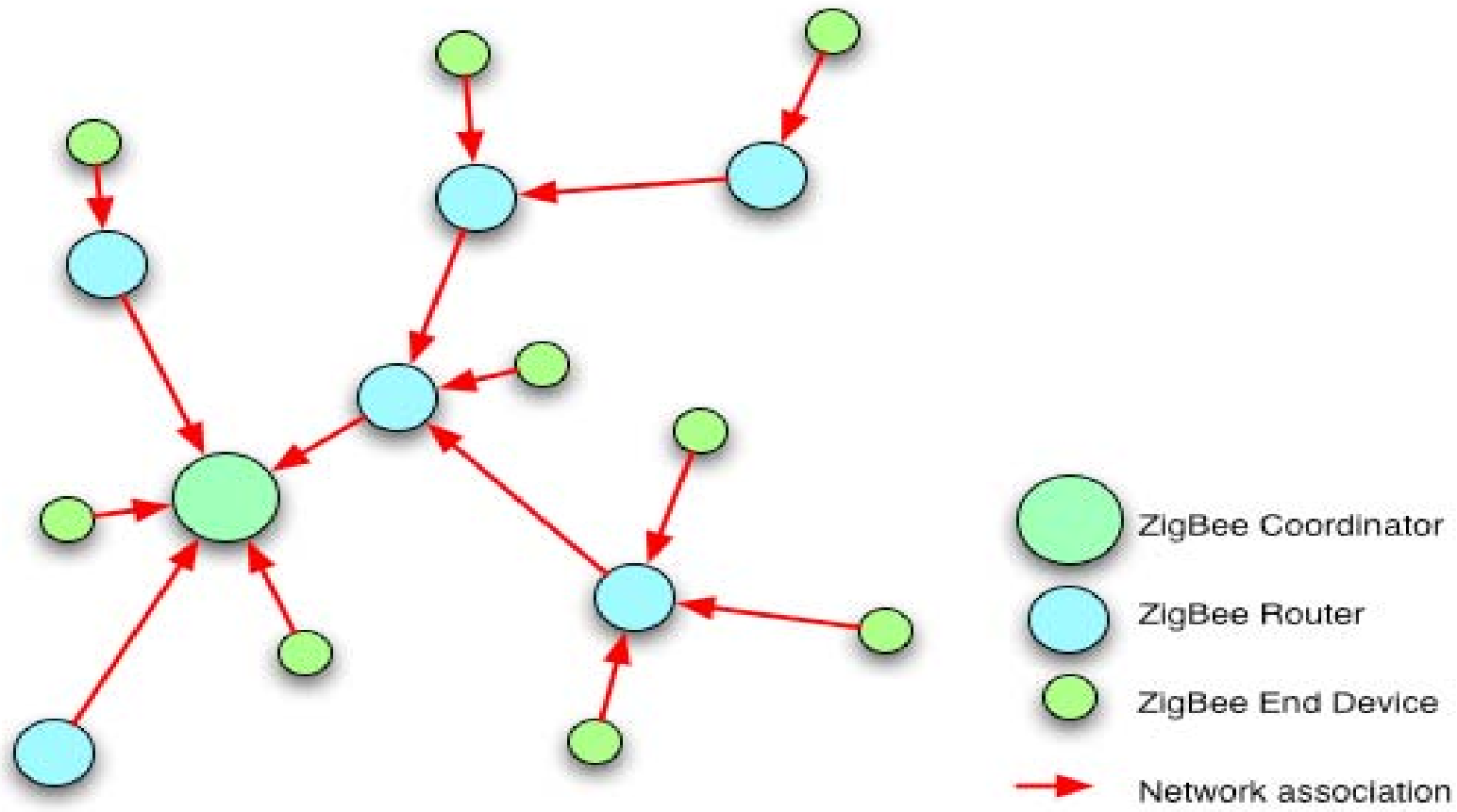
ZigBee Network Topologies

ZigBee routers help expanding the network



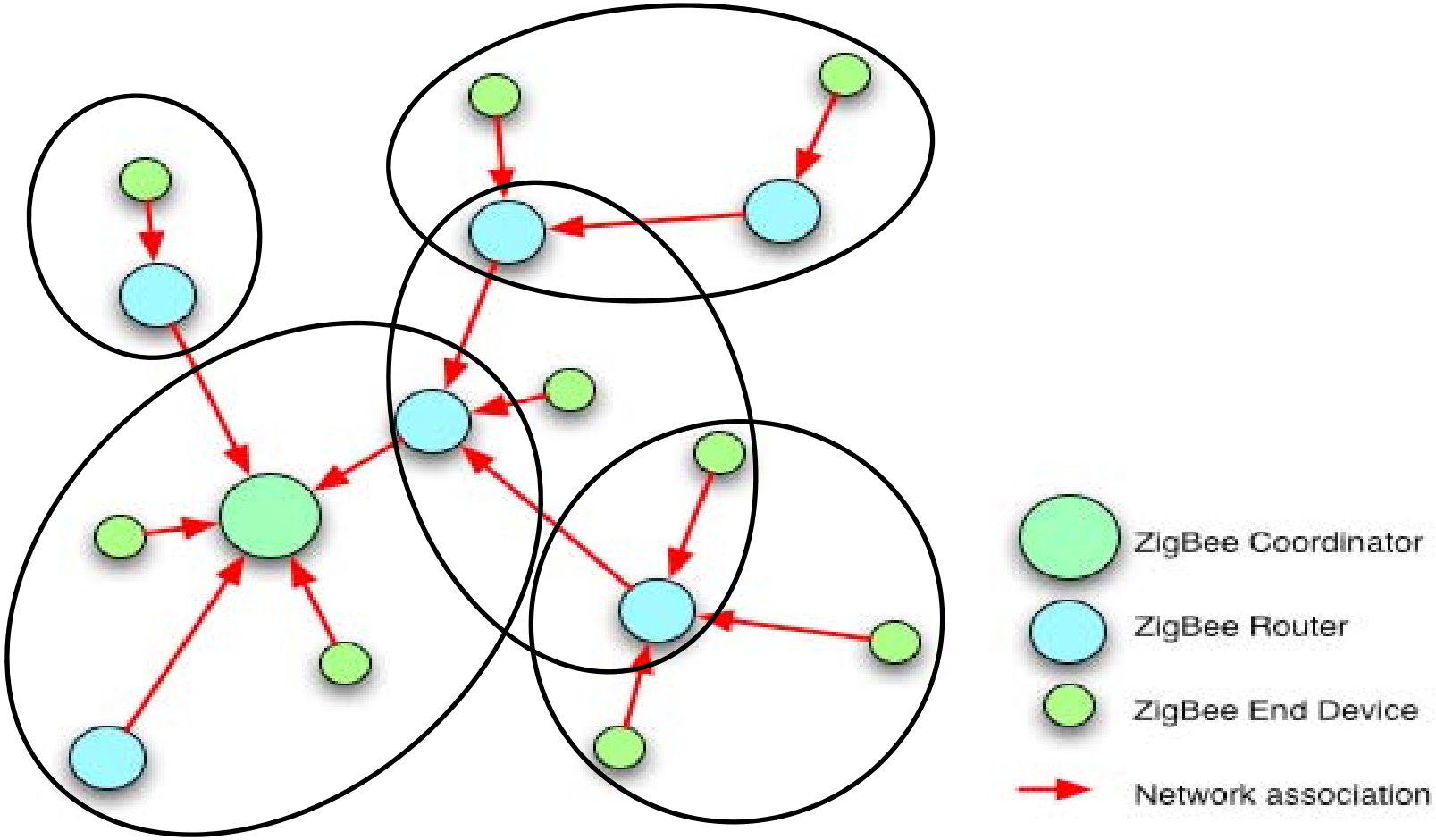
ZigBee Network Topologies

ZigBee routers help expanding the network



ZigBee Network Topologies

We can form Tree Clusters.



ZigBee Tree Clusters

- Each cluster has one FFD as its root.
- The root for the overall tree is the network coordinator.
- They allow routing with minimum overhead.
- The tree may span physically large areas.
- In total, we can have 255 clusters of 254 nodes = 64,770 nodes.

ZigBee Addressing

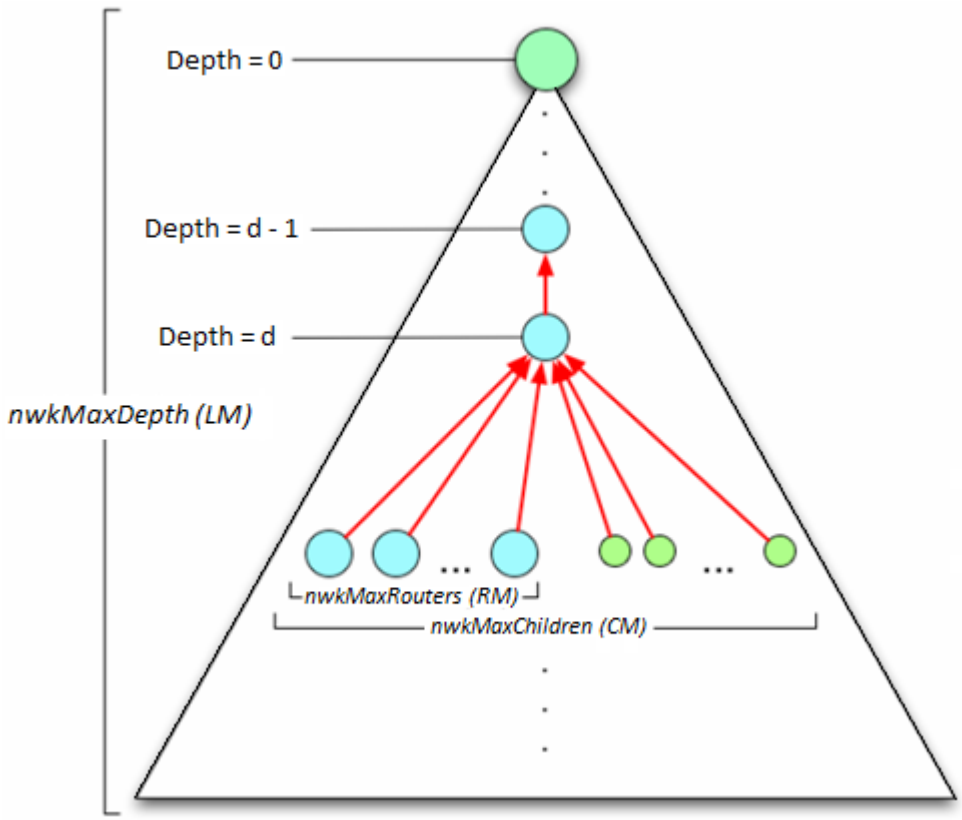
- For each new node (i.e., associated device):
  - A unique address is allocated by parent (router/coordinator)
  - Recall that the parent can only be a FFD.
- The max number of devices that a parent can support = 32.
- Two types of addresses:
  - *Network Address*: 16-bit, only unique in this network
  - *Extended Address*: 64-bit, unique in all networks

ZigBee Addressing

- The following network attributes are important:
  - *nwkcMaxDepth*:
    - The maximum absolute depth allowed in this network.
  - *nwkMaxDepth (Lm)*:
    - The maximum absolute depth a particular device can have.
  - *nwkMaxChildren (Cm)*:
    - The maximum number of children a device is allowed to have.
  - *nwkMaxRouters (Rm)*:
    - The maximum number of routers a device can have as children.
    - It is set by the coordinator for all devices in the network.

ZigBee Addressing

- The network attributes for a node/router with absolute depth d:



ZigBee Addressing

- These attributes let us compute the function Cskip(d).
  - Size of address block allocated by each parent at depth d.
  - We have:

$$Cskip(d) = \begin{cases} 1 + Cm \times (Lm - d - 1) & Rm = 1 \\ \dfrac{1 + Cm - Rm - Cm \times Rm^{Lm-d-1}}{1 - Rm} & \text{otherwise} \end{cases}$$

- A FFD parent with Cskip(d) > 0 may accept child devices.

ZigBee Addressing

- A parent assigns addresses to children based on:
  - Whether the child is router capable or not.

- Let A_{parent} denote the address of a parent at depth d.

- **Router Capable Child**: [*n*th such child at depth d+1]

Address: $A_n = A_{parent} + Cskip(d) \times (n-1) + 1$

Address Block: $A_{parent} + Cskip(d) \times (n-1) + 1, \cdots, A_{parent} + Cskip(d) \times n$

ZigBee Addressing

- **End-Device Child**: [*m*th such child at depth d+1]

Address: $A_m = A_{parent} + Cskip(d) \times Rm + m$

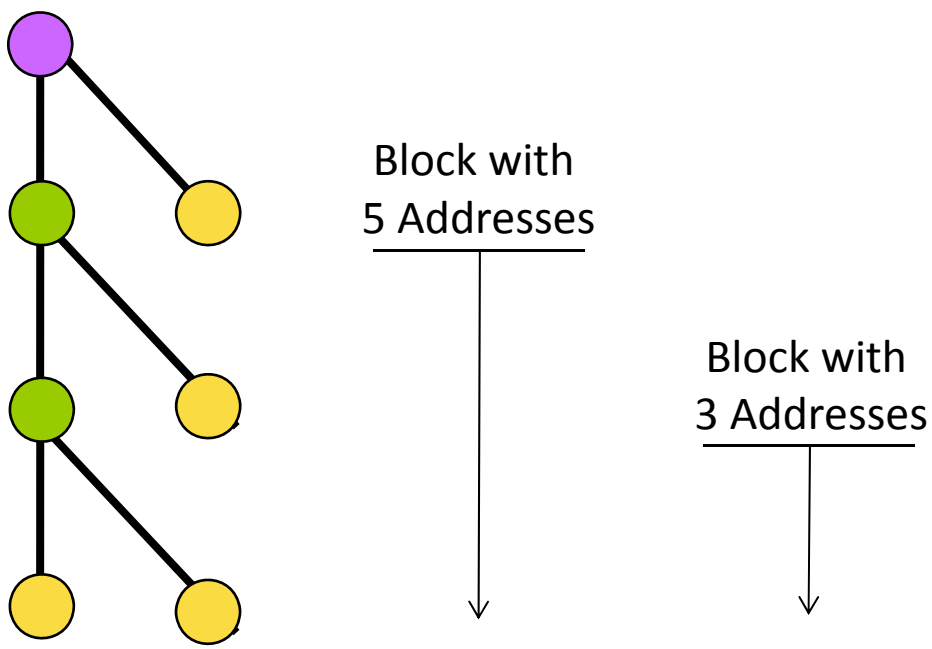
- Note that each child needs an address.

- A router child also needs an address block for its future children.

- Overall Idea: Assure having unique addresses for all nodes.

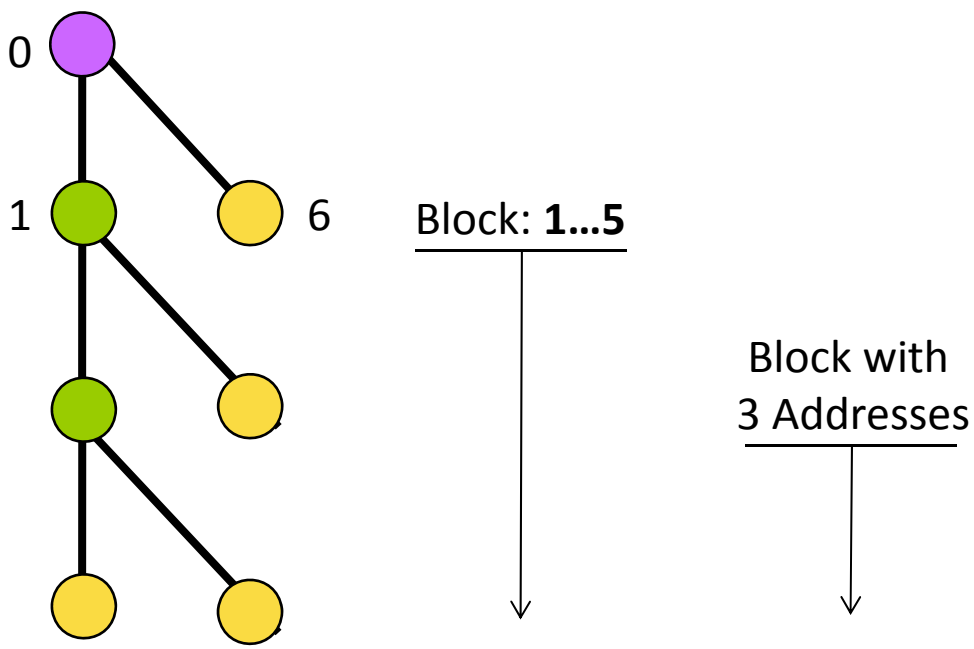
ZigBee Addressing

- Example: Rm = 1, Cm = 2, and Lm = 3.
  - Cskip(0) = 1 + 2 x (3 – 0 – 1) = 5
  - Cskip(1) = 1 + 2 x (3 – 1 – 1) = 3
  - Cskip(2) = 1 + 2 x (3 – 2 – 1) = 1



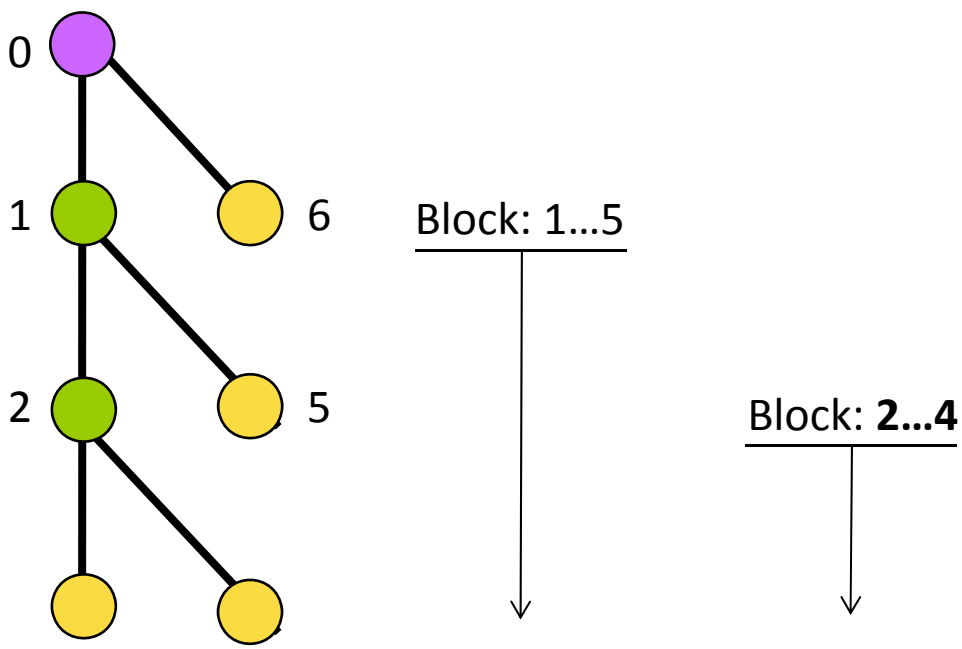
ZigBee Addressing

- Consider addressing at the network coordinator with $A_{NC} = 0$.
  - Router Child: **Addr** = 0 + 5 x (1 – 1) + 1 = **1**
    Addr Block = 1 … 5 x 1 = **1 … 5**
  - End-device Child: **Addr** = 0 + 5 x 1 + 1 = **6**



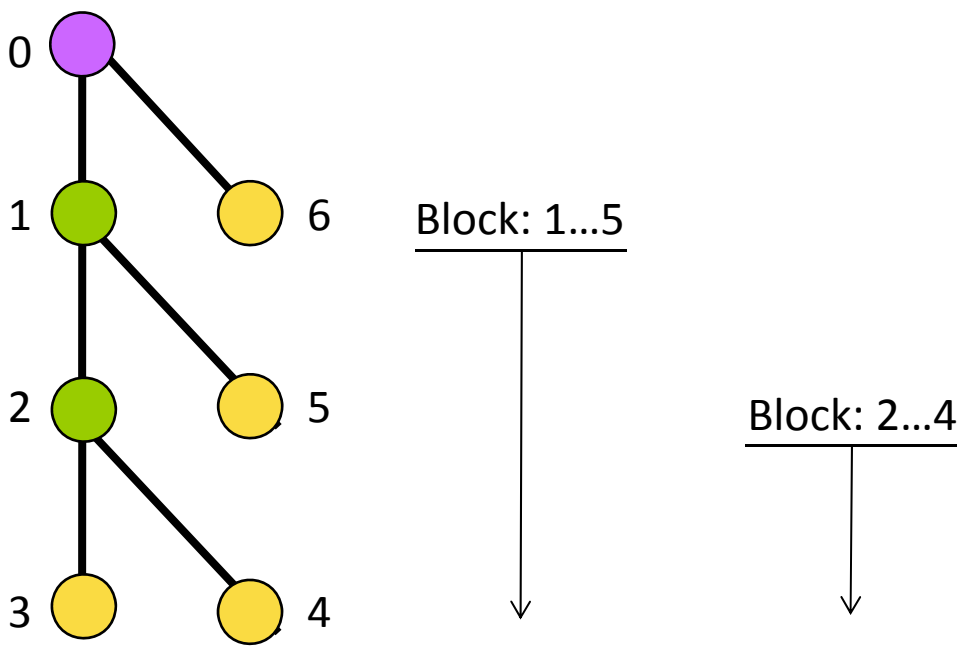
ZigBee Addressing

- At the router node at depth 1 with $A_{parent} = 1$.
  - Router Child: **Addr** = 1 + 3 x (1 – 1) + 1 = **2**
    Addr Block = 2 … 1 + 3 x 1 = **2 … 4**
  - End-device Child: **Addr** = 1 + 3 x 1 + 1 = **5**



ZigBee Addressing

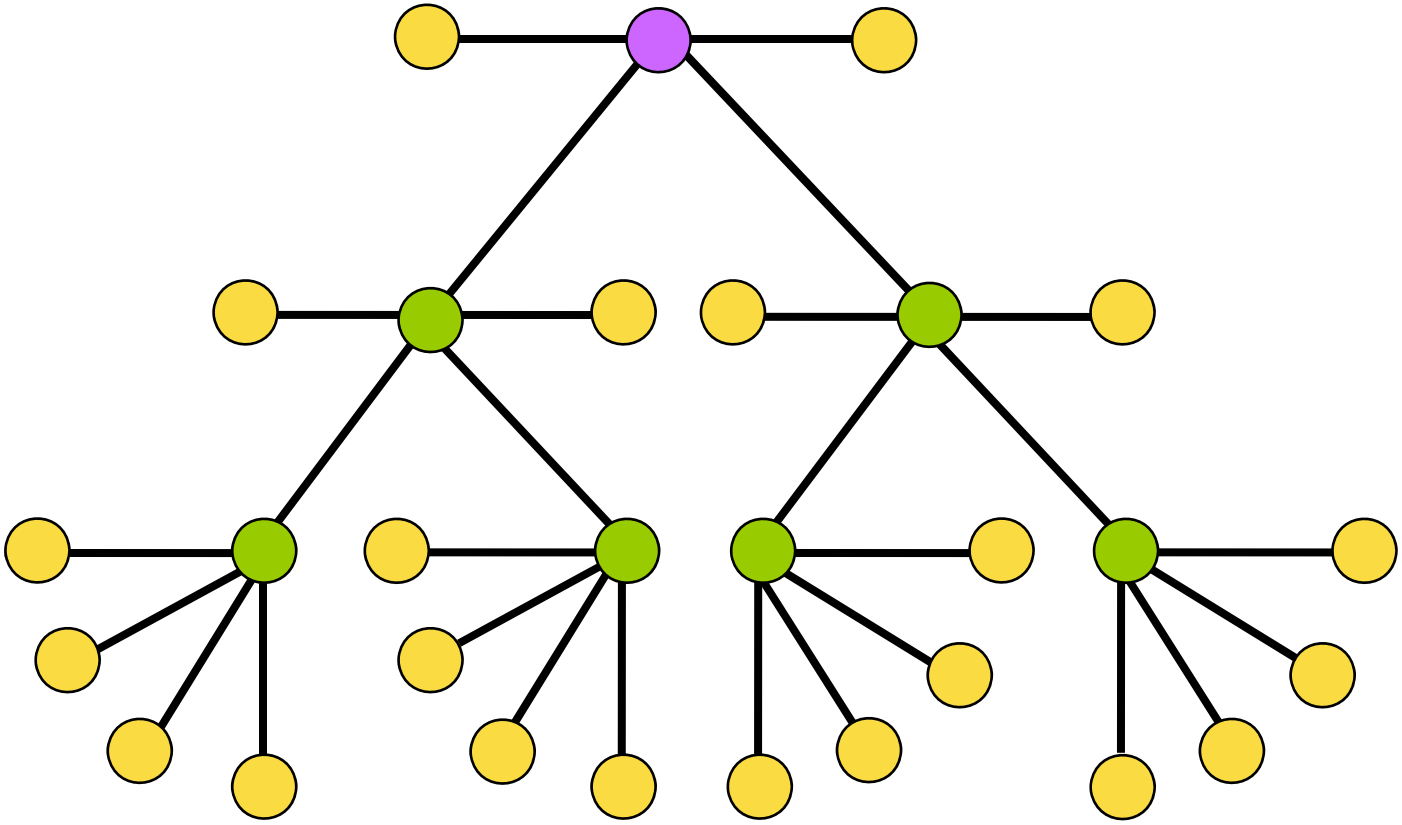
- At the router node at depth 2 with $A_{parent} = 2$.
  - Router Child: **Addr** = 2 + 1 x (1 – 1) + 1 = **3**
    Addr Block = 3 … 2 + 1 x 1 = **3 … 3**
  - End-device Child: **Addr** = 2 + 1 x 1 + 1 = **4**



ZigBee Addressing

- Example: Rm = 2, Cm = 4, and Lm = 3.
  - Cskip(0) = $(1 + 4 – 2 – 4 \times 2^{3-0-1}) / (1-2) = 13$
  - Cskip(1) =
  - Cskip(2) =
- Show how the address blocks are allocated.

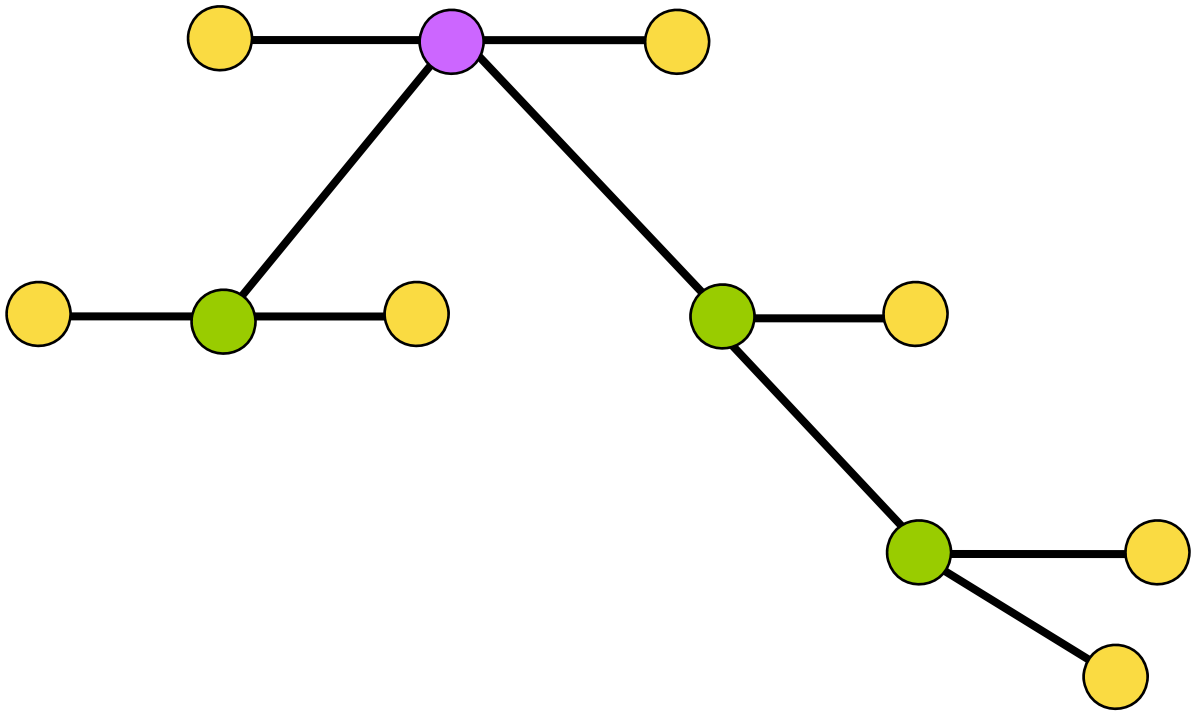
ZigBee Addressing



Your Job: Choose the addresses and address blocks!

ZigBee Addressing

- Q: What if the topology is not complete?



- Q: What if the topology is not star? Does it affect addresses?

ZigBee Routing

- We need to find a path from a source to a destination node.

- Key observation: For a router device at depth d + 1, we have

Address: $A_n = A_{parent} + Cskip(d) \times (n-1) + 1$

Address Block: $A_{parent} + Cskip(d) \times (n-1) + 1, \cdots, A_{parent} + Cskip(d) \times n$

- We can rewrite the address block as

$$A_n, \cdots, A_n + Cskip(d) - 1$$

Q: Can we use this observation for routing?

ZigBee Routing

- Assume that such router is searching for a path for address D.

- If the following is True, then D is a descendent of the router:

$$A_n < D \leq A_n + Cskip(d) - 1 \quad \Rightarrow \quad \boxed{A_n < D < A_n + Cskip(d)}$$

- Otherwise, the router should forward the message to its parent.

- Thus, we can easily find a router with D as its descendent.

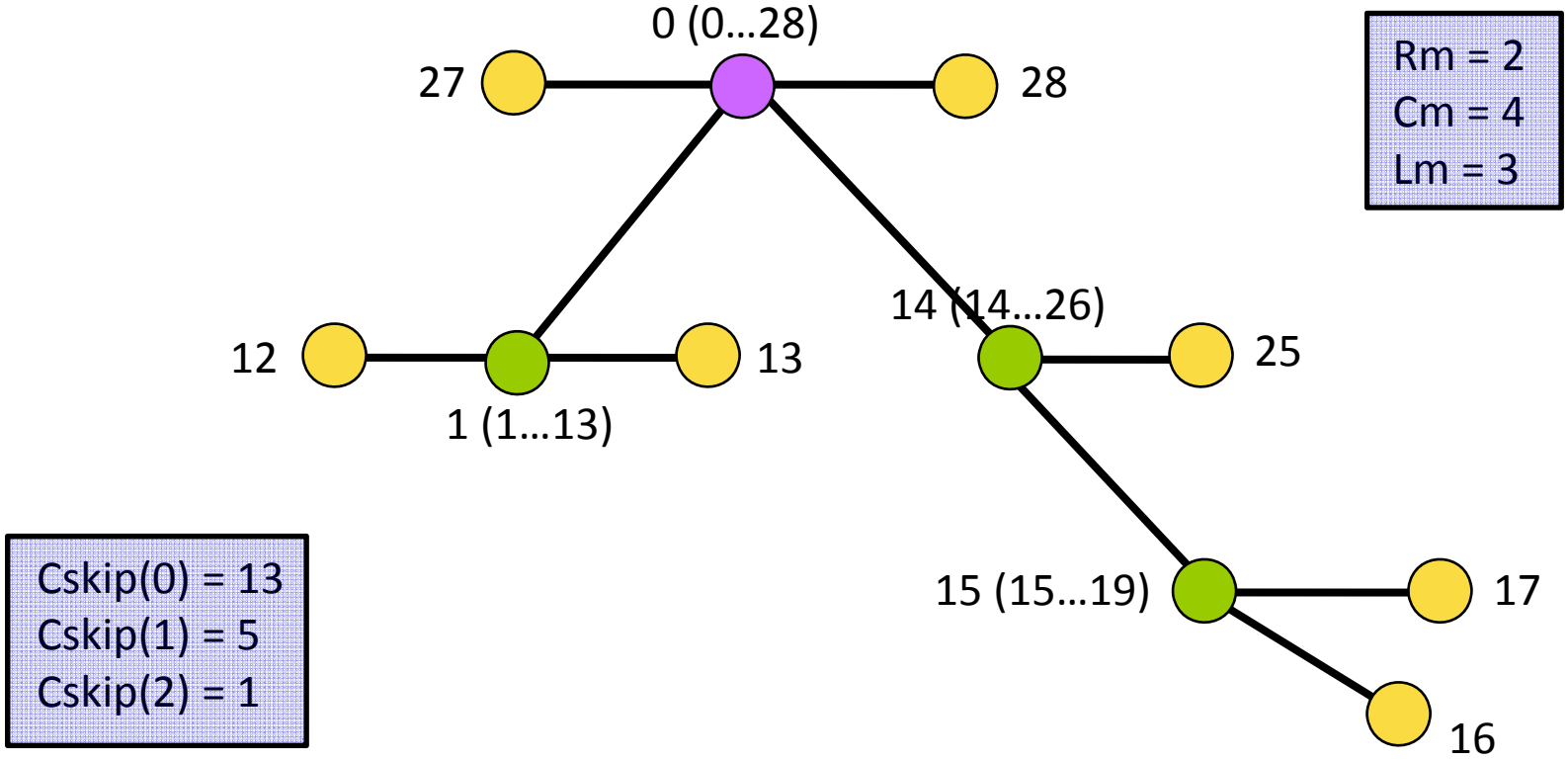
ZigBee Routing

- Next, we should find a way for a router to forward the message:
  - To the right child at next depth level.
- This is trivial if D is the address for an end-device. (Q: Why?)
- Otherwise, the address of the right router child is obtained as

$$A_n + 1 + \left\lfloor \frac{D - (A_n + 1)}{Cskip(d)} \right\rfloor Cskip(d)$$

ZigBee Routing

- Example: Node **13** wants to send a message to node **17**.



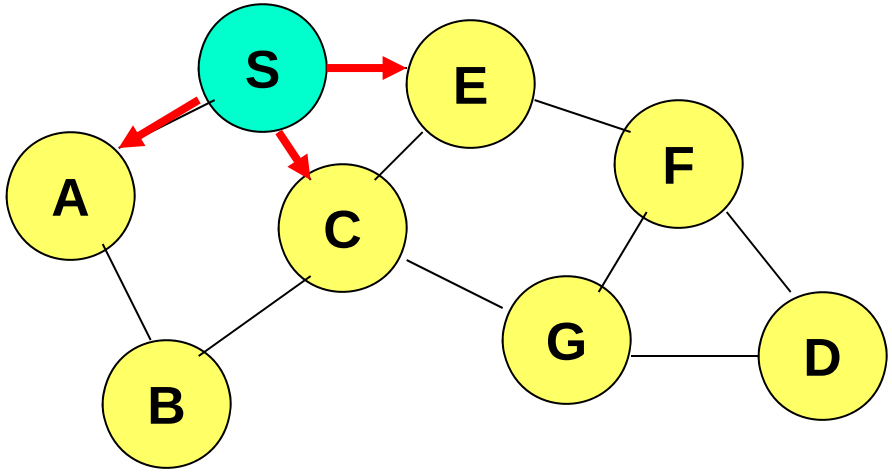
- Q: Can you explain how the destination is found?

ZigBee Routing

- This routing mechanism is particularly good for tree topologies.
- Although it works for other topologies as well.
- However, for more complex networks, ZigBee uses:
  - AODV: Ad-hoc On-demand Distance Vector
    - Uses Bellman-Ford (BF) Equation as a DV algorithm…
  - But first it requires route discovery on-demand

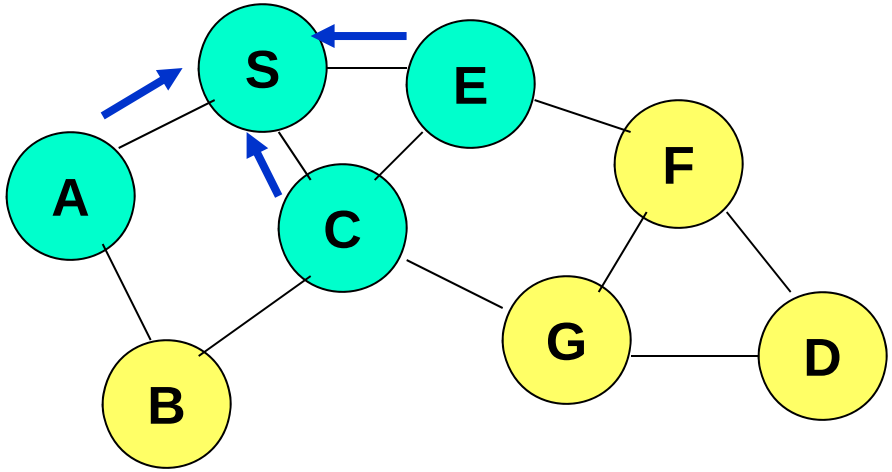
ZigBee Routing

- AODV route discovery is done using:
  - Route Request (RREQ) and Route Reply (RREP) Messages
- Source floods RREQ messages:



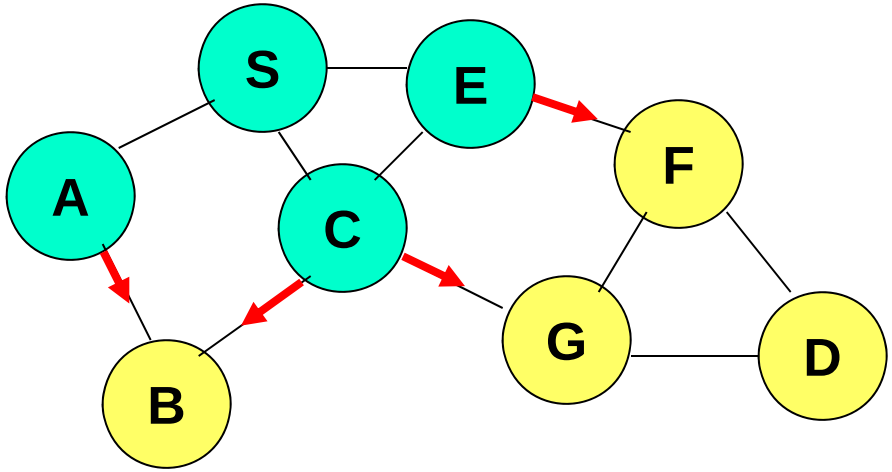
ZigBee Routing

- AODV route discovery is done using:
  - Route Request (RREQ) and Route Reply (RREP) Messages
- Revere paths are formed when nodes hear RREQ:



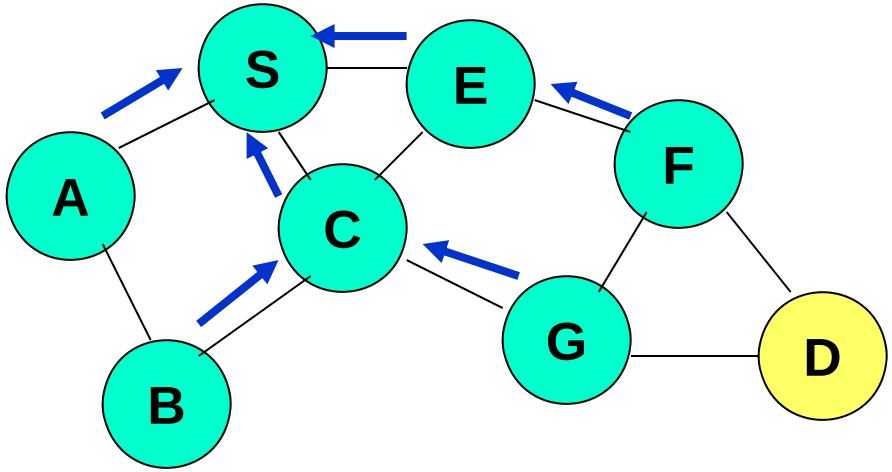
ZigBee Routing

- AODV route discovery is done using:
  - Route Request (RREQ) and Route Reply (RREP) Messages
- RREQ flooding continues in the network:



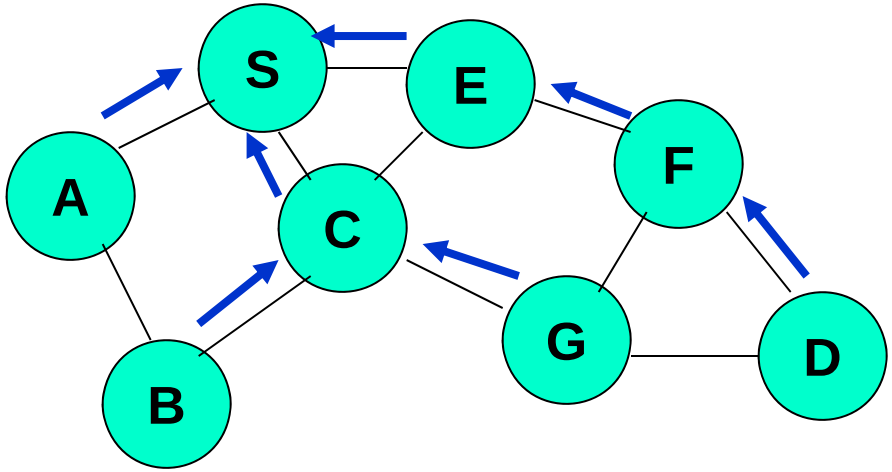
ZigBee Routing

- AODV route discovery is done using:
  - Route Request (RREQ) and Route Reply (RREP) Messages
- Revere paths are formed when nodes hear RREQ:



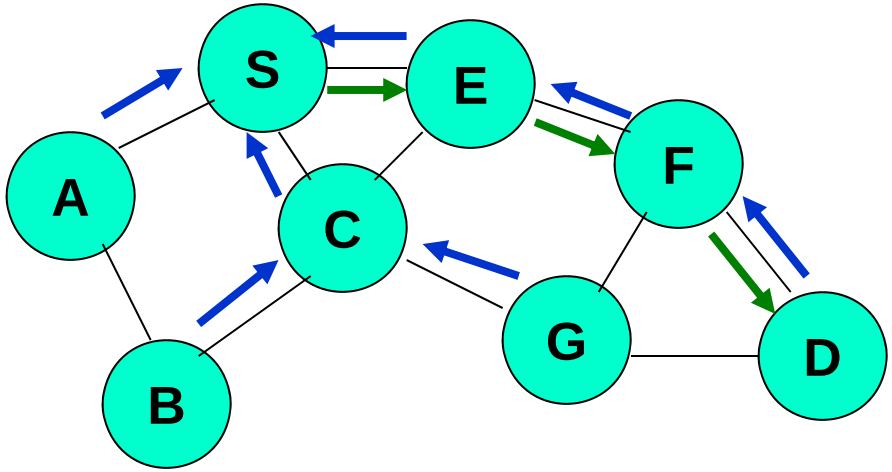
ZigBee Routing

- AODV route discovery is done using:
  - Route Request (RREQ) and Route Reply (RREP) Messages
- RREP message(s) is/are sent through reverse path(s):

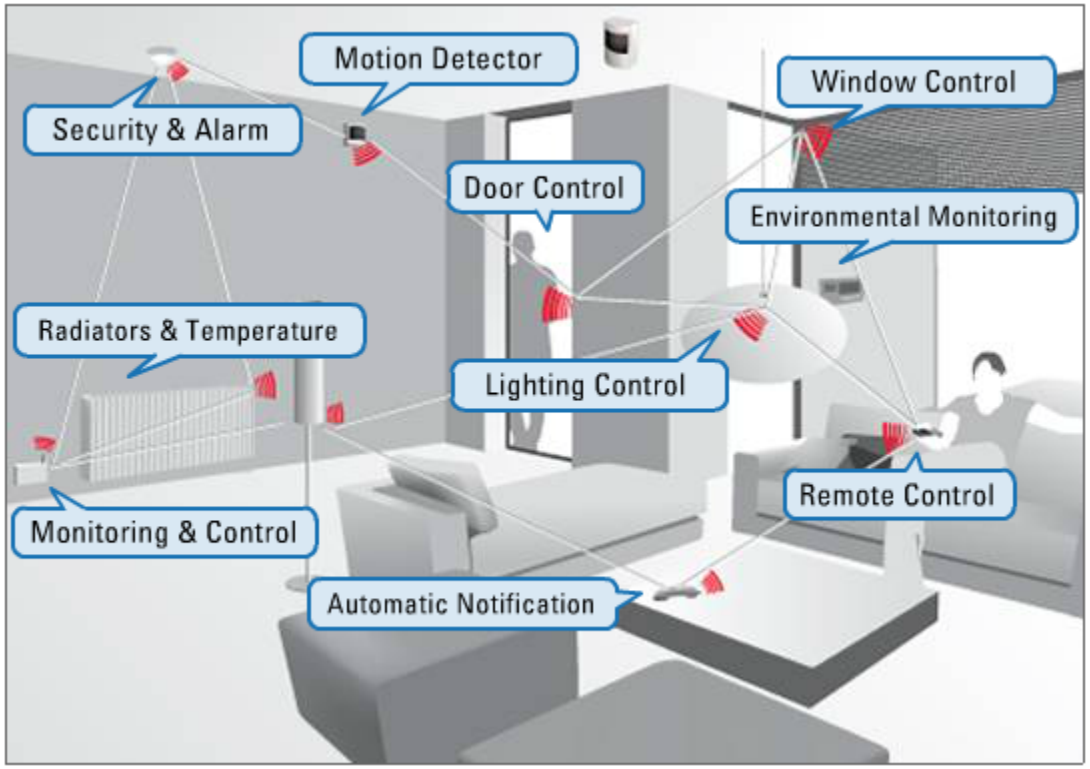


ZigBee Routing

- AODV route discovery is done using:
  - Route Request (RREQ) and Route Reply (RREP) Messages
- This will lead to forming / discovering forward path(s):



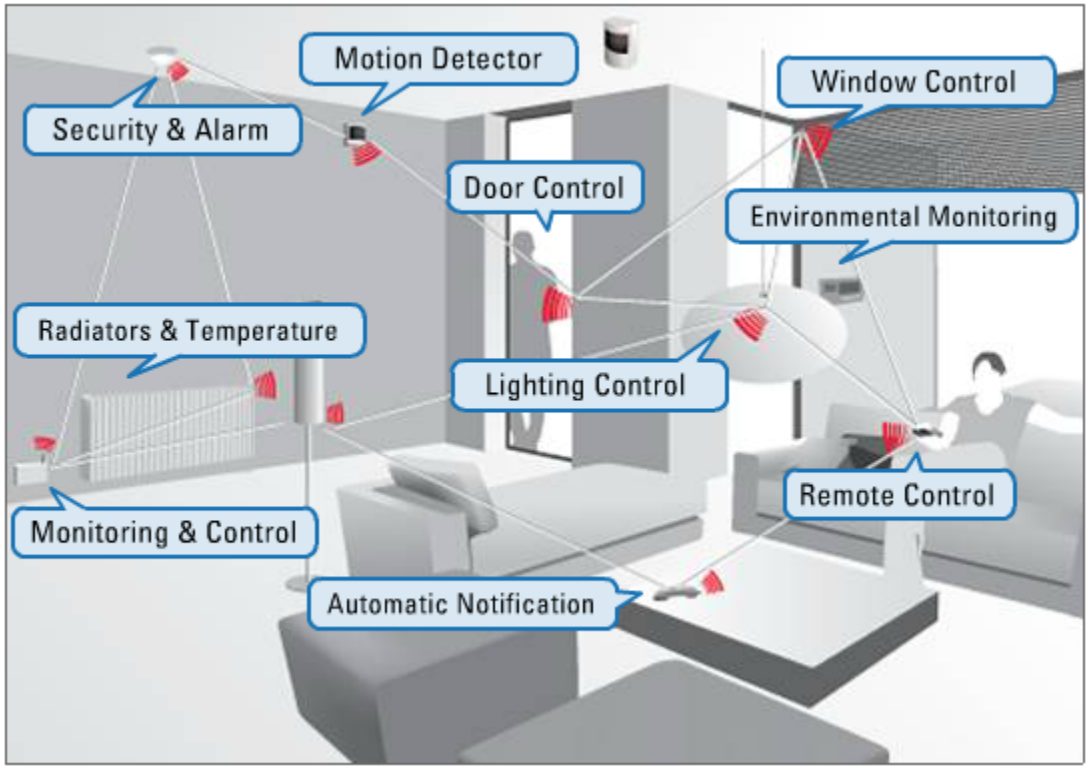
ZigBee Building Solutions



www.ti.com

- Automatic Notification: Call the owner if problem occurs.
- Door Control: When the door is locked, lights are turned off.

ZigBee Building Solutions

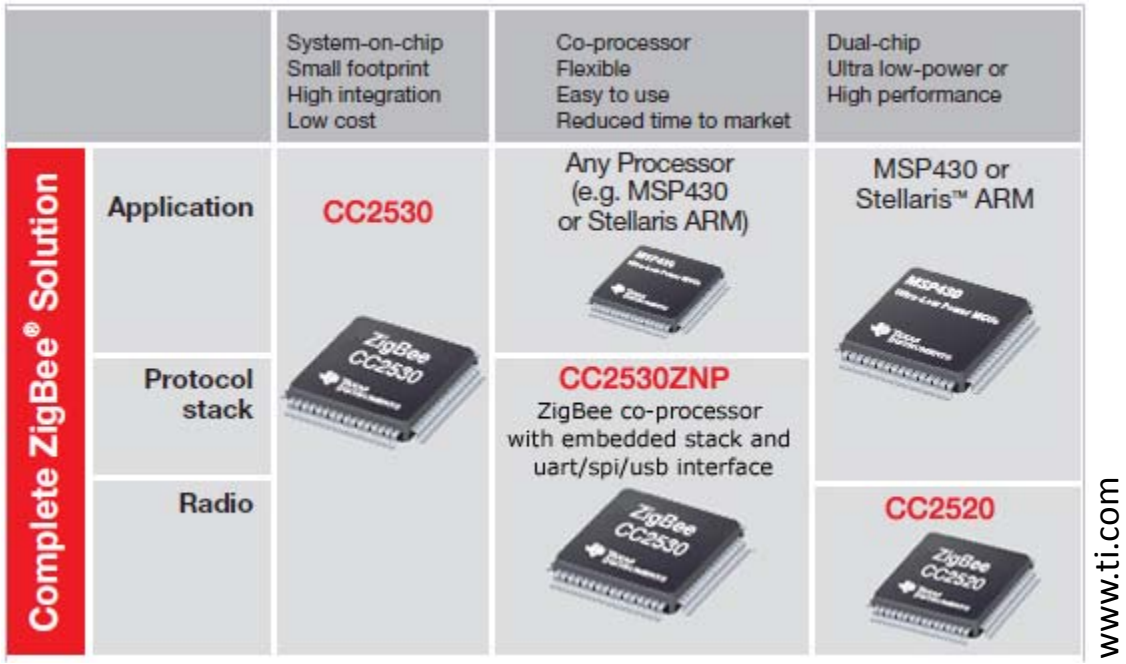


www.ti.com

- Smart appliances can also communicate with smart meters.
- Example: They can obtain prices and adjust their load. (Topic 4!)

ZigBee Building Solutions

•ZigBee solutions by Texas Instrument (TI) at different layers:

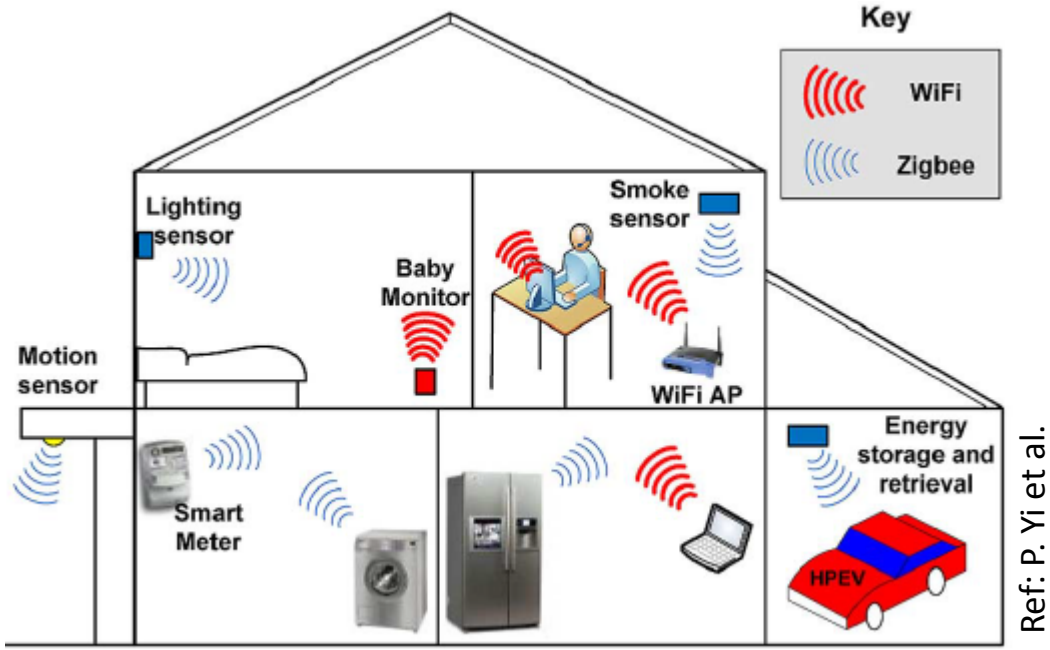


www.ti.com

• Refer to TI's ZigBee pages for more detail.

ZigBee Collocation with WiFi

- ZigBee and WiFi collocate at 2.4 GHz Frequency Band



Ref: P. Yi et al.

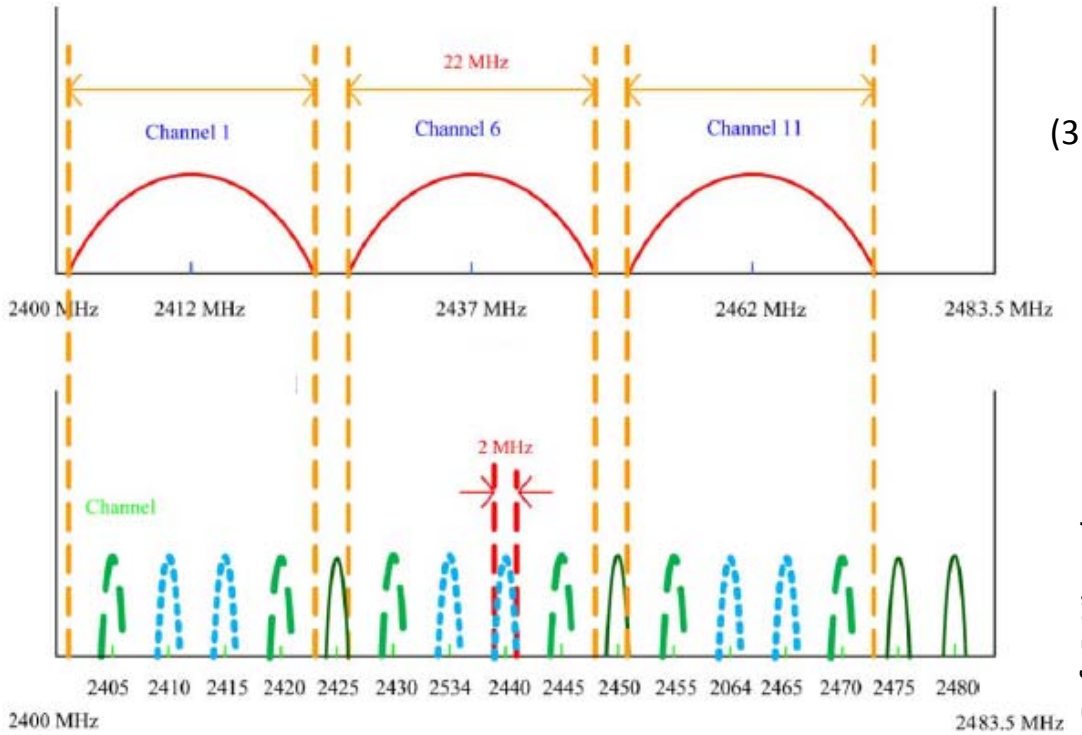
- In addition to medium access control:
  - They should automatically avoid common channels.

ZigBee Collocation with WiFi

- ZigBee and WiFi collocate at 2.4 GHz Frequency Band

WiFi:

ZigBee:



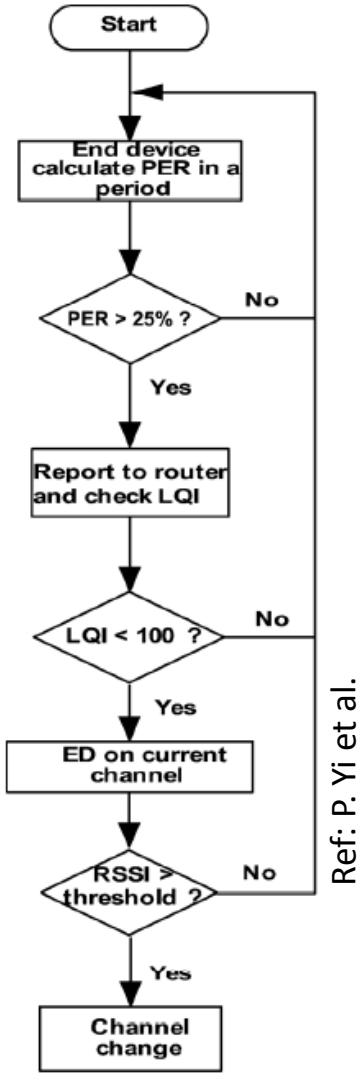
(3 Orthogonal Channels)

Ref: P. Yi et al.

- ZigBee (or WiFi or both) should search for unused channels.

ZigBee Collocation with WiFi

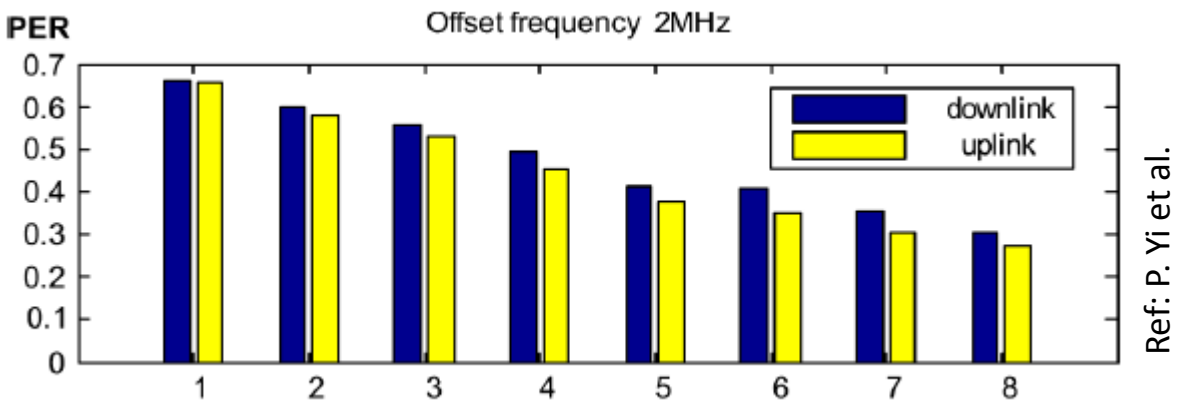
- An Algorithm for ZigBee Channel Switching:
- PER: Packet Error Rate
  - To be checked by End-Device
- LQI: Link Quality Indicator
  - To be checked by Router / Coordinator
  - Strength of Received Packets
  - From 0 to 255 [Strongest]
- ED: Energy Detection
- RSSI: Received Signal Strength Indicator



Ref: P. Yi et al.

ZigBee Collocation with WiFi

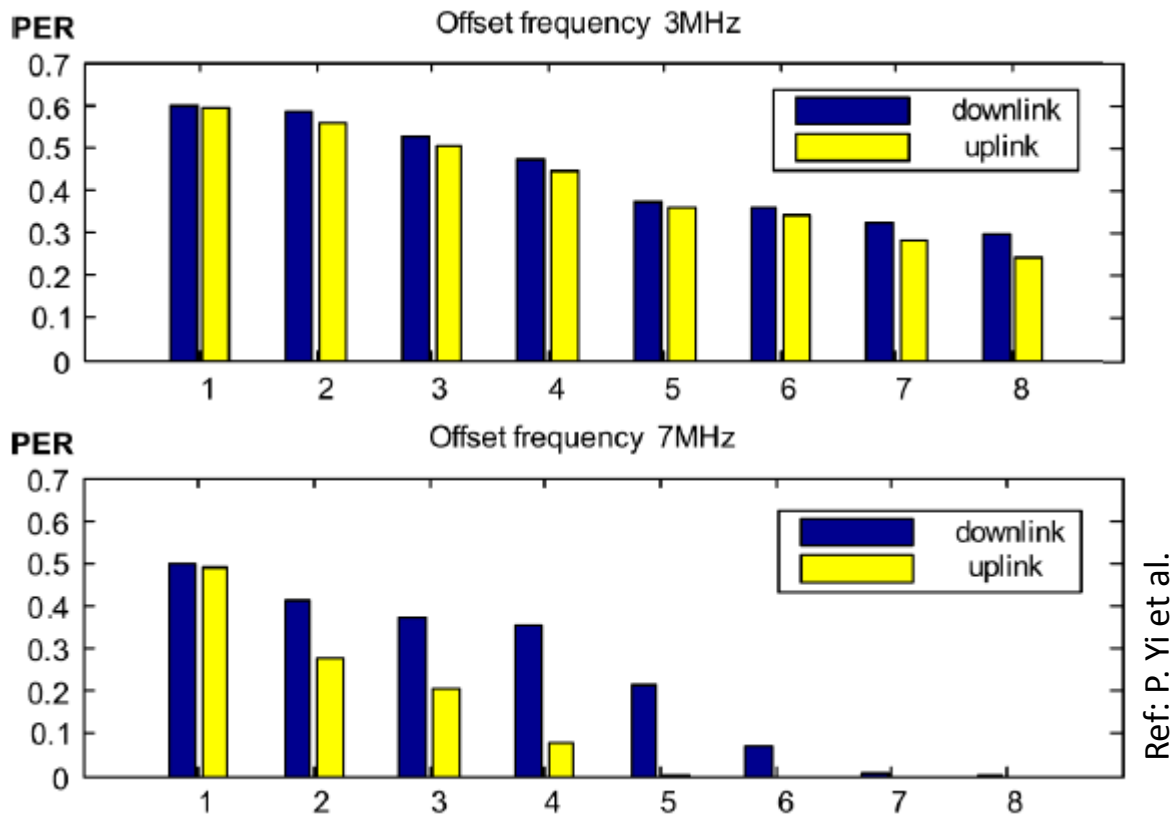
- Experimental Results by P. Yi et al. to obtain:
  - Safe Distance
  - Safe Offset Frequency
- WiFI Uplink and Downlink as source of interference on ZigBee:



PER vs Distance (Meter)

ZigBee Collocation with WiFi

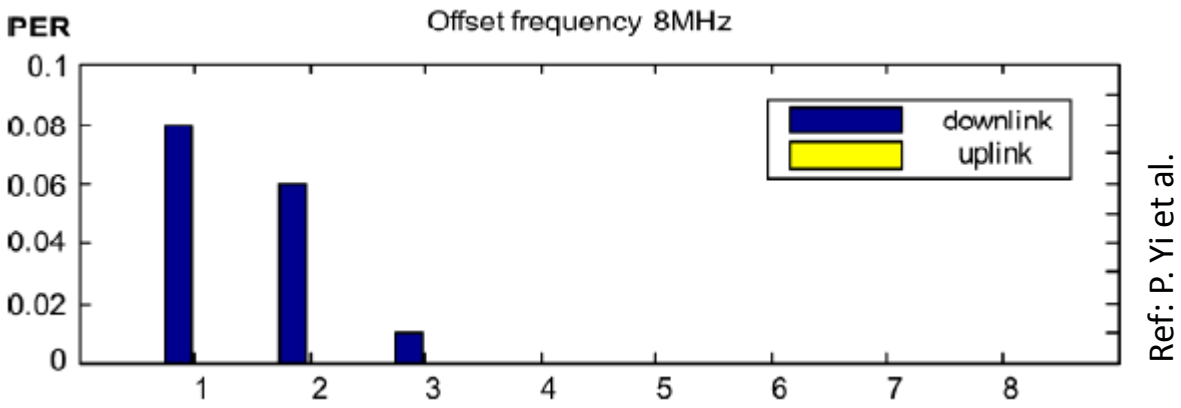
- At 7 MHz Frequency Offset, “Safe Distance” is 5 Meter.



PER vs Distance (Meter)

ZigBee Collocation with WiFi

- 8 MHz is “Safe Frequency Offset” regardless of Distance.



PER vs Distance (Meter)

- We can do similar experiments for other technologies.

- One can also study ZigBee interference on WiFi [the reverse!].

Z-Wave

- An alternative home area networking technology for ZigBee:
  - To resolve ZigBee/WiFi collocation problem.

- Z-Wave operates at around 900 MHz band
  - It does not collocate with WiFi
  - It may compete with some cordless telephones

Z-Wave

- Similar to ZigBee, Z-Wave aims to build a “smart home”:
  - A wireless HAN “ecosystem”

Z-Wave appliances can participate in AMI, AMR, and Demand Response

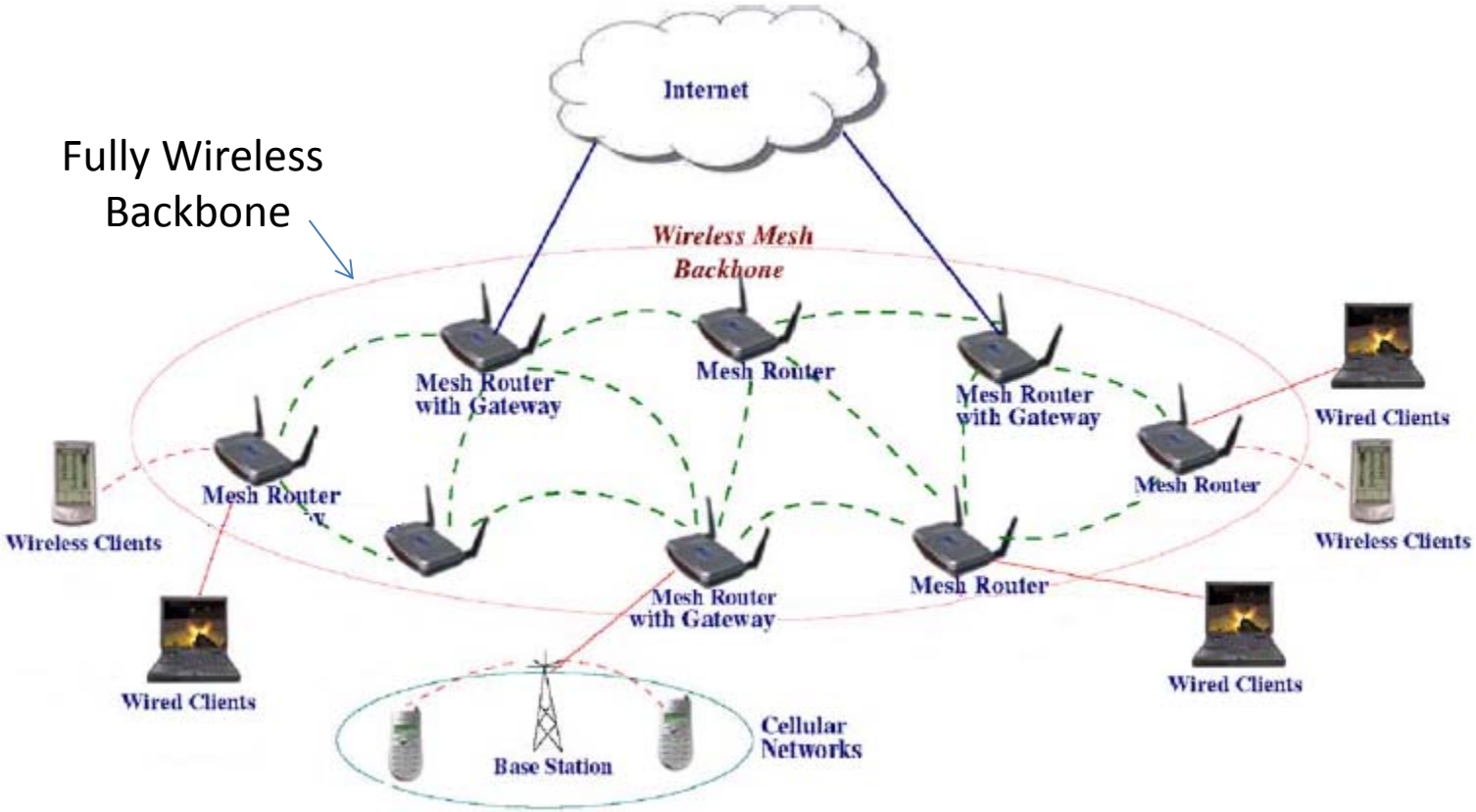
Wireless Mesh Networks (Metropolitan Area)

Wireless Mesh Networks (WMNs)

- WMNs are composed of several wireless access points (routers).
  - Usually WiFi or WiMax Routers
- Together, they create a fully wireless communication backbone:
  - To serve wireless mesh clients (fixed / mobile)
- The WMN can be connected to the Internet or other networks:
  - Through a few gateway routers

Wireless Mesh Networks (WMNs)

- Example: a WMN with Internet and Cellular Connectivity:



Ref: Akyildiz et al.

Wireless Mesh Networks (WMNs)

- Example: Wireless Mesh Routers

(a)

With Two Network Interface Cards (NICs)

(b)

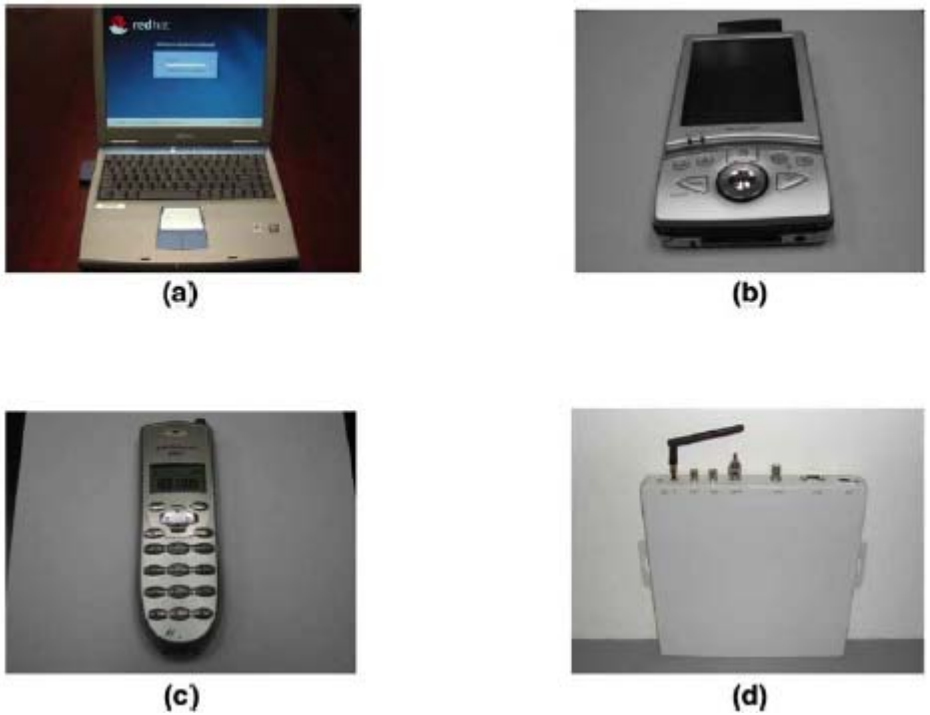
With One Network Interface Card

Ref: Akyildiz et al.

Q: What is the benefit of having multiple NICs on a Wireless Mesh Rouet?

Wireless Mesh Networks (WMNs)

- Example: Wireless Mesh Clients



Ref: Akyildiz et al.

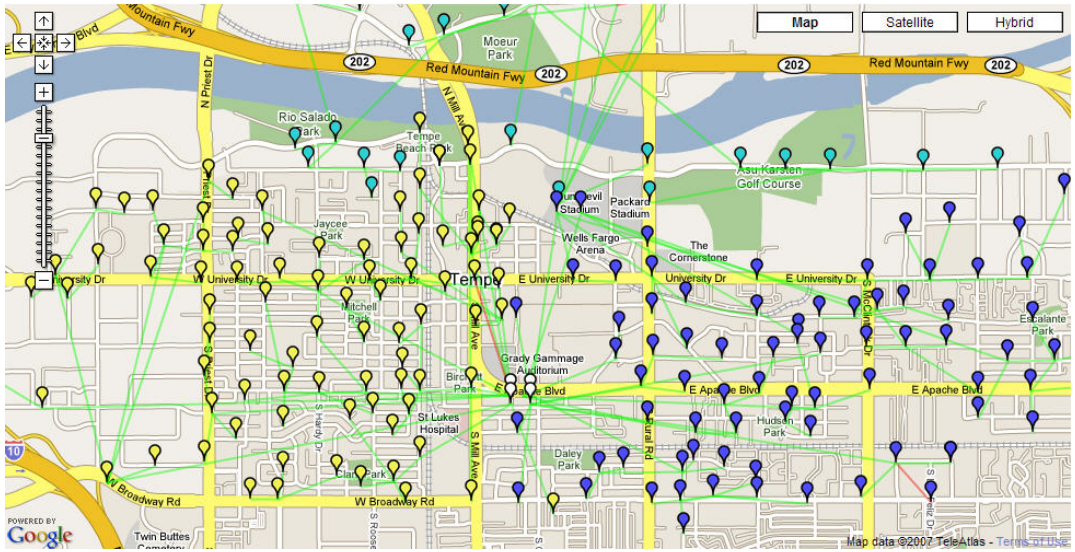
(a) Laptop, (b) PDA, (c) Wi-Fi IP Phone and (d) Wi-Fi RFID Reader.

WMNs Applications Before Smart Grid

- Some of the Initial Applications of WMNs included:
  - Community Networks
  - Enterprise Networks
  - Local Area Networks for Hotels, Malls, Parks, Trains, etc.
  - Metropolitan Area Networks
- City-wide WMNs have been deployed in multiple U.S. cities.

City-Wide Wireless Mesh Networking

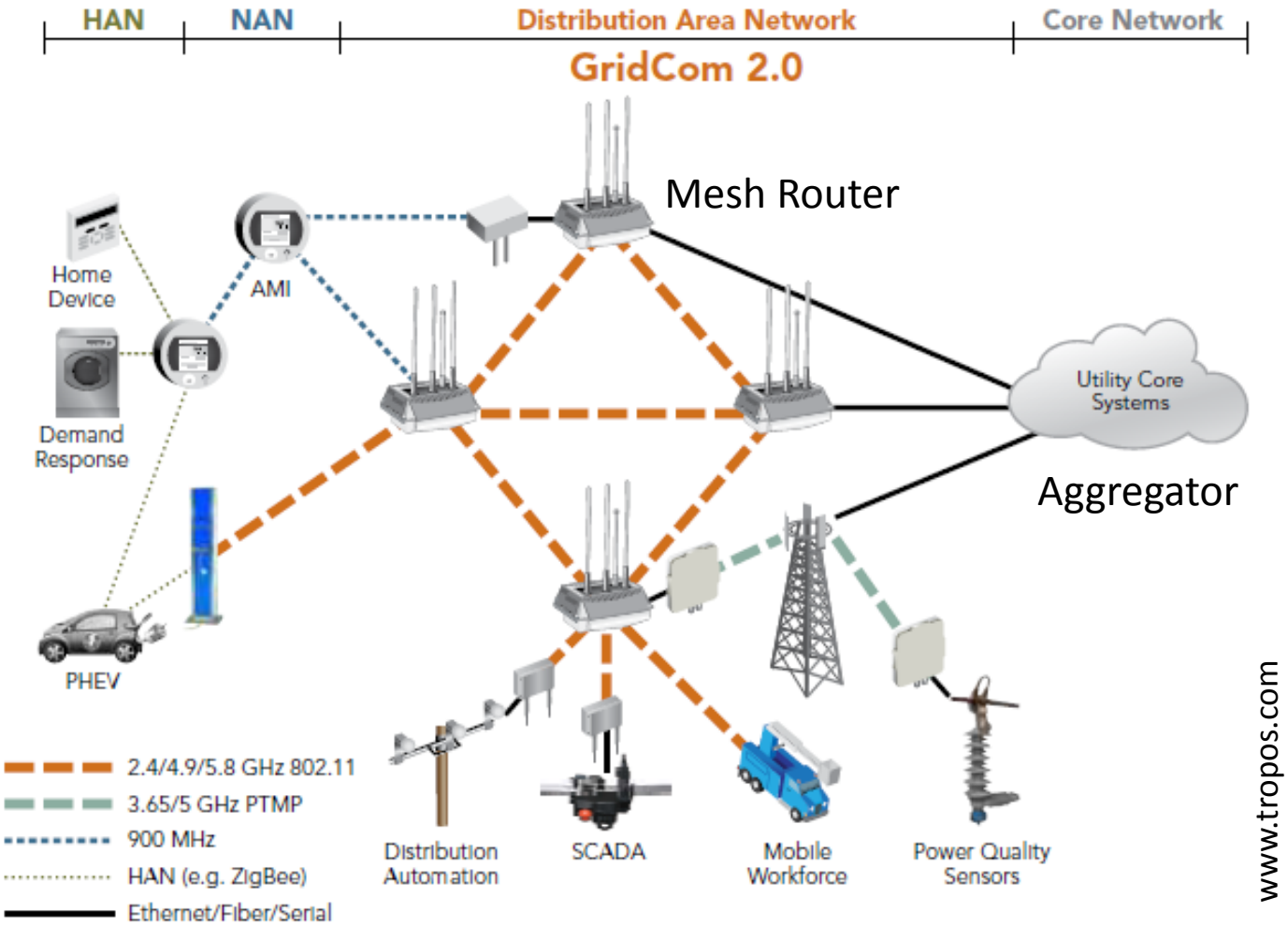
- Tempe, AZ Wireless Mesh Network
- Nearly 600 Mesh Access Points
- Coverage to an Area of 40 Square Miles
- Project Completed in only 120 days!



WMNs Benefits

- Some of the advantages of WMNs:
  - Low up-front costs
  - Ease of incremental deployment
  - Ease of maintenance
- The wireless mesh clients can also be:
  - Smart Meters, Sensors, Sub-stations, etc.

WMNs for Smart Grid Communications



Video to Watch: http://www.youtube.com/watch?v=09dhjDcaT7g

Tropos Wireless Mesh Routers for Smart Grid

Tropos 1410 Wireless Mesh Routers

Wireless Technology: IEEE 802.11b/g/n

Frequency Band: 2.4-2.483 GHz

Media Access Protocol: CSMA/CA with ACK

Dimensions: 15.16” high x 6.97” wide x 2.01 deep

Weight: 4.0 lbs

Wind survivability: >165 mph

Communication Range: About 100 m

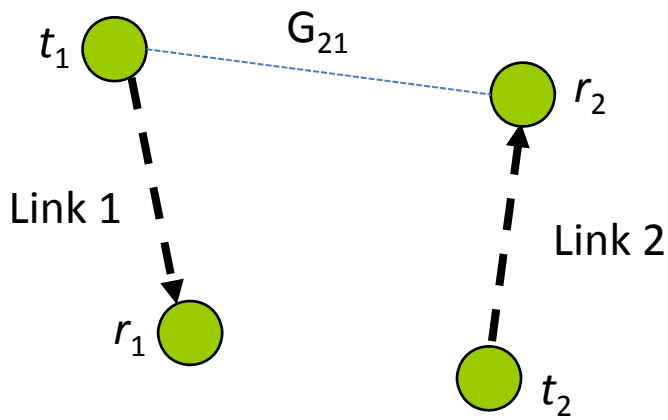
WMNs Challenges

- Key challenges in WMNs:
  - Wireless Interference and Frequent Collisions
  - Wireless Multi-hop Transmissions (e.g., for TCP connections)
  - Congestion at Gateways (Q: Why?)

- DoE has requirements for Smart Grid Communications [will see]:
  - Packet Loss and Delay (Q: How can we assure these?)

Modeling Packet Loss in WMNs

- Consider two wireless links *i* and *j*:
  - P_i: transmit power of link i's transmitter node
  - G_{ij}: channel gain from link j's transmitter to link i's receiver.



- A simple model for $G_{ij} = k\,(d_{ij})^{-2}$, where d_{ij} is the distance.

Modeling Packet Loss in WMNs

- Received Signal Power at link i's receiver node:

$$G_{ii}P_i$$

- Received Interference Power at link i's receiver from j's transmitter

$$G_{ij}P_j$$

- Similarly, we can obtain interference power from all other links.

Modeling Packet Loss in WMNs

- We can define signal to interference ratio (SIR) for link i as:

$$SIR_i = \frac{G_{ii} P_i}{\sum_{k \neq i} G_{ik} P_k}$$

$G_{ii} P_i$ → Signal Power

$\sum_{k \neq i} G_{ik} P_k$ → Aggregate Interference Power

- For correct reception of the packet, it is required that

$$SIR_i \geq SIR^{th} \quad \text{(Threshold)}$$

- Otherwise, the packet is lost.

Modeling Packet Loss in WMNs

- The probability of losing the packet on link i:

(Outage)

$$O_i = \text{Prob}\left\{SIR_i < SIR^{th}\right\}$$
$$= \text{Prob}\left\{G_{ii}P_i < SIR^{th}\sum_{k\neq i} G_{ik}P_k\right\}$$

- Key Question: Why are we talking about "probability" here?
  - What is the "stochastic/random" part?

Modeling Packet Loss in WMNs

- Obviously not all nodes transmit at all times!

- We assume some random distribution for packet transmission.

- If nodes transmit following independent exponential distributions:

$$O_i = 1 - \prod_{k \neq i} \frac{1}{1 + \frac{SIR^{th} G_{ik} P_k}{G_{ii} P_i}}$$

[Proof: See Appendix I in IEEE TWC paper by S. Kandukuri and S. Boyd]

Modeling Packet Loss in WMNs

- Let us consider the packet loss model again:

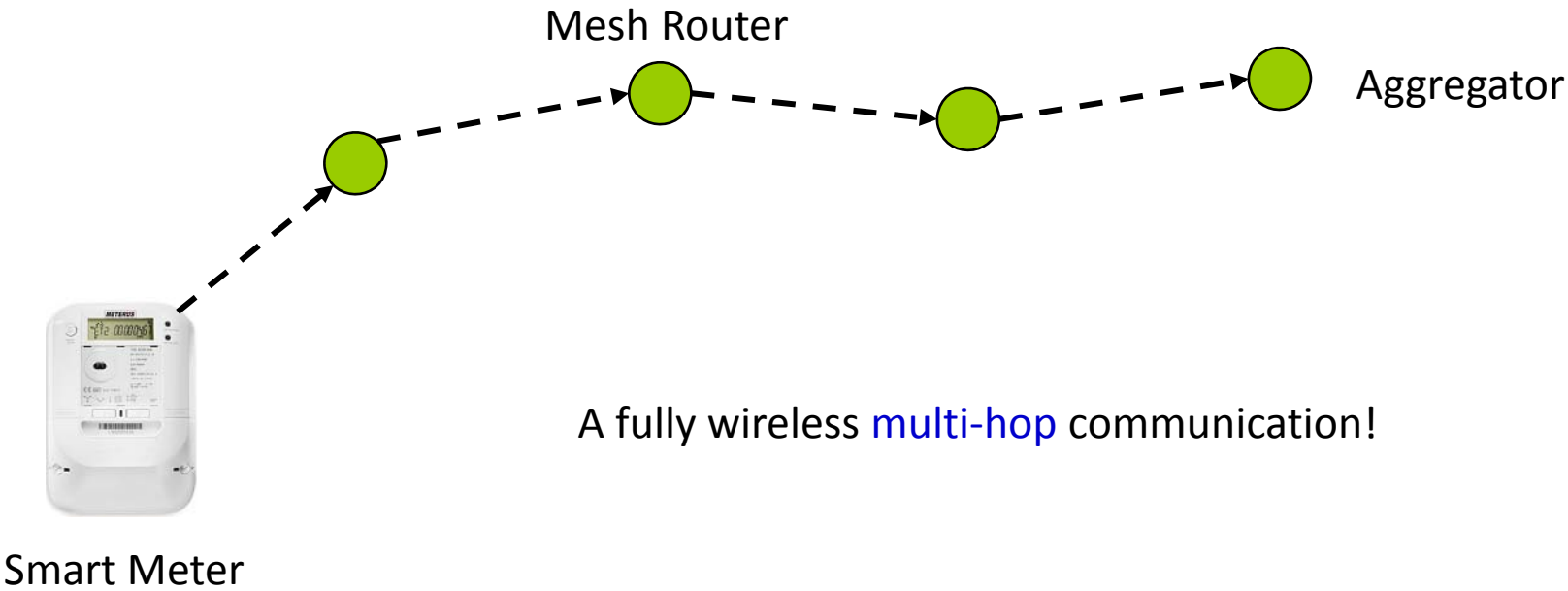
$$O_i = 1 - \prod_{k \neq i} \frac{1}{1 + \frac{SIR^{th} G_{ik} P_k}{G_{ii} P_i}}$$

- Probability of packet loss increases If:
  - Link i transmits with lower power
  - Interfering links transmit with higher power
  - Interfering links get closer
  - There are more interfering links in the neighborhood

Modeling Packet Loss in WMNs

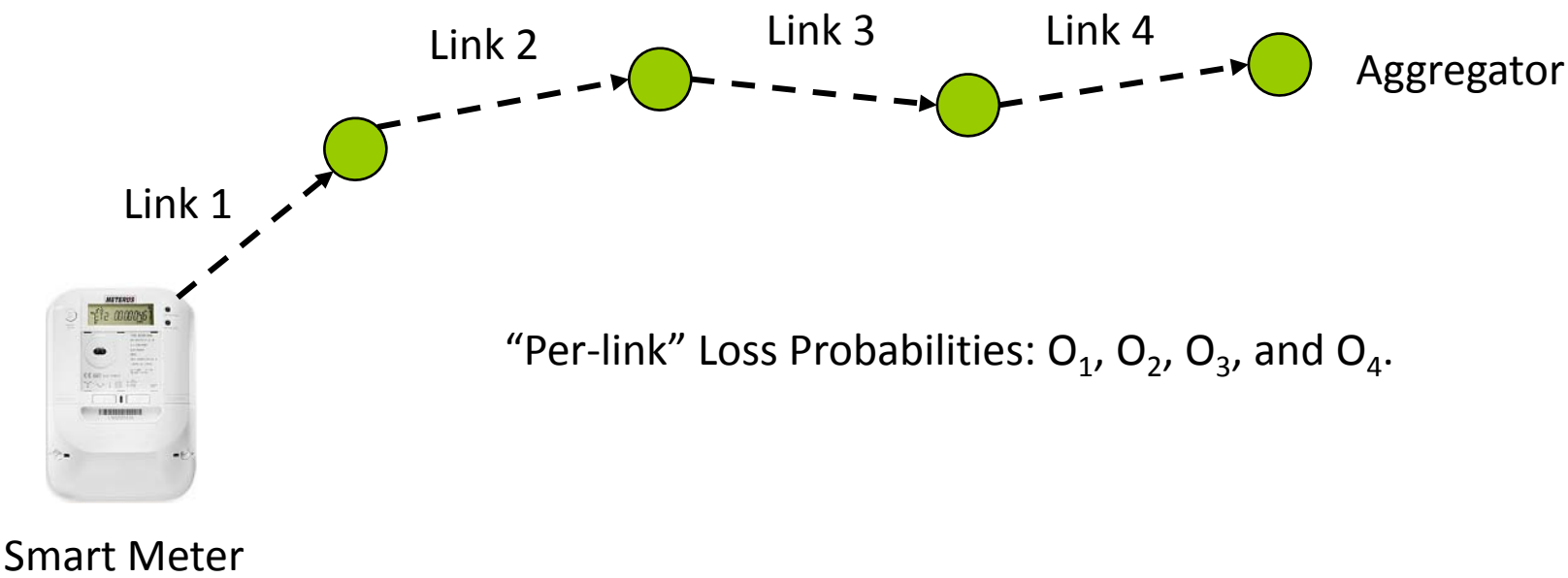
- The model so far only gives “per-link” packet loss.

- Q: How about end-to-end packet loss probability?



A fully wireless multi-hop communication!

Modeling Packet Loss in WMNs



"Per-link" Loss Probabilities: O_1, O_2, O_3, and O_4.

- End-to-end Probability of Packet Loss (Q: Why?):

$$O_{Path} = 1-(1-O_1)(1-O_2)(1-O_3)(1-O_4)$$

Modeling Packet Loss in WMNs

- In general, for a path with *R* as the set of wireless links:

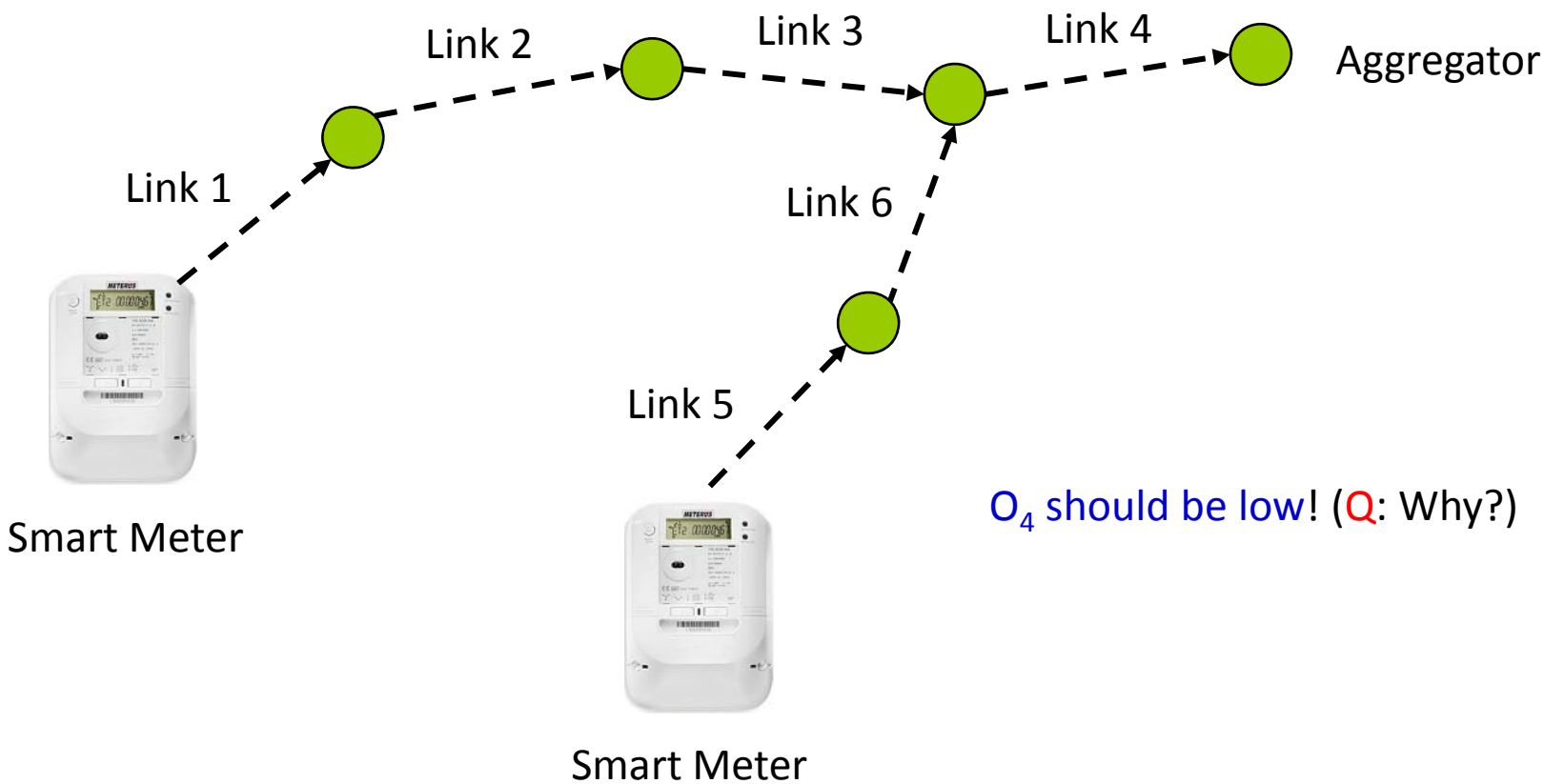
$$O_{Path} = 1 - \prod_{i \in R} (1 - O_i)$$

- For each path in WMN (e.g., AMI), we can calculate O_{path} if know
  - Locations of the mesh routers and clients (channel gains)
  - Transmit power of mesh routers and clients
  - The SIR threshold values for the technology being used

[Example: You can check if it satisfies the DoE requirements!]

Modeling Packet Loss in WMNs

- We want low "per-link" loss rates for links closer to aggregator:



O_4 should be low! (Q: Why?)

Modeling Packet Loss in WMNs

- Q: How can we assure required packet loss bounds for all path?

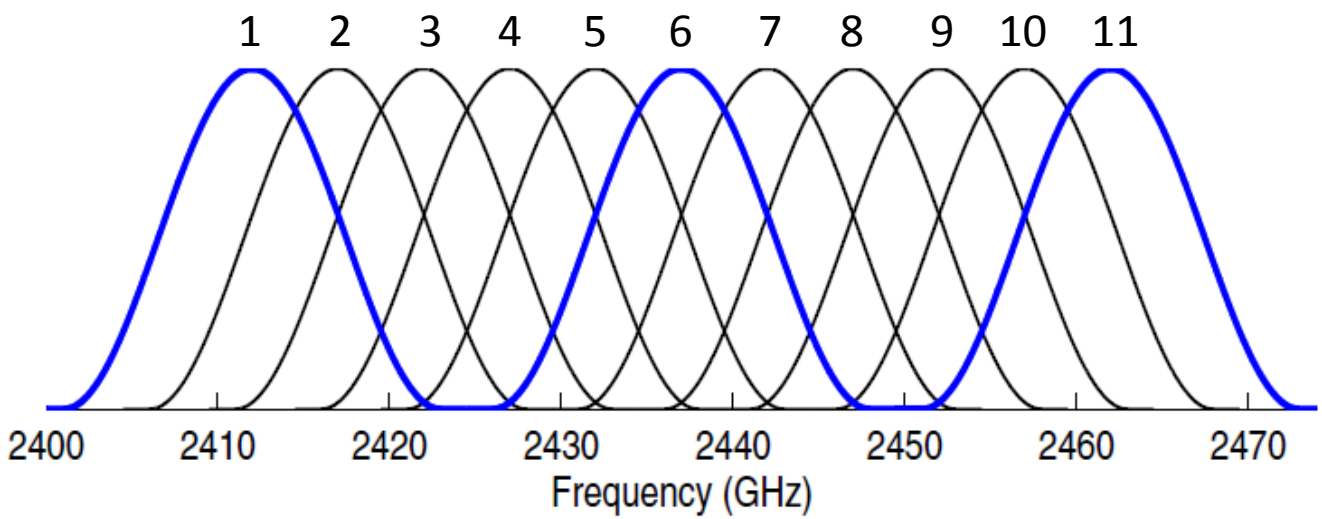
- First of all, we should not have paths that are too long!
  - This requires having several gateways in large WMNs.

- Second, we need to do resource management:
  - Power allocation, channel assignment, etc.

Channel Assignment in WMNs

- Assume that we use WiFi technology for our WMN.

- Let us look at the available 11 channels in IEEE 802.11b:

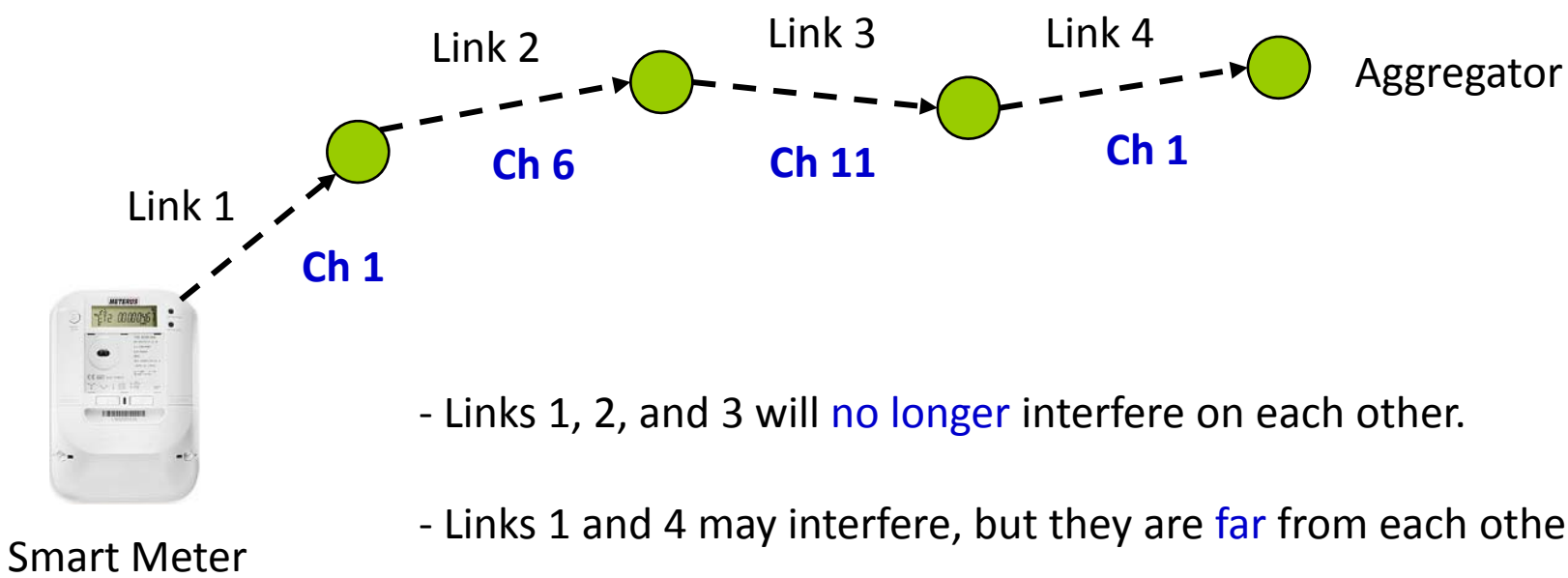


Partially Overlapping: 1 and 2

Non-Overlapping: 1 and 6 and 11

Channel Assignment in WMNs

- We assign different non-overlapping channels to different links:



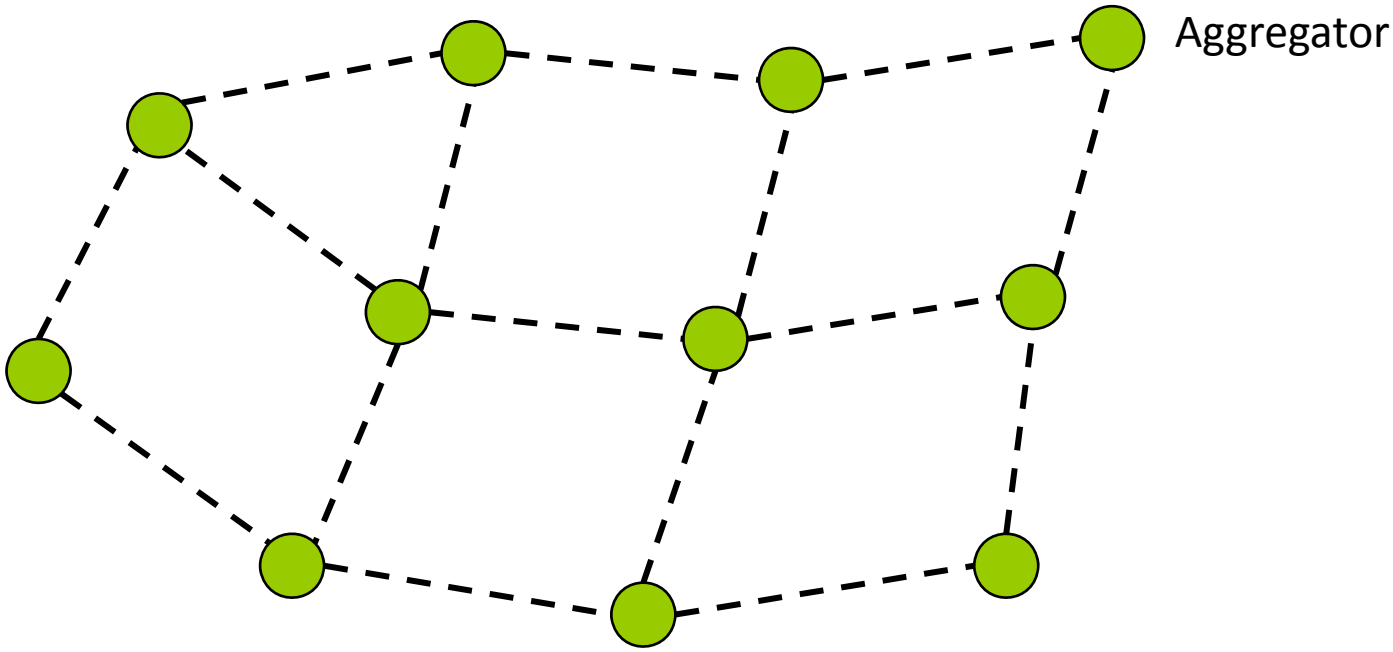
- Links 1, 2, and 3 will no longer interfere on each other.

- Links 1 and 4 may interfere, but they are far from each other.

Such multi-channel deployment requires mesh routers with multiple NICs. (Q: Why?)

Channel Assignment in WMNs

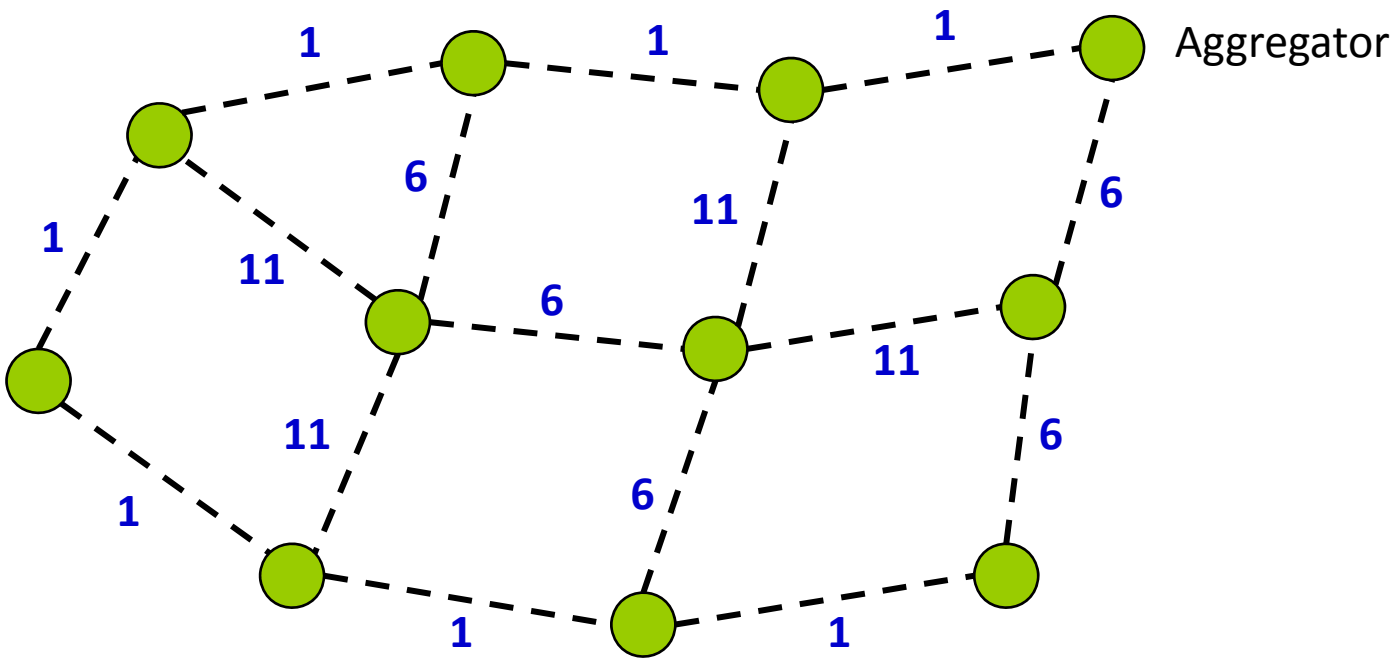
- Same idea applies to a more complex network:



- Channel assignment depends on the number of NICs per node.

Channel Assignment in WMNs

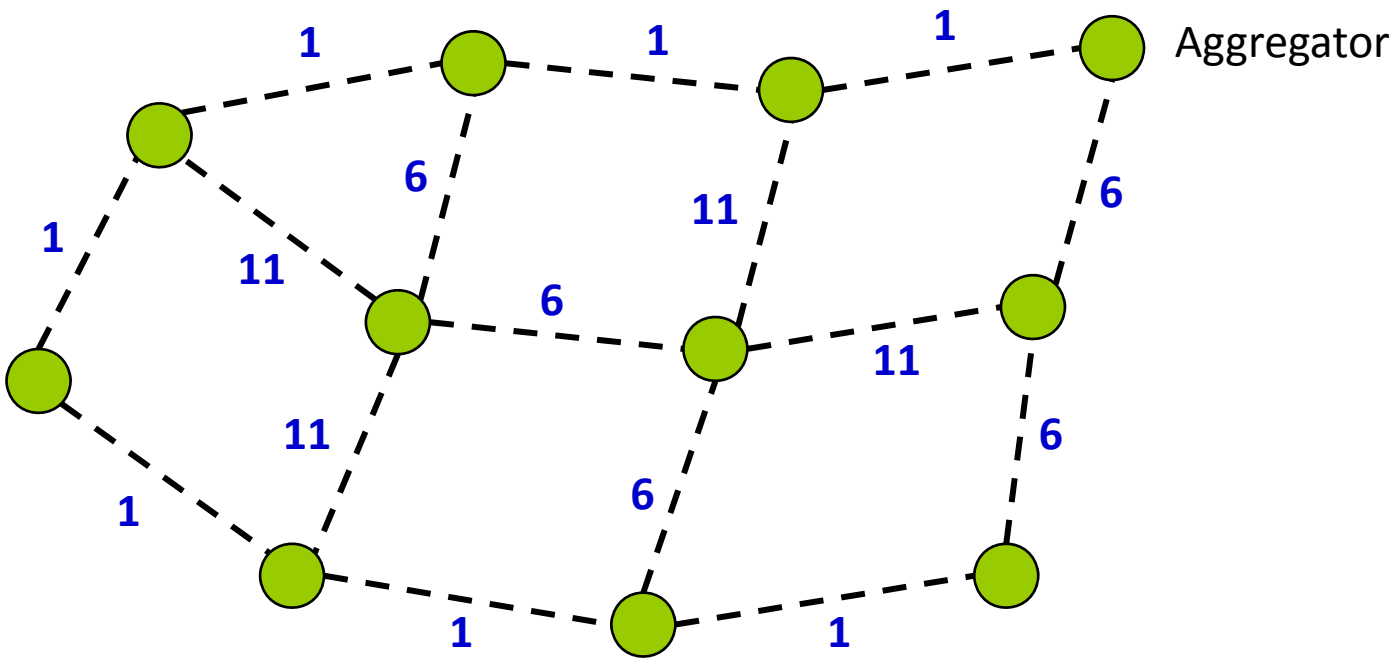
- Same idea applies to a more complex network:



- Channel assignment depends on the number of NICs per node.

Channel Assignment in WMNs

- Same idea applies to a more complex network:



- Knowing NIC = 2: Q: Do you see more than 2 channels per node?

Channel Assignment in WMNs

- Here, we have three different contention domains:
  - **Channel 1**: Seven Links
  - **Channel 6**: Five Links
  - **Channel 11**: Four Links
- Note that links on channel 1 are far from each other
  - We can better remove interference with more channels/NICs.

ATCP for WMNs

- When it comes to wireless networks:
  - Packet loss due to link failure/interference can affect TCP.
  - The problem: TCP back-off every time a packet is lost.
- One Solution: Ad-hoc Transmission Control Protocol (TCP)
- ATCP uses network feedback:
  - ICMP Destination Unreachable (when a path breaks)
  - Early Congestion Notification (when there is congestion)

ATCP for WMNs

- The key idea: We want to distinguish:
  - Packet loss due to congestion
  - Packet loss due to wireless interference/collision

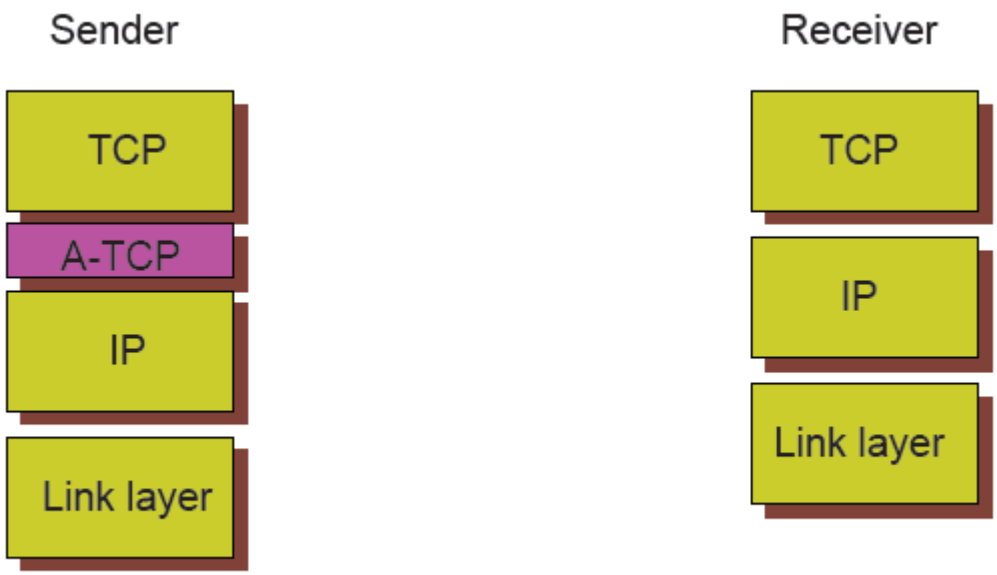
- ECN Flags: Indication of congestion

- Timeout and 3 duplicate ACKs: Indication of collision/link problem

[Link problems can be because of mobility]

ATCP for WMNs

- ATCP in the TCP/IP Stack:



- It only affects the TCP sender side. It is a cross-layer solution.

ATCP for WMNs

- ATCP / TCP Behavior:
  - Timeout and 3rd Duplicate ACK:
    - Retransmit the segment
    - No Congestion Control Reaction
    - Assumed to be due to link collision
  - ACK with ECN Flag:
    - Invokes Congestion Control

ATCP for WMNs

- ATCP / TCP Behavior:
  - ICMP Destination Unreachable Message:
    - Stops Transmission
    - Enters “Persist Mode”
    - Starts Persist Timer
      - Probes for Path Availability when Timer Expires
    - Resume Transmission when New Path Found

IEC 61850
(Communications of Substations)

IEC 61850 Overview

- IEC: International Electrotechnical Commission

- IEC 61850
  - Smart Grid Communications Standard
  - Communications across Intelligent Electronic Devices (IEDs)
    - Focus: Sub-stations (but also supports meters, etc.)
  - Runs over TCP/IP networks

IEC 61850 Overview

- Example Sub-station:

Ref: ABB Switzerland Ltd Corporate Research

IEC 61850 Overview

- IEC 61850 Aims to provide inter-operability

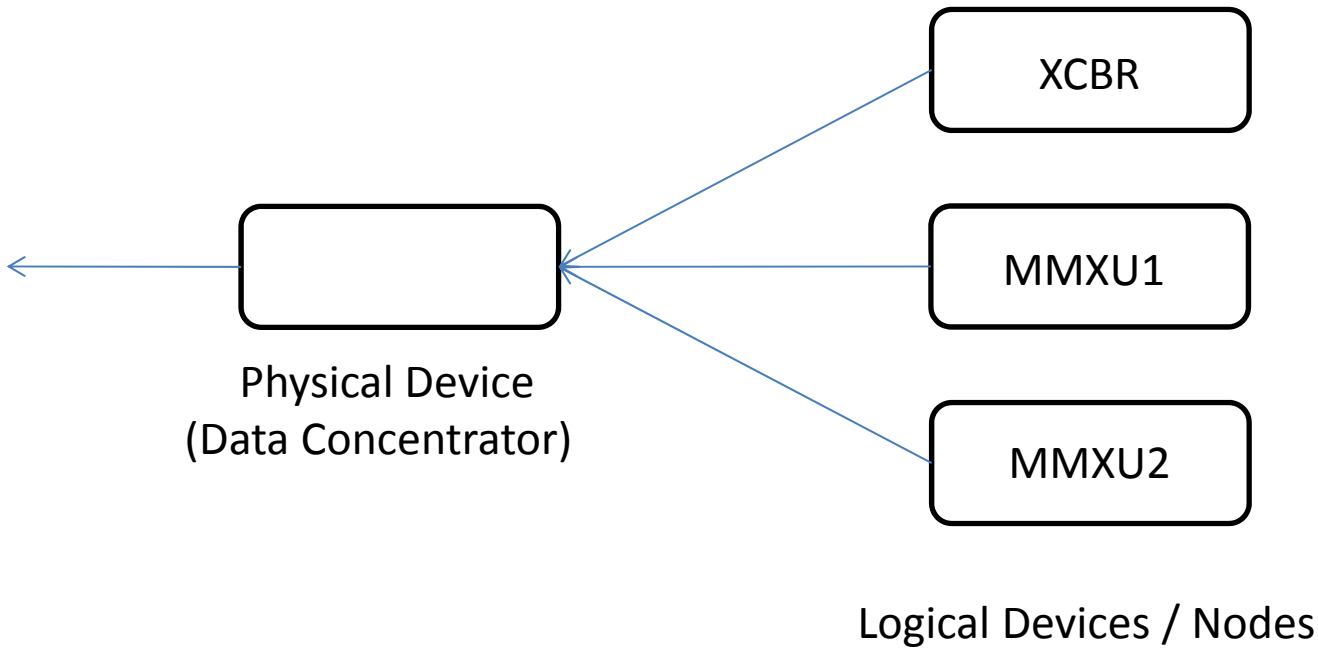
- Key focus: IEC 61850 provides a comprehensive model for how power system devices should organize data in a manner that is consistent across all types and brands of devices.

- The IEC 61850 devices are intended to be plug-and-play.

- They are configured by uploading simple configuration files.

IEC 61850 Overview

- IEC 61850 Network Architecture:



- XCBR: Circuit Breaker, MMXU1: Measurement Unit for Feeder 1, …

IEC 61850 Overview

- Data types to be transmitted for each logical device:
  - Should follow certain specifications:

XCBR Class				
DATA NAME	COMMON DATA CLASS	DESCRIPTION	T	MANDATORY/ OPTIONAL
LNName	Secure	Shall be inherited from Logical-Node Class (see IEC 61850-7-2)		
DATA				
Common Logical Node Information				
		LN shell inherit all Mandatory Data from Common Logical Node Class		Mandatory
Loc	SPS	Local operation (local means without substation automation communication, hardwired direct control)		Mandatory
EE Health	INS	External equipment health		Optional
EE Name	DPL	External equipment name plate		Optional
OpCnt	INS	Operation counter		Mandatory

Object Name

Data Class Name (Data Structure)

IEC 61850 Overview

- Data types to be transmitted for each logical device:

XCBR Class (Cont.)				
DATA NAME	COMMON DATA CLASS	DESCRIPTION	T	MANDATORY/ OPTIONAL
Controls				
Pos	DPC	Switch position		Mandatory
BlkOpn	SPC	Block opening		Mandatory
BlkCls	SPC	Block closing		Mandatory
ChaMotEna	SPC	Charger motor enabled		Optional
Metered Values				
SumSwARs	BCR	Sum o Switched Amperes, resetable		Optional
Status Information				
CBOpCap	INS	Circuit breaker operating capability		Mandatory
POWCap	INS	Point on Wave switching capability		Optional
MaxOpCap	INS	Circuit breaker operating capability when fully charged		Optional

Object Name

Data Class Name (Data Structure)

IEC 61850 Data Classes

- Example: SPS: Single Point Status

SPS Class					
ATTRIBUTE NAME	ATTRIBUTE TYPE	FUNCTIONAL CONSTRAINT	TRGOP	VALUE / VALUE RANGE	MANDATORY/ OPTIONAL
DataName	Inherited from Data Class (see IEC 61850-7-2)				
DATA ATTRIBUTE					
Status					
stVal	BOOLEN	ST	dchg	TRUE|FALSE	Mandatory
q	Quality	ST	qchg		Mandatory
t	TimeStamp	ST			Mandatory
Substitution					
subEna	BOOLEN	SV			PICS_SUBST
subVal	BOOLEN	SV		TRUE|FALSE	PICS_SUBST
subQ	Quality	SV			PICS_SUBST
subID	VISIBLE STRING64	SV			PICS_SUBST
Configuration, description and extension					
d	VISIBLE STRING255	DC		Text	Optional
dU	UNICODE STRING255	DC			Optional
cdcNs	VISIBLE STRING255	EX			AC_DLNDA_M
cdcName	VISIBLE STRING255	EX			AC_DLNDA_M
dataNs	VISIBLE STRING255	EX			AC_DLN_M

ST: Status

DC: Description

SV: Substitution

IEC 61850 Data Classes

- Other Data Classes:
  - Status information (binary, integer):
    - **SPS**: Single Point Status
    - **DPS**: Double Point Status
    - **INS**: Integer Status
    - **ACT**: Protection Activation info
    - **ACD**: Activation Info Directional Protection
    - **SEC**: Security Violation Counting
    - **BCR**: Binary Counter Reading

IEC 61850 Data Classes

- Other Data Classes:
  - Control Status:
    - **SPC**: Single Point Control
    - **DPC**: Double Point Control
    - **INC**: Integer Status Control
    - **BSC**: Binary Controlled Step Position Info
    - **ISC**: Integer Controlled Step Position Info
- Just like the example for SPS, each item has a data structure.

IEC 61850 Logical Nodes

- Recall that we used names **X**CBR, **M**MXU1, … for logical nodes.

- The first letter indicates the type for the logical node:
  - **X**: Switchgear
  - **M**: Metering and Measurement
  - **A**: Automatic Control
  - **C**: Supervisory Control
  - **G**: Generic Function

IEC 61850 Logical Nodes

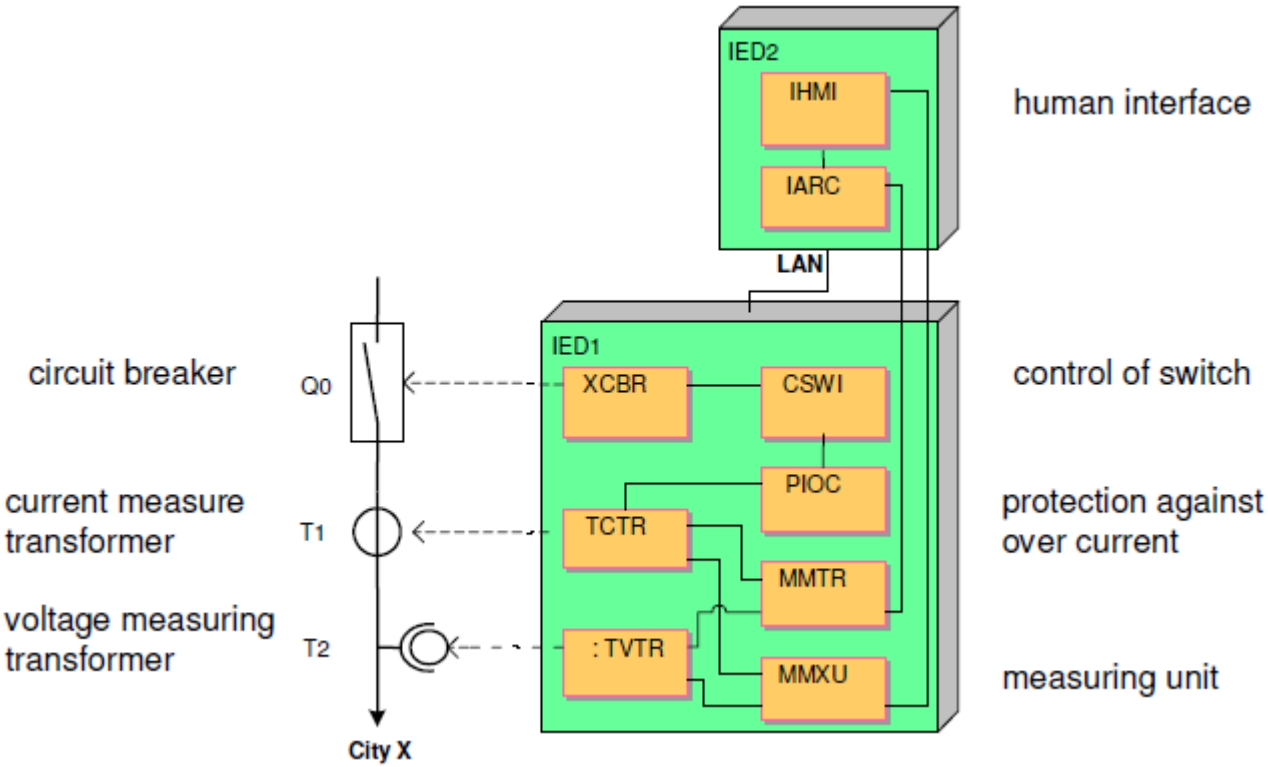
- Recall that we used names **X**CBR, **M**MXU1, … for logical nodes.

- The first letter indicates the type for the logical node:
  - **I**: Interfacing
  - **P**: Protection
  - **S**: Sensors
  - **T**: Instrument Transformer
  - **Y**: Power Transformers

Z: Other devices

IEC 61850 Logical Nodes

- Example: Can you identify different logical nodes?

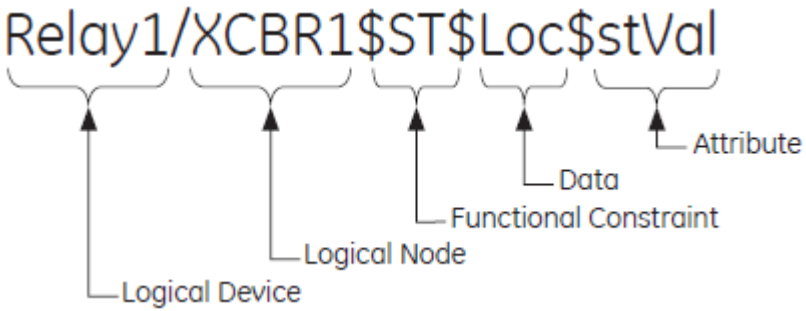


Ref: ABB Switzerland Ltd Corporate Research

IEC 61850 Logical Nodes

- IEC 61850 gives an object-oriented model for communications.

- Example for Object Names:



- We would like to know if the circuit breaker logical node XCBR1 in logical device Relay 1 is in the remote or local mode of operation.

IEC 61850 Logical Nodes

- The object names are used to form MMS messages:
  - MMS: Manufacturing Messaging Specification
- The messages are exchanged as application-layer messages.
- The MMS messages are exchanged over TCP/IP networks
  - LAN
  - Web-Based

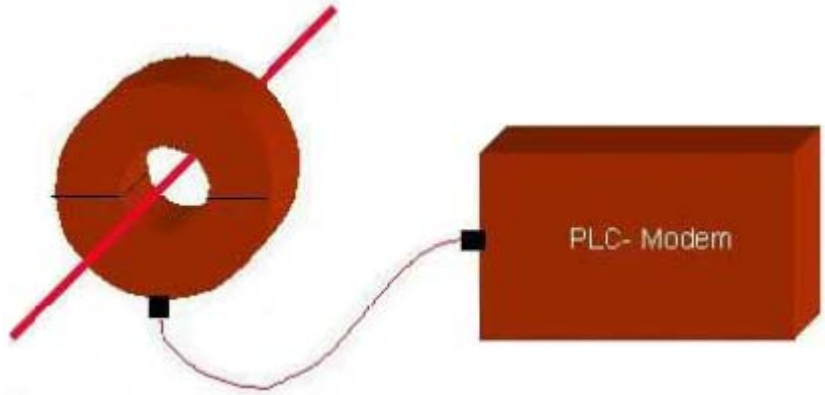
Power Line Communications

PLC Overview

- Power Line Communications (PLC):
  - Carrying data on a conductor also used for power transmission
- PLC is a wired communications technology
  - But it can compete with wireless technologies with low cost
  - Because the infrastructure already exists
- Harsh environment of the power transmission lines.

PLC Overview

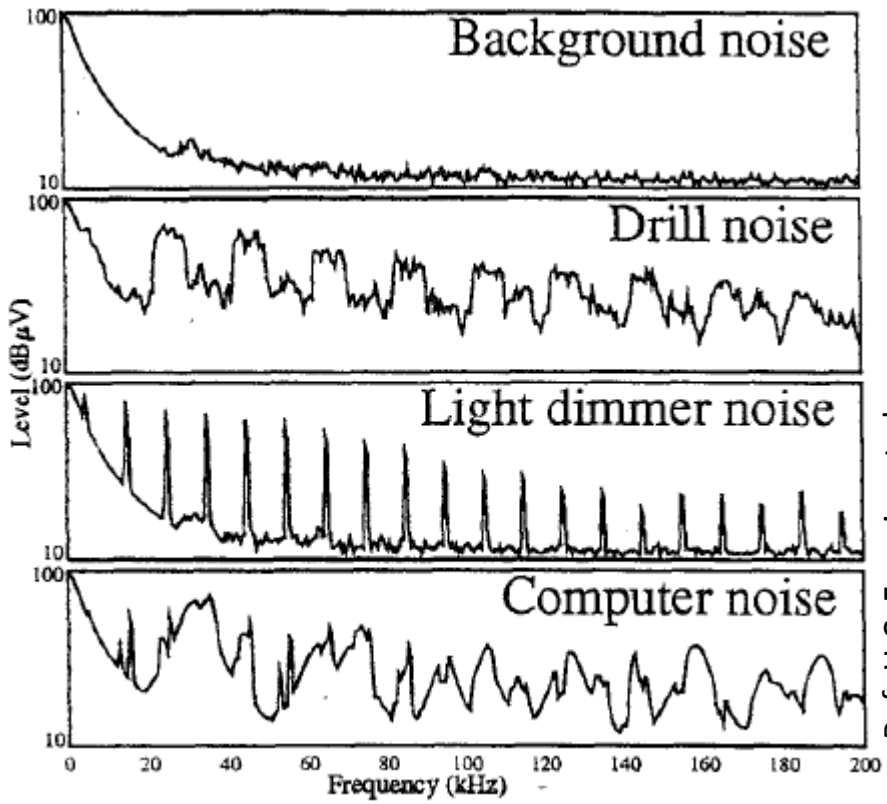
- Idea:
  - Digital signal to be transmitted is modulated over power line.
  - This is done by a proper coupler device.
  - The signal is propagated over the power line.
  - It will be decoupled and decoded at the receiver side.



Inductive coupler
PLC-Modem

PLC Overview

- Harsh Noise Environment:



Ref: H.C. Ferreira et al.

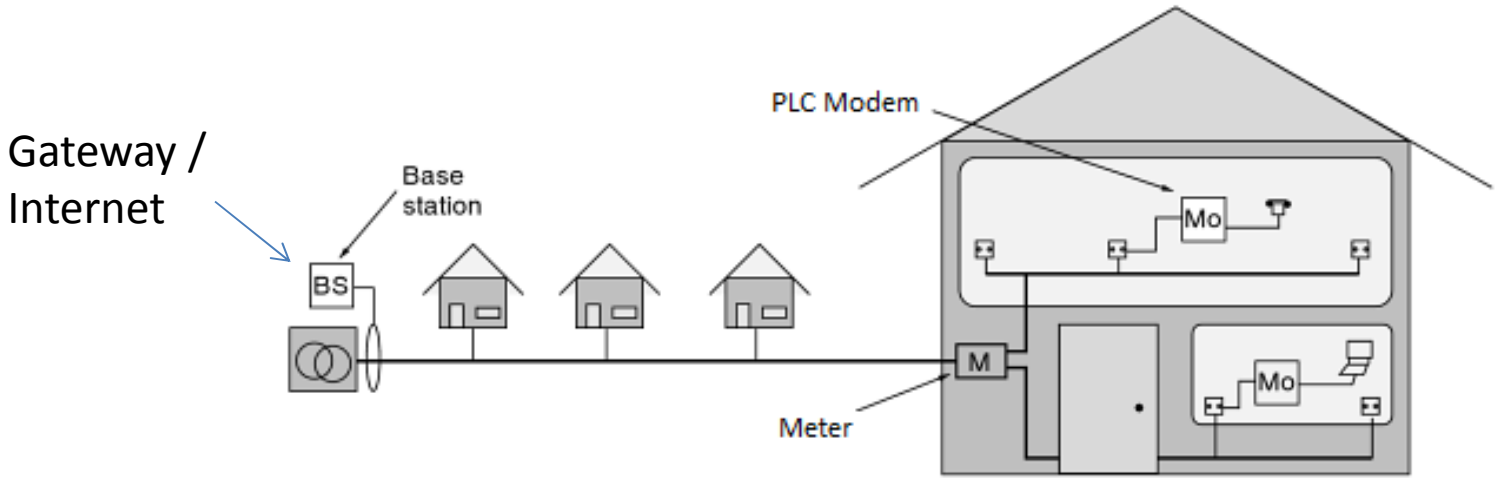
Power spectral densities of noise due to various sources

PLC Classes

- Three classes of PLC Technologies:
  - Broadband (BB):
    - Operating at 1.8 – 250 MHz.
    - Data Rate: Up to 200 Mbps
    - Initial Application: Residential Internet Access
    - Short Communication Range (few kilometers)
    - Good for AMI/AMR, Not Good for sub-stations (Q: Why?)

PLC Classes

- Three classes of PLC Technologies:
  - Broadband (BB):



Example: Residential broadband access / AMI / AMR

PLC Classes

- Three classes of PLC Technologies:
  - Narrowband (NB):
    - Operating at 3 – 500 kHz.
      - United States FCC: 10-490 kHz
    - Data Rate: Up to 500 kbps (usually several kbps)
    - Considered for sub-station communications

PLC Classes

- Three classes of PLC Technologies:
  - Ultra Narrowband (UNB):
    - Operating at 30 Hz – 3 kHz.
    - Data Rate: Up to 100 bps (very low, but good enough!)
    - Communication Range: 150 km or more
    - Current Applications:
      - AMI, AMR, Demand Response (Direct Load Control)

HomePlug

- HomePlug is an industry Alliance to enable and promote PLC:

  - HomePlug 1.0: Residential Internet
  - HomePlug AV: Residential Cable TV
  - HomePlug Green PHY: Smart Grid Applications (in-home)
    - Wired alternative/addition to ZigBee and Z-Wave for HAN

DoE Requirements for Smart Grid Communications

DoE Smart Grid Communication Requirements

Application	Network Requirements			
	Bandwidth	Latency	Reliability	Security
AMI	10-100 kbps/node	2-15 sec	99-99.99%	High
Demand Response	14kbps- 100 kbps/node	500 ms- several minutes	99-99.99%	High
Wide Area Situational Awareness	600-1500 kbps	20 ms-200 ms	99.999-99.9999%	High
Distribution Energy Resources and Storage	9.6-56 kbps	20 ms-15 sec	99-99.99%	High
Electric Transportation	9.6-56 kbps	2 sec-5 min	99-99.99%	Relatively high
Distribution Grid Management	9.6-100 kbps	100 ms-2 sec	99-99.999%	High

Not that high!

Other Smart Grid Communications Technologies

Other Smart Grid Communication Technologies

Type/Name of Standards	Details	Application
IEC 61970 and IEC 61969	Providing Common Information Model (CIM): IEC 61970 works in the transmission domain and IEC 61969 works in the distribution domain	Energy management systems
IEC61850	Flexible, future proofing, open standard, communication between devices in transmission, distribution and substation automation systems	Substation Automation
IEC 60870-6 /TASE.2	Data exchange between utility control centers, utilities, power pools, regional control centers	Inter-control center communications
IEC 62351 Parts 1-8	Defining cyber security for the communication protocols	Information Security Systems
IEEE P2030	A Guide for smart grid inter-operability of energy technology and IT operation with the electric power system (EPS)	Customer-side applications
IEEE P1901	High speed power line communications	In-home multimedia, utility and smart grid applications
ITU-T G.9955 and G.9956	ITU-T G.9955 and G.9956 contain the physical layer specification and the data link layer specification	Distribution Automation, AMI
OpenADR	Dynamic pricing, Demand Response	Price Responsive and Load Control
BACnet	Scalable system communications at customer side	Building automation
HomePlug	Powerline technology to connect the smart appliances to HAN	HAN
HomePlug Green PHY	Specification developed as a low power, cost-optimized power line networking specification standard for smart grid applications	HAN
U-SNAP	Providing many communication protocols to connect HAN devices to smart meters	HAN

Ref: V.C. Güngör et al.

Other Smart Grid Communication Technologies

Type/Name of Standards	Details	Application
U-SNAP	Providing many communication protocols to connect HAN devices to smart meters	HAN
ISA100.11a	Open standard for wireless systems	Industrial Automation
SAE J2293	Standard for the electrical energy transfer from electric utility to EVs	Electric Vehicle Supply Equipment
ANSI C12.22	Data network communications are supported and C12.19 tables are transported	AMI
ANSI C12.18	Data structures transportation via the infrared optical port han	AMI
ANSI C12.19	Flexible metering model for common data structures and industry "vocabulary" for meter data communications	AMI
Z-Wave	Alternative solution to ZigBee that handles the interference with 802.11/b/g	HAN
M-Bus	European standard and providing the requirements for remotely reading all kinds of utility meters	AMI
PRIME	Open, global standard for multi-vendor interoperability	AMI
G3-PLC	Providing interoperability, cyber security, and robustness	AMI
SAE J2836	Supporting use cases for plug-in electric vehicles communication	Electric Vehicle
SAE J2847	Supports communication messages between PEVs and grid components	Electric Vehicle

Ref: V.C. Güngör et al.

References

- A. Van-Nieuwenhuyse, M. Alves, and A. Koubâa, "On the use of the ZigBee protocol for Wireless Sensor Networks", *Technical Report, IPP Hurray*, Jun 2006. [On-line] http://www.open-zb.net/publications/tr-hurray-060603.pdf.

- P. Yi, A. Iwayemi, and C. Zhou, "Developing ZigBee Deployment Guideline Under WiFi Interference for Smart Grid Applications", *IEEE Transactions on Smart Grid*, Vol. 2, No. 1, pp. 110-120, March 2011.

- S. Safaric and K.~Malaric, "ZigBee Wireless Standard", *Proc. of the IEEE International Symposium on Multimedia Signal Processing and Communications*, Zadar, Croatia, June 2006.

References

- M. Armel, "ZigBee Overview", Lecture Notes, The George Washington Univ. 2007. [On-line] http://www.seas.gwu.edu/~cheng/388/LecNotes2007/ZigBee.pdf.

- S. C. Ergen, "ZigBee/IEEE 802.15.4 Summary", Technical Report, University of California - Berkeley, September 2004. [On-Line] http://pages.cs.wisc.edu/~suman/courses/838/papers/zigbee.pdf.

- ZigBee Alliance, "ZigBee and Wireless Radio Frequency Coexistence", Document Number: Zigbee_07-5219, June 2007, [On-Line] www.zigbee.org.

References

- ZigBee Alliance, "ZigBee Overview", Document Number: Zigbee_07-5482, June 2007, [On-Line] www.zigbee.org.

- J. Liu and S. Singh, “ATCP: TCP for mobile Ad Hoc Networks”, *IEEE Journal on Selected Areas in Communications*, pp. 1300-1315, vol. 19, no. 7, July 2001.

- S. Kandukuri and S. Boyd, "Optimal power control in interference-limited fading wireless channels with outage-probability specifications", *IEEE Transactions on Wireless Communications*, pp. 46 - 55, vol. 1, no. 1, January 2002.

- I. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," *Computer Networks*, vol. 47, pp. 445-487, March 2005.

References

- Department of Energy, “Communications Requirements of Smart Grid Technologies", October 5, 2010.

- G. Iyer, P. Agrawal, E. Monnerie, R.S. Cardozo, “Performance analysis of wireless mesh routing protocols for smart utility networks”, in *Proc. of the IEEE International Conference on Smart Grid Communications*, Brussels, Belgium, October 2011.

- M. Erol-Kantarci, H. T. Mouftah, “Wireless Sensor Networks for Cost-Efficient Residential Energy Management in the Smart Grid”, *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 314-325, June 2011.

References

- M. Adamiak, D. Baigent, and R. Mackiewicz, “IEC 61850 Communication Networks and Systems In Substations: An Overview for Users”, in *Proc. of Syst. Protection Seminar*, 2004.

- V. C. Güngör, D. Sahin, T. Kocak, S. Ergüt, C. Buccella, C. Cecati, G. P. Hancke, “Smart Grid Technologies: Communication Technologies and Standards”, *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529-539, November 2011.

- H.C. Ferreira, H.M. Grovk, 0. Hooijen, and A.J. Han-Vinck, “Power Line Communications: An Overview”, *Proc. of the IEEE AFRICON*, Stellenbosch , South Africa, September 1996.