Wireless Protocols for IoT: Zigbee

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

These slides and audio/video recordings of this class lecture are at:
http://www.cse.wustl.edu/~jain/cse574-24/

Student Questions

1. Zigbee Features, Versions, Device Types, Topologies
2. Zigbee Protocol Architecture
3. Zigbee Application, Zigbee Application Support Layer
4. Network Layer, Routing: AODV, DSR
5. Zigbee Smart Energy V2

Note: This is the 3rd lecture in a series of class lectures on IoT. Bluetooth, Bluetooth Smart, and IEEE 802.15.4 were covered in the previous lectures.

Student Questions

Zigbee PRO Features

- Zigbee PRO: Published in 2007.
- **Stochastic addressing**: A device is assigned a random address and announced. The mechanism for addressing conflict resolution. Parents don't need to maintain the assigned address table.
- **Link Management**: Each node maintains the quality of links to neighbors. Link quality is used as link cost in routing.
- **Frequency Agility**: Nodes experience interference report to the channel manager (e.g., trust center), which then selects another channel
- **Multicast**
- **Many-to-One Routing**: To concentrator
- **Asymmetric Link**: Each node has different transmit power and sensitivity. Paths may be asymmetric.
- **Fragmentation** and Reassembly

Student Questions

- In a concentrator like an coordinator?

Yes and no. Some applications (not all) have n-to-1 traffic. In those cases, the central point is called a concentrator.

- Can you please explain Stochastic addressing?

Discussed in Slide 13-18.
Stochastic=Random

- You discuss Zigbee Pro here. Then in 4-6, talk about Zigbee classic. Then on Slide 7, we go back to Zigbee Pro.

The slides are out-of-order.

- How does Zigbee PRO's asymmetric link management affect routing efficiency in large-scale mesh networks?

Routing is double the work since each side has to find its route. Of course, with or without asymmetry, this is not for large-scale networks.

Zigbee Overview

- Industrial monitoring and control applications requiring small amounts of data, turned off most of the time (<1% duty cycle), e.g., wireless light switches, meter readings, patient monitoring
- The First standard was published in 2004
- Ultra-low power, low-data rate, multi-year battery life
- Power management to ensure low power consumption.
- Less Complex. 32kB protocol stack vs 250kB for Bluetooth
- **Range**: 1 to 100 m, up to 65000 nodes.
- **Tri-Band**:
  1. 16 Channels at 250 kbps in 2.4 GHz ISM
  2. 10 Channels at 40 kb/s in the 915 MHz ISM band (Americas)
  3. One Channel at 20 kb/s in European 868 MHz band
  - Also, 920 MHz in Japan, 784 MHz in China

Student Questions

- Is the channel width still 5 MHz?

No. Bit rates are explicitly specified in the last point. Widths are similar.

- Why is it "Tri-Band"?

2.4GHz, 915 MHz, 868 MHz
(Not counting country-specific variations)

- So Zigbee is for tiny amounts of data, but we want it to go a long way? This seems like a particular application.

It is designed for a typical home environment, which is too big for Bluetooth. This is better.

- What does ISM stand for?

Industrial, Scientific, and Medical

Zigbee Overview

- Industrial monitoring and control applications requiring small amounts of data, turned off most of the time (<1% duty cycle), e.g., wireless light switches, meter readings, patient monitoring
- The first standard was published in 2004
- Ultra-low power, low-data rate, multi-year battery life
- Power management to ensure low power consumption.
- Less Complex. 32kB protocol stack vs 250kB for Bluetooth
- **Range**: 1 to 100 m, up to 65000 nodes.
- **Tri-Band**:
  - 16 Channels at 250 kbps in 2.4GHz ISM
  - 10 Channels at 40 kb/s in the 915 MHz ISM band (Americas)
  - One Channel at 20 kb/s in European 868 MHz band
  - 920 MHz in Japan

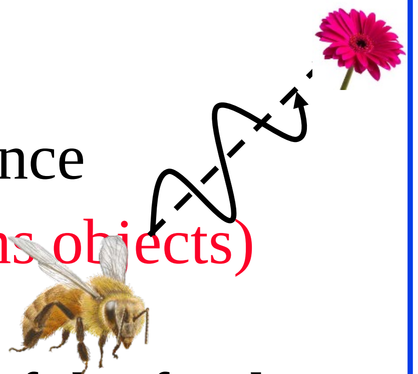
Student Questions

- Can Zigbee replace HomePlug to build a home network?

These are two different media. HomePlug is for electrical wires. Zigbee is wireless. Each has its application environment.

Zigbee Overview (Cont)

- IEEE 802.15.4 MAC and PHY
  (Except for Zigbee Smart Energy 2.0)
  Higher layer and interoperability by Zigbee Alliance
- Up to 254 devices or ~2^{16} end nodes (Applications objects)
- Named after the zigzag dance of the honeybees
  The direction of the dance indicates the location of the food



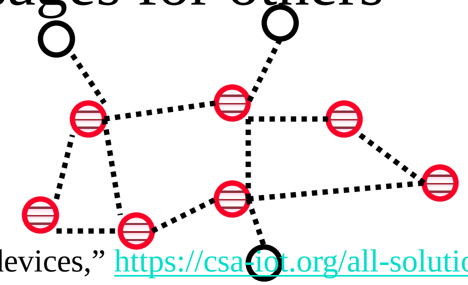
- Multi-hop ad-hoc mesh network

Multi-Hop Routing: message to non-adjacent nodes

Ad-hoc Topology: No fixed topology. Nodes discover each other

Mesh Routing: End-nodes help route messages for others

Mesh Topology: Loops possible



Ref: Connectivity Standards Alliance, "Zigbee: The full stack solution for all smart devices," https://csa-iot.org/all-solutions/zigbee/

Student Questions

- Could you go over the difference between mesh topology and router again? I'm more confused on the idea of mesh topology.

Mesh routing means "end-nodes" do the routing. For example, you may forward your neighbor's packets to them. This has not been successful due to economic considerations. What's in it for me?
Mesh topology is as shown. Some nodes are end nodes and some are intermediate nodes. This is quite common.

- Is there any difference between multi-hop vs. mesh routing?

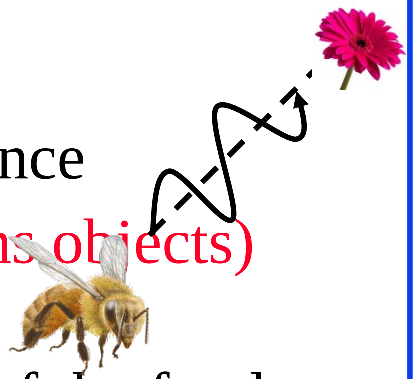
A chain is multi-hop but not mesh. Mesh routing is designed to avoid cycles.

- What is the difference between devices and simpler nodes?

End nodes are applications inside a device. Devices have 8-bit addresses, and end nodes have 16-bit addresses. It is explained in Slide 13-10. Some device and end-nodes addresses are reserved.

Zigbee Overview (Cont)

- IEEE 802.15.4 MAC and PHY
  (Except for Zigbee Smart Energy 2.0)
  Higher layer and interoperability by Zigbee Alliance
- Up to 254 devices or ~2^{16} end nodes (Applications objects)
- Named after the zigzag dance of the honeybees
  The direction of the dance indicates the location of the food



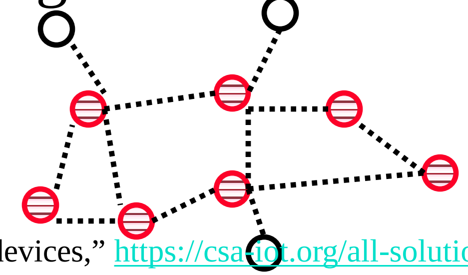
- Multi-hop ad-hoc mesh network

Multi-Hop Routing: message to non-adjacent nodes

Ad-hoc Topology: No fixed topology. Nodes discover each other

Mesh Routing: End-nodes help route messages for others

Mesh Topology: Loops possible



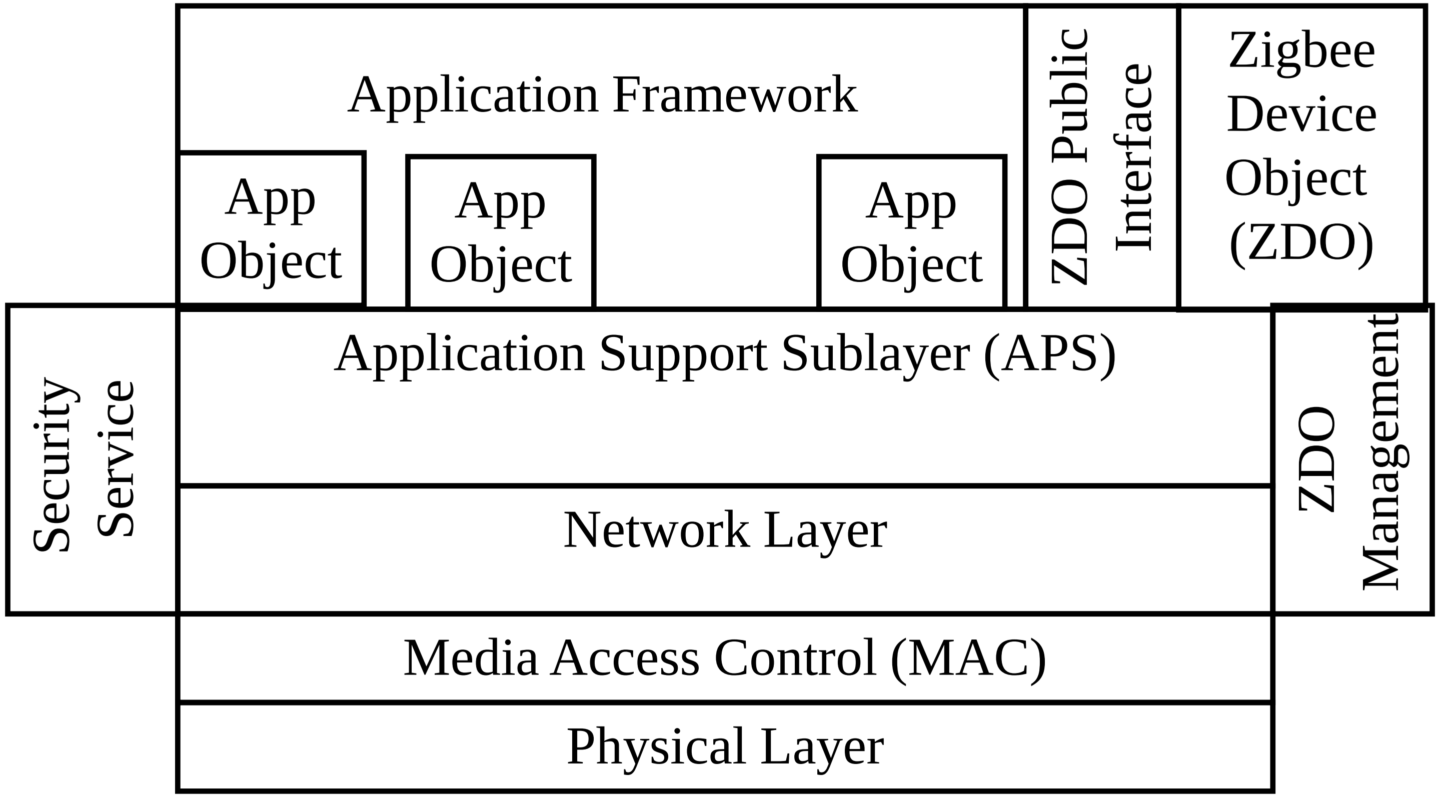
Ref: Connectivity Standards Alliance, "Zigbee: The full stack solution for all smart devices," https://csa-iot.org/all-solutions/zigbee/

Student Questions

- You mention that mesh topology isn't a tree. What topology is a tree?

The tree has no loops.

Zigbee Protocol Architecture



Student Questions

- ❑ There is no transport layer in Zigbee protocol?

APS is transport + session + presentation

- ❑ Can you please highlight the application layer?

See Slide 13-10.

- ❑ Why do the Security Service and ZDO Management components in the Zigbee Protocol Architecture span across multiple layers, and how does this cross-layer approach benefit the overall functionality and security of the network?

Security and management are required for all layers always in all protocols.

PRO Features (Cont)

- **Power Management**: Routers and Coordinators use main power. End Devices use batteries.
- **Security**: Standard and High
  End-Devices get new security keys when they wake up.
- **Backward Compatible**:
  - Pro-devices act as non-routing Zigbee end devices (ZEDs) on the legacy Zigbee network.
  - Legacy Zigbee devices act as non-routing Zigbee end-devices on Zigbee Pro Network

Student Questions

- Why do routers need main power? Is this because they need to be on all the time?

Yes, Exactly.

Zigbee Device Types

- **Coordinator**: Selects channel, starts the network, assigns short addresses to other nodes, transfers packets to/from other nodes
- **Router**: Transfers packets to/from other nodes
- **Full-Function Device**: Capable of being a coordinator or router
- **Reduced-Function Device**: Not capable of being a coordinator or a router ⇒ Leaf node
- **Zigbee Trust Center (ZTC):** Provides security keys and authentication
- **Zigbee Gateway**: Connects to other networks, e.g., WiFi

Student Questions

- So only Reduced-Function devices can use batteries in pro-devices?

RFD's can use main's power or battery depending upon their location. By they way, non-RFDs are not prohibited from using batteries. But you will need big batteries to support the power requirements.

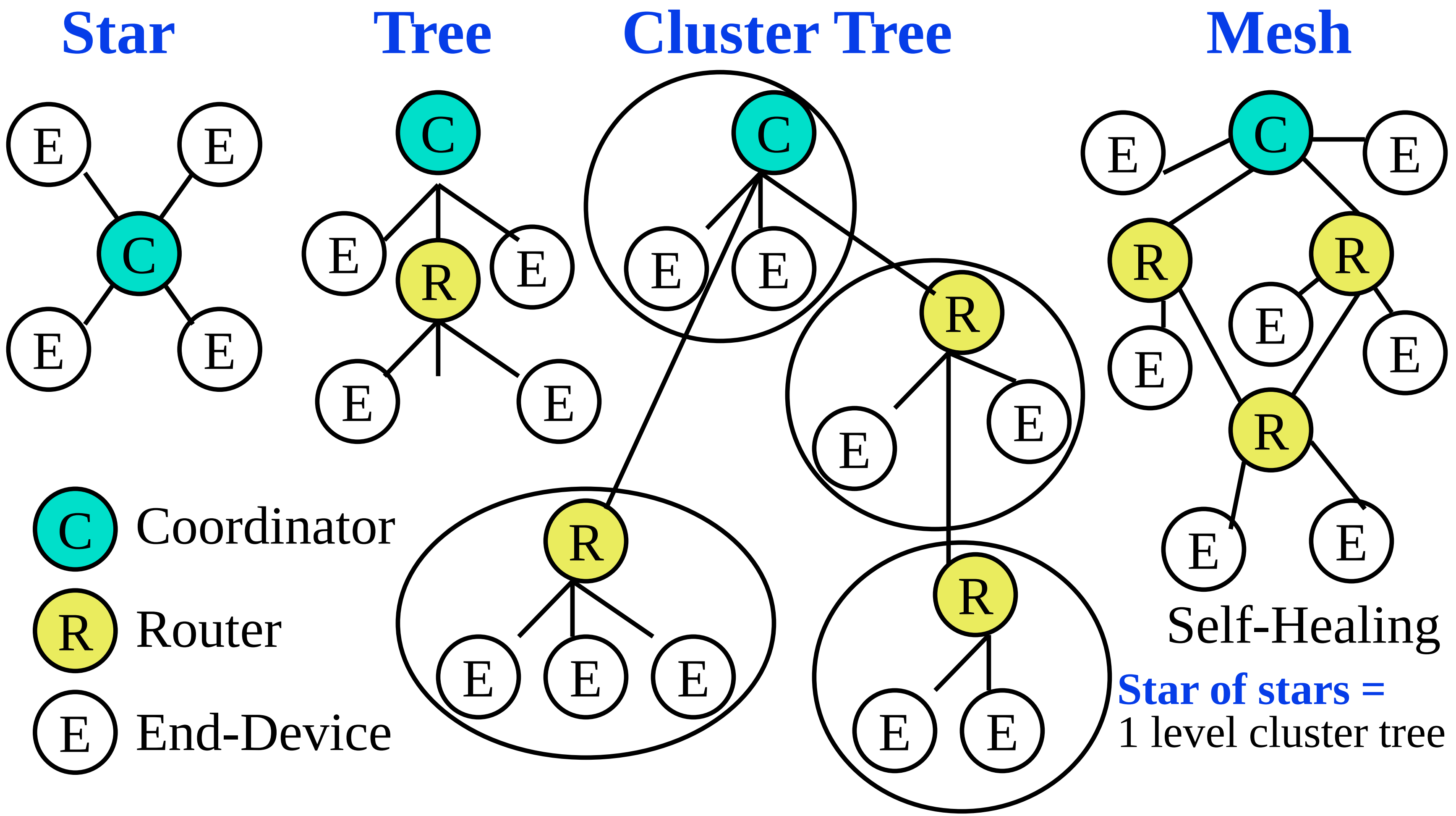
- Does the ZTC exist outside of the hub//gateway?

It is a function. Not a box. Functions can reside in any box. Most boxes implement more than one function. ZTC can reside in the hub or in the cloud.

- Because ZTC provides security keys and authentication, would it be somewhat "safer" than Bluetooth?

ZTC is a function. It is generally packaged with the hub. It can be physically secured in a locked location. Bluetooth does not technically have a hub. So yes.

Zigbee Topologies



Student Questions

- How is a topology decided on?

Decided by the users and manufacturers. Some users don't like trees (no redundancy). Some don't like mesh (looping). Some manufacturers may not support complicated (mesh) routing to keep costs down.

- Can there be multiple coordinators in the cluster tree topology?

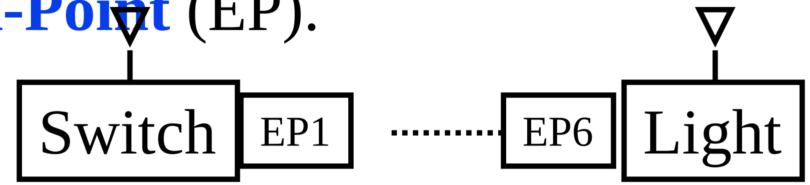
Only one as shown.

- Do end nodes equal end devices?

No. End nodes are defined in the next slide.
End nodes = Application objects

Zigbee Protocol Architecture (Cont)

- **Application Objects**: e.g., Remote control application. They are also referred to as **End-Point** (EP).



- **End-Node**: End device. Each node can have up to 250 application objects.
- **Zigbee Device Object (ZDO)**: Control and management of application objects. Initializes coordinator, security service, device, and service discovery
- **Application Support Layer (APS)**: Serves application objects.
- **Network Layer**: Route Discovery, neighbor discovery
- ZDO Management
- Security Service

Student Questions

- If a lightbulb or a switch is an end-point, what sort of thing functions as a node?

A light bulb can also be a wireless hub ⇒ 2 functions = 2 end points

Zigbee Application Layer

- Application layer consists of application objects (aka endpoints) and Zigbee device objects (ZDOs)
- 256 End Point Addresses:
  - 240 application objects: Address EP1 through EP240
  - ZDO is EP0
  - End Points 241-254 are reserved
  - EP255 is broadcast
- Each End Point has one application profile, e.g., light on/off profile
- Zigbee forum has defined several profiles.
  Users can develop other profiles
- **Attributes**: Each profile requires several data items. Each data item is called an "attribute" and is assigned a 16-bit "attribute ID" by the Zigbee forum

Student Questions

- What are endpoints 241-254 reserved for?

Future use

Zigbee Application Layer (Cont)

- **Clusters**: A collection of attributes and commands on them. A 16-bit ID represents each cluster. Commands could be read/write requests or read/write responses
- **Cluster Library**: A collection of clusters. Zigbee forum has defined several cluster libraries, e.g., the General cluster library contains on/off, level control, alarms, etc.
- **Binding**: Establishing a logical relationship (parent, child, ..)
- **ZDO**:
  - Uses device and service discovery commands to discover details about other devices.
  - Uses binding commands to bind and unbind endpoints.
  - Uses network management commands for network discovery, route discovery, link quality indication, join/leave requests

Student Questions

- Does a device implement a set of clusters?

Yes.

- Module 12 (802.15.4) defines "cluster" as one piconet with some PAN ID. I wonder which one is being used?

That was a cluster of devices. This is a cluster of software and database.

Zigbee Application Profiles

- **Smart Energy**: Electrical, Gas, and Water Meter reading
- **Commercial Building Automation**: Smoke Detectors, lights, …
- **Home Automation**: Remote control lighting, heating, doors, …
- **Personal, Home, and Hospital Care (PHHC)**: Monitor blood pressure, heart rate, …
- **Telecom Applications**: Mobile phones
- **Remote Control for Consumer Electronics**: In collaboration with Radio Frequency for Consumer Electronics (RF4CE) alliance
- **Industrial Process Monitoring and Control**: temperature, pressure, position (RFID), …
- Many others

Ref: A. Elahi and A. Gschwender, "Zigbee Wireless Sensor and Control Network," Prentice Hall, 2009, 288 pp., ISBN:0137134851, Safari Book

Student Questions

- Since all of these use Zigbee, is it true that all of these applications have very small amounts of data associated with them?

Yes. Note no video.

Sample Zigbee Products

Lock
(Kwikset)

Light Bulb
(Sengled)

Hub
(Samsung)

Motion Detector
(Bosch)

Outlet
(Samsung)

Temperature Sensor
(Visonic)

Student Questions

- ❑ Phillips Hue smart lightbulb devices are moving away from requiring a hub. Does this mean that devices like this are moving away from Zigbee or are connecting in a different way?

Yes. Wi-Fi with existing access points or APs built-in the bulbs can do the same job cheaply.

Zigbee Address Assignment

- Each node gets a unique 16-bit address
- Two Schemes: Distributed and Stochastic
- Distributed Scheme: Good for tree structure
  - Each child is allocated a sub-range of addresses.
  - Need to limit maximum depth L,
    Maximum number of children per parent C, and Maximum number of routers R
  - Address of the n^{th} child is parent+(n-1)S(d)

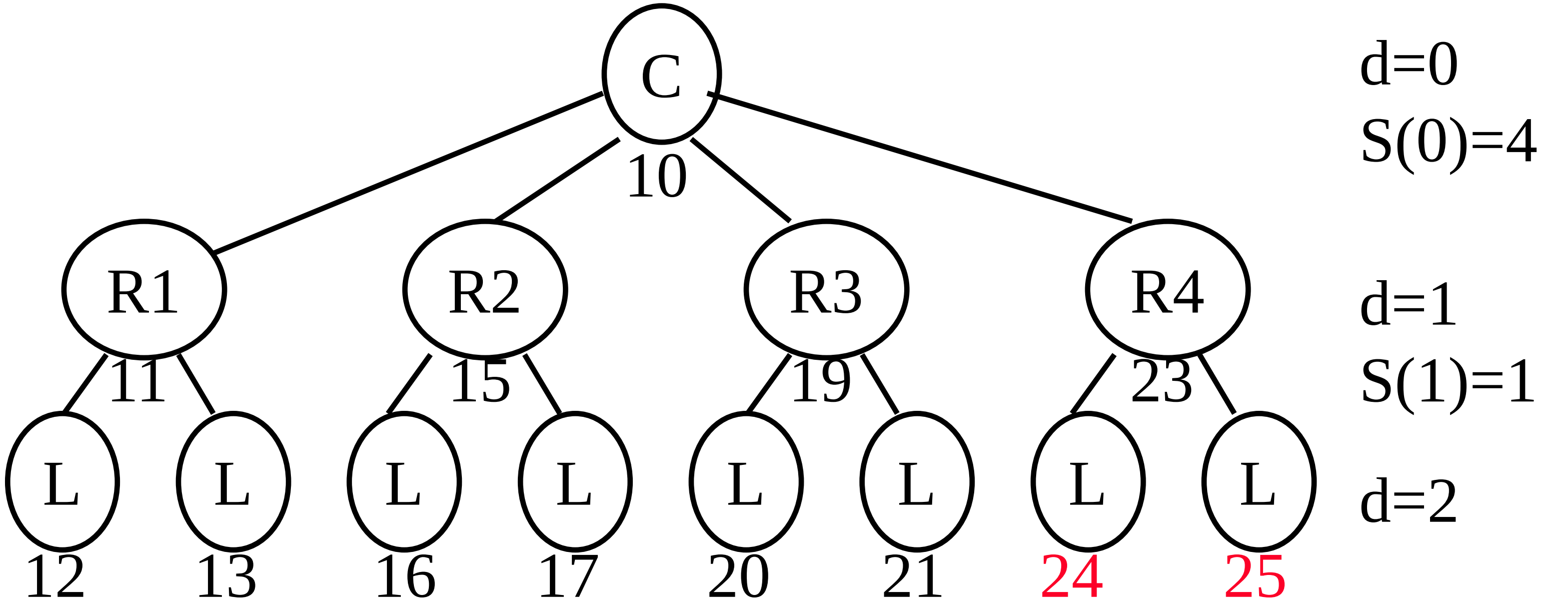
$$S(d) = \begin{cases} 1 + C(L-d) & \text{if } R = 1 \\ \frac{CR^{L-d-1}-1-C+R}{R-1} & \text{if } R > 1 \end{cases}$$

Student Questions

- Could you give some intuition behind this formula?

Graph theory. S(d)(R-1) is approximately the range of addresses allocated.*

Distributed Scheme Example



- Max depth L=2, Routers R=4, Children C=3
- Coordinator: d=0. Skip

$$S(0) = \frac{CR^{L-d-1} - 1 - C + R}{R-1} = \frac{3 \times 4^{2-0-1} - 1 - 3 + 4}{4-1} = 4$$

Student Questions

- Why address 24 is skipped here?

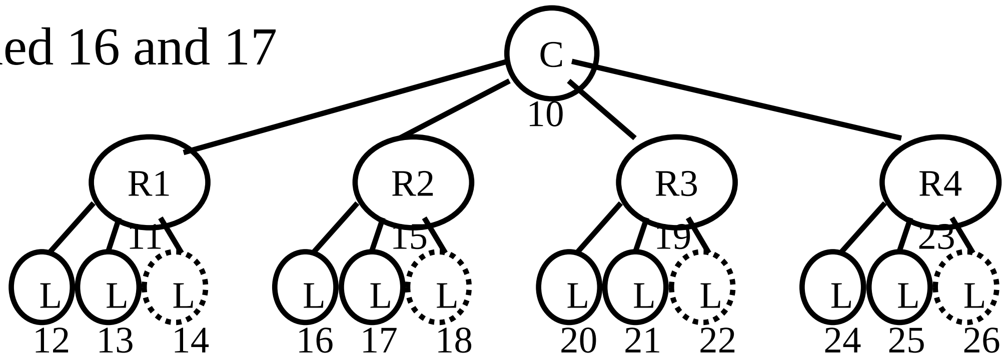
Corrected.

Distributed Scheme Example (Cont)

- Assume the address of coordinator is 10 (decimal)
- Address of R1 = 10+1 = 11
- Address of R2 = 10+1+S(0) = 11+4=15
- Address of R3 = 10+1+2*S(0) = 11+8 = 19
- Address of R3 = 10+1+3*S(0) = 11+12 =23
- Routers R1-R4 compute S(1):

$$S(1) = \frac{CR^{L-d-1} - 1 - C + R}{R-1} = \frac{3 \times 4^{2-1-1} - 1 - 3 + 4}{4-1} = 1$$

- Children of R1 are assigned 12 and 13
- Children of R2 are assigned 16 and 17



Student Questions

- Why does there need to be a gap of S(d-1) for the children? Why d-1 specifically?
- D=Current depth, L=Max depth

S ensures enough space for the families to grow to the maximum depth. d-1 is related to L-d-1 in the expression.

Stochastic Address Assignment

- Parent draws a 16-bit random number between 0 and 2^{16}-1 and assigns it to a new child. A new number is drawn if the result is all-zero (null) or all-one (broadcast). So the assigned address is between 1 and 2^{16}-2.
- Parent then advertises the number to the network
- If another node has that address, an address conflict message is returned, and the parent draws another number and repeats
- There is no need to pre-limit # of children or depth

Student Questions

- For Zigbee's Distributed Addressing Scheme and Stochastic Addressing, what scenarios would one be preferred over the other?

If the network is pre-planned, distributed addressing is more efficient. If the network grows and shrinks randomly, stochastic addressing is better.

Zigbee Routing

1. Ad-Hoc On-Demand Distance Vector (**AODV**)
2. Dynamic Source Routing (**DSR**)
3. Hierarchical Tree Routing
4. Many-to-one routing

Note: Zigbee does not use DSR. It is presented here for completeness.

Student Questions

AODV

- **A**d-hoc **O**n-demand **D**istance **V**ector Routing
- On-demand ⇒ Reactive ⇒ Construct a route when needed
- Avoids unnecessary computations if there is no traffic
- Source broadcasts Route-Request (RREQ) command to all its neighbors containing source, destination, broadcast ID
- Each node determines if this is a new request or if this copy has a lower cost. If yes, it makes a "reverse route" entry for the source in its table w the previous node as the optimal reverse path.
- The node then checks if it has a route to the destination. If yes, it sends "route-reply" to the source. Otherwise, it forwards the request to all its neighbors except where it came from.
- When the source receives a "route reply," it selects the lowest cost path and sends the packet
- If a node cannot forward the packet, it sends a "Route Error" back to the source, which will re-initiate route discovery.

Student Questions

- Does this route error happen when a node in the lowest cost path drops off between the route reply and the sending of the packet? Or are there other reasons that can cause a route error?

Yes.

- What is the cost function?

You define. Cost of a link = 1/bandwidth, length, or dollar cost, …

- In AODV routing, when exploring the correct route, should we not check every neighbor except the one that we just came from?

That would be an optimization. As presented here, it goes to all.

- Do you have an example of when this routing method would be insufficient or an alternative would be preferred?

The method is sufficient always. However, the pros and cons are discussed later in Slide 13.36.

AODV Routing

- **Routing Table**: The path is not stored. Only next hop.
  - Entry = <destination, next node, "sequence #" (timestamp)>
- **Route Discovery**: Flood a **route request (RREQ)** to all neighbors. Neighbors broadcast to their neighbors

Src Addr	Req ID	Dest Addr	Src Seq #	Dest Seq #	Hop Count

- Request ID is the RREQ serial number. Used to discard duplicates.
  Source sequence # is a clock counter incremented when RREQ is sent.
  Destination sequence # is the most recent sequence from the destination that the source has seen. Zero if unknown.

Ref: K. Garg, "Mobile Computing: Theory and Practice," Pearson, 2010, ISBN: 81-3173-166-9, 232 pp., Safari Book.

Student Questions

- What are Src seq # and Dest seq # for?
  To distinguish old requests from new ones. Like time stamps.

AODV Routing (Cont)

- Intermediate nodes can reply to RREQ only if they have a route to the destination with a higher destination sequence #
- ***Route reply*** **(RREP)** comes back "unicast" on the reverse path

Src Addr	Dest Addr	Dest Seq #	Hop Count	Life Time

- Destination Sequence # is from the Destination's counter Lifetime indicates how long the route is valid
- Intermediate nodes record nodes from both RREP and RREQ if it has a lower cost path ⇒ the reverse path
- Backward route to Destination is recorded if the sequence number is higher or if the sequence number is the same and hops are lower
- Old entries are timed out
- AODV supports only symmetric links

Student Questions

- If AODV only supports symmetric, what does Zigbee PRO (with an asymmetric link) use?

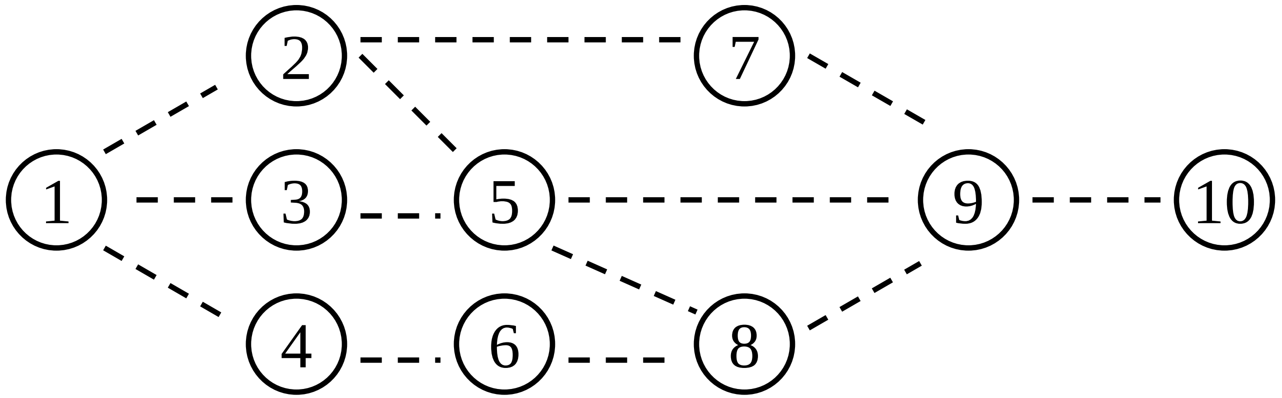
The path is used only in one direction. Reverse traffic finds another path.

- How is the lifetime parameter determined?

It is determined from the volatility of the information similar to that used in webpages.

AODV Routing: Example

- Node 1 broadcasts RREQ to 2, 3, 4:
  "*Anyone has a route to 10 fresher than 1. This is my broadcast #1*"
- Node 2 broadcasts RREQ to 1, 5, 7
- Node 3 broadcasts RREQ to 1, 5
- Node 4 broadcasts RREQ to 1, 6



Student Questions

- What does "fresher than 1" mean?

Here, 1 is the sequence number or time stamp.

- What is the problem we are trying to do here?

Node 1 is trying to find a route to Node 10.

AODV Example (Cont)

Pkt #	Pkt #				Req	Src	Dest			New Table Entry				
In	Out	From	To	Message	ID	Seq #	Seq #	Hops	Action at Receipient	Dest	Seq	Hops	Next	
	1	1	2	RREQ	1	1	1	1	New RREQ. Broadcast	1	1	1	1	← Table entry at 2 for node 1
	2	1	3	RREQ	1	1	1	1	New RREQ. Broadcast	1	1	1	1	
	3	1	4	RREQ	1	1	1	1	New RREQ. Broadcast	1	1	1	1	← Table entry at 4 for node 1
1	4	2	1	RREQ	1	1	1	2	Duplicate Req ID. Discard					
1	5	2	7	RREQ	1	1	1	2	New RREQ. Broadcast	1	1	2	2	
1	6	2	5	RREQ	1	1	1	2	New RREQ. Broadcast	1	1	2	2	
2	7	3	1	RREQ	1	1	1	2	Duplicate ID. Discard					
2	8	3	5	RREQ	1	1	1	2	Duplicate ID. Discard					
3	9	4	1	RREQ	1	1	1	2	Duplicate ID. Discard					
3	10	4	6	RREQ	1	1	1	2	New RREQ. Broadcast	1	1	2	4	
5	11	7	2	RREQ	1	1	1	3	Duplicate ID. Discard					
5	12	7	9	RREQ	1	1	1	3	New RREQ. Broadcast	1	1	3	7	
6	13	5	3	RREQ	1	1	1	3	Duplicate ID. Discard					
6	14	5	2	RREQ	1	1	1	3	Duplicate ID. Discard					
6	15	5	9	RREQ	1	1	1	3	Duplicate ID. Discard					
6	16	5	8	RREQ	1	1	1	3	New RREQ. Broadcast	1	1	3	5	
10	17	6	4	RREQ	1	1	1	3	Duplicate ID. Discard					
10	18	6	8	RREQ	1	1	1	3	Duplicate ID. Discard					
12	19	9	8	RREQ	1	1	1	4	Duplicate ID. Discard					
12	20	9	5	RREQ	1	1	1	4	Duplicate ID. Discard					
12	21	9	7	RREQ	1	1	1	4	Duplicate ID. Discard					
12	22	9	10	RREQ	1	1	1	4	New RREQ. Respond	1	1	4	9	
16	23	8	6	RREQ	1	1	1	4	Duplicate ID. Discard					
16	24	8	5	RREQ	1	1	1	4	Duplicate ID. Discard					
16	25	8	9	RREQ	1	1	1	4	Duplicate ID. Discard					
22	26	10	9	RREP	1	1	6	1	New RREP. Record and forward	10	6	1	10	← Table entry at 9 for node 10
26	27	9	7	RREP	1	1	6	2	New RREP. Record and forward	10	6	2	9	
27	28	7	2	RREP	1	1	6	3	New RREP. Record and forward	10	6	3	7	← Table entry at 2 for node 10
28	29	2	1	RREP	1	1	6	4	New RREP. Record and forward	10	6	4	2	

Student Questions

- What is the packet number "in" doing?

So you can co-relate it with packet#-out and follow the path of a packet.

- "Can you go over the table again? I was following up to where table at 10 is updated, but not quite after this part. Especially on how the time count is 6.

6 happens to be the sequence # at 10 at the time. It is arbitrary.

- Also, what does the first column Pkt# In mean?
  See above.
- What do "Dest," "Seq," and "Next" mean in this example?

These are new routing table entries at the "To-node". For example, Row 1 says that the best path from 2 to 1 is 1-hop via 1.

- Why is the dest seq number 6 in the final four lines? Node 10 is only 4 hops from node 1.

Time at 10 is 6.

- The line in red: is the table entry at 10 for node 9? Is the destination 1?

The entry is for destination 1. All messages to 1 should be sent thru 9.

- The line in red: what if we have two nodes that reach the destination node? Do we discard the second arrival request? If so, do we always choose the (next) to be the first hop to reach the destination request?

The second arrivals are late and so not optimal. If two arrive at the same time, either one could be recorded.

AODV Example (Cont)

Pkt # In	Pkt # Out	From	To	Message	Req ID	Src Seq #	Dest Seq #	Hops	Action at Receipient	New Table Entry Dest	Seq	Hops	Next
	1	1	2	RREQ	1	1	1	1	New RREQ. Broadcast	1	1	1	1
	2	1	3	RREQ	1	1	1	1	New RREQ. Broadcast	1	1	1	1
	3	1	4	RREQ	1	1	1	1	New RREQ. Broadcast	1	1	1	1
1	4	2	1	RREQ	1	1	1	2	Duplicate Req ID. Discard				
1	5	2	7	RREQ	1	1	1	2	New RREQ. Broadcast	1	1	2	2
1	6	2	5	RREQ	1	1	1	2	New RREQ. Broadcast	1	1	2	2
2	7	3	1	RREQ	1	1	1	2	Duplicate ID. Discard				
2	8	3	5	RREQ	1	1	1	2	Duplicate ID. Discard				
3	9	4	1	RREQ	1	1	1	2	Duplicate ID. Discard				
3	10	4	6	RREQ	1	1	1	2	New RREQ. Broadcast	1	1	2	4
5	11	7	2	RREQ	1	1	1	3	Duplicate ID. Discard				
5	12	7	9	RREQ	1	1	1	3	New RREQ. Broadcast	1	1	3	7
6	13	5	3	RREQ	1	1	1	3	Duplicate ID. Discard				
6	14	5	2	RREQ	1	1	1	3	Duplicate ID. Discard				
6	15	5	9	RREQ	1	1	1	3	Duplicate ID. Discard				
6	16	5	8	RREQ	1	1	1	3	New RREQ. Broadcast	1	1	3	5
10	17	6	4	RREQ	1	1	1	3	Duplicate ID. Discard				
10	18	6	8	RREQ	1	1	1	3	Duplicate ID. Discard				
12	19	9	8	RREQ	1	1	1	4	Duplicate ID. Discard				
12	20	9	5	RREQ	1	1	1	4	Duplicate ID. Discard				
12	21	9	7	RREQ	1	1	1	4	Duplicate ID. Discard				
12	22	9	10	RREQ	1	1	1	4	New RREQ. Respond	1	1	4	9
16	23	8	6	RREQ	1	1	1	4	Duplicate ID. Discard				
16	24	8	5	RREQ	1	1	1	4	Duplicate ID. Discard				
16	25	8	9	RREQ	1	1	1	4	Duplicate ID. Discard				
22	26	10	9	RREP	1	1	6	1	New RREP. Record and forward	10	6	1	10
26	27	9	7	RREP	1	1	6	2	New RREP. Record and forward	10	6	2	9
27	28	7	2	RREP	1	1	6	3	New RREP. Record and forward	10	6	3	7
28	29	2	1	RREP	1	1	6	4	New RREP. Record and forward	10	6	4	2

← Table entry at 2 for node 1 (row Out 1)

← Table entry at 4 for node 1 (row Out 3)

← Table entry at 9 for node 10 (row Out 26)

← Table entry at 2 for node 10 (row Out 28)

Student Questions

- Why the time at 10 is 6?

That happens to be an example. You can use any other value.

- How are the packet # IN and # OUT numbers assigned in the AODV table?

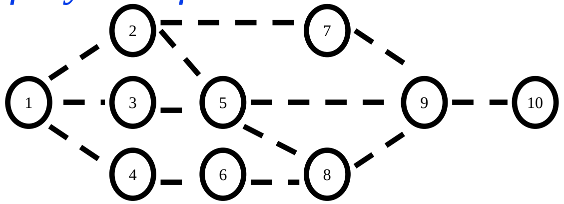
In # is repeated as many times as the number of neighbors. Out #s are sequential.

- The Dest Seq# cannot be less than the prev dest seq#.

No, the seq # belongs to the node first starting the message. They can be lower or higher than those from other nodes.

- ❑ Can you go over this slide/RREP again?

Sure. This is the homework 13A and will be in the exam. So please follow carefully now for the last time.



End of Part 1

Multicast Route Discovery

- Similar to unicast route discovery
- If a node receives an RREQ but is not a member of the group or does not have the route to any member of the group, it creates a reverse-route entry and broadcasts the request to other neighbors
- If the node is a group member, it sends an RREP message to the source and forwards it to other neighbors. Intermediate nodes make a note of this and set up a forward path

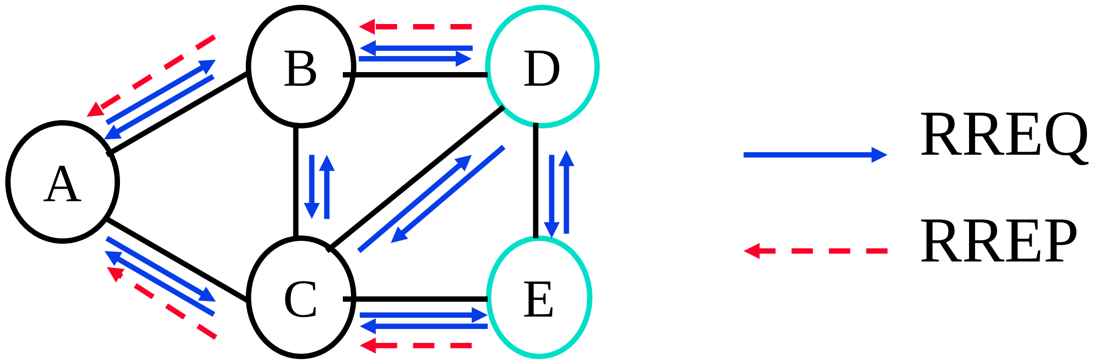
Student Questions

- Does the addition of multicast route discovery introduce any new security risks into a ZigBee mesh network? If so, can these risks be mitigated?

Security is a topic for another course. However, it should suffice to say that route discovery messages (multicast/unicast) are sent to the connected nodes which are authenticated at the time of connection and may even use pre-negotiated encryption.

Multicast Discovery Example

- D and E are members. B and C are not.
- A concludes that the paths are ABD and ACE



Student Questions

- Why is the path ACD not included in concludes?

We make a tree. ACD will cause a loop.

Route Maintenance in AODV

- Each node keeps a list of active neighbors (replied to a hello within a timeout)
- If a link in a routing table breaks, all active neighbors are informed by "Route Error (RERR)" messages
- RERR is also sent if a packet transmission fails
- RERR contains the destination sequence # that failed
- When a source receives a RERR, it starts route discovery with that sequence number.
- Disadvantage: Intermediate nodes may send more up-to-date but still stale routes.
- Ref: RFC 3561, July 2003

Student Questions

Dynamic Source Routing (DSR)

- On-Demand (reactive) routing using "Source Route. "
- Source Route = List of routers along the path in the packet.
- **Routing database**: Complete route to recent destinations
- Each entry has an expiration period and is timed out
- If a route is not available, send a "*route request*" to all neighbors

Src Addr	Broadcast 255...255	RREQ	Req ID	Dest Addr	Route Record

- Each neighbor adds itself to the route in the request and forwards it to all its neighbors (only the first receipt). Does not change the source address.
- If a node knows the route, it appends the rest of the route and returns the "*route reply (RREP)*. "
- RREP goes back along the recorded path
- All nodes record paths in RREP and RREQ. Multiple routes cached.

Student Questions

- So would the RREP be the same packet with source and destination address flipped?

Almost yes. The packet type may also need to be changed from request to reply.

- I wonder why Zigbee is not using DSR?

See AODV vs. DSR comparison in Slide 13-32.

- If a node knows the route and returns the RREP, does it still forward the RREQ to its neighbors to get up-to-date information?

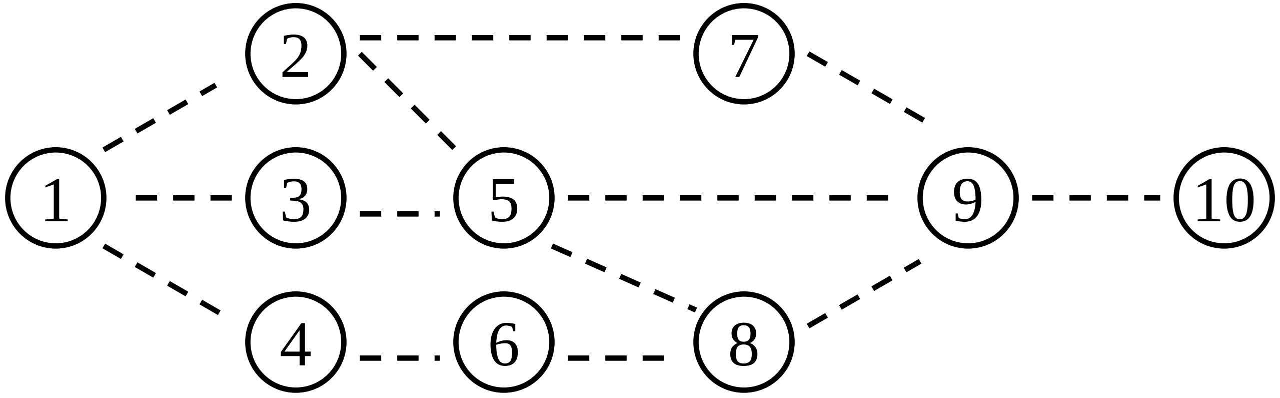
No.

- Is there a possibility that the Route Record section could become too long to fit within the available bytes?

Yes. That would exceed the network diameter. Network sizes are limited.

DSR: Example

- Node 1 sends RREQ to 2, 3, 4:
  "*Any one has a route to 10*"
- Nodes 2 send RREQ to 5, 7. Note: RREQ not sent to 1.
- Node 3 sends RREQ to 5
- Node 4 sends RREQ to 6



Student Questions

- In DSR each node does not send requests to neighbor nodes already in the path

Yes.

DSR Example (Cont)

Pkt # In	Pkt # Out	From Node	To Node	Message Type	Req ID	Hops	Action at Receipient	Route Record in Packet
	1	1	2	RREQ	1	1	New RREQ. Record and forward	1-2
	2	1	3	RREQ	1	1	New RREQ. Record and forward.	1-3
	3	1	4	RREQ	1	1	New RREQ. Record and forward.	1-4
1	4	2	5	RREQ	1	2	New RREQ. Record and forward.	1-2-5
1	5	2	7	RREQ	1	2	New RREQ. Record and forward.	1-2-7
2	6	3	5	RREQ	1	2	Duplicate ID. Same hops. Record and forward.	1-3-5
3	7	4	6	RREQ	1	2	New RREQ. Record and forward.	1-4-6
4	8	5	8	RREQ	1	3	New RREQ. Record and forward.	1-2-5-8
4	9	5	9	RREQ	1	3	New RREQ. Record and forward.	1-2-5-9
5	10	7	9	RREQ	1	3	New RREQ. Same hops. Record and forward.	1-2-7-9
6	11	5	8	RREQ	1	3	Duplicate ID. Longer Path. Discard.	1-3-5-8
6	12	5	9	RREQ	1	3	New RREQ. Record and forward.	1-3-5-9
7	13	6	8	RREQ	1	3	New RREQ. Same hops. Record and forward.	1-4-6-8
8	14	8	6	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-2-5-8-6
8	15	8	9	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-2-5-8-9
9	16	9	8	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-2-5-8-9
9	17	9	7	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-2-5-9-7
9	18	9	10	RREQ	1	4	New RREQ. Respond through route 10-9-5-2-1	1-2-5-9-10
10	19	9	10	RREQ	1	4	New RREQ. Respond through route 10-9-7-2-1	1-2-7-9-10
10	20	9	8	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-2-7-9-8
10	21	9	5	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-2-7-9-5
12	22	9	10	RREQ	1	4	New RREQ. Respond through route 10-9-5-3-1	1-3-5-9-10
12	23	9	8	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-3-5-9-8
12	24	9	7	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-3-5-9-7
13	25	8	5	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-4-6-8-5
13	26	8	9	RREQ	1	4	Duplicate ID. Longer Path. Discard.	1-4-6-8-9
18	27	10	9	RREP	1	1	Record and forward along return path	10-9 (1-2-5-9-10)
19	28	10	9	RREP	1	1	Record and forward along return path	10-9 (1-2-7-9-10)
22	29	10	9	RREP	1	1	Record and forward along return path	10-9 (1-3-5-9-10)
27	30	9	5	RREP	1	2	Record and forward along return path	10-9-5 (1-2-5-9-10)
28	31	9	7	RREP	1	2	Record and forward along return path	10-9-7 (1-2-7-9-10)
29	32	9	5	RREP	1	2	Record and forward along return path	10-9-5 (1-3-5-9-10)
30	33	5	2	RREP	1	3	Record and forward along return path	10-9-5-2 (1-2-5-9-10)
31	34	7	2	RREP	1	3	Record and forward along return path	10-9-7-2 (1-2-7-9-10)
32	35	5	3	RREP	1	3	Record and forward along return path	10-9-5-3 (1-3-5-9-10)
33	36	2	1	RREP	1	4	Record and forward along return path	10-9-5-2-1 (1-2-5-9-10)
34	37	2	1	RREP	1	4	Record and forward along return path	10-9-7-2-1 (1-2-7-9-10)
35	38	3	1	RREP	1	4	Record and forward along return path	10-9-5-3-1 (1-3-5-9-10)

Student Questions

- Is the slide updated in the 2020 version? I don't understand why packet 18 has 1-2-5-9-7 in Route Record in Packet field. Can we go over the table again when the packet reaches node 10?

You are right. The record in packet 18 should be 1-2-5-9-10. Now it has been corrected.

- Why from node 9 to node 5 RREQ is discarded? Is it not a longer path?

Node 5 discarded RREQ because it saw that RREQ in row 4. Then it was only two hops.

- What if 9 received RREQ from node 5 before node 7?

Both are the same hops. Both are recorded and forwarded regardless of the order.

- How to decide in the exam?

There is no arbitrary answer to decide.

- In the exam, is it all right to stop calculating table entries once the node of interest has been explored, or do we still need to explore all other possible routes?

Stop

- Will there be AODV and SDR tables in Exam 3?

Why not?

Route Maintenance in DSR

- If a transmission fails, route error (RERR) is sent to the source. It contains hosts at both ends of the link.
- Intermediate nodes remove or truncate all routes with that link.
- Source may re-initiate the route discovery.
- Caching multiple routes results in a faster recovery. But the routes may be stale, resulting in cache poisoning at other nodes.
- Not suitable for high-mobility environments.
- Source-route overhead in each packet.
- Ref: RFC 4728, February 2007

Student Questions

- Can you explain how cache poisoning may occur?
- What does "Source-route overhead in each packet" mean?

The packets become long if the source route is long.

- Can you explain again what "It contains hosts at both ends of the link" means?

The node that could not be reached and the last node that could be reached.

- Is the host at the end of the link that fails the one that was failed to be sent to or the one doing the sending right before?

The other end of failed link has no information about the request.

AODV vs. DSR

- In DSR, a single RREQ can result in routes to several destinations
- In DSR, RERR messages are sent to the source, not broadcast ⇒ Many nodes are unaware of the failure
- In DSR, route discovery is delayed until all cached entries have been tried ⇒ Not suitable for high mobility

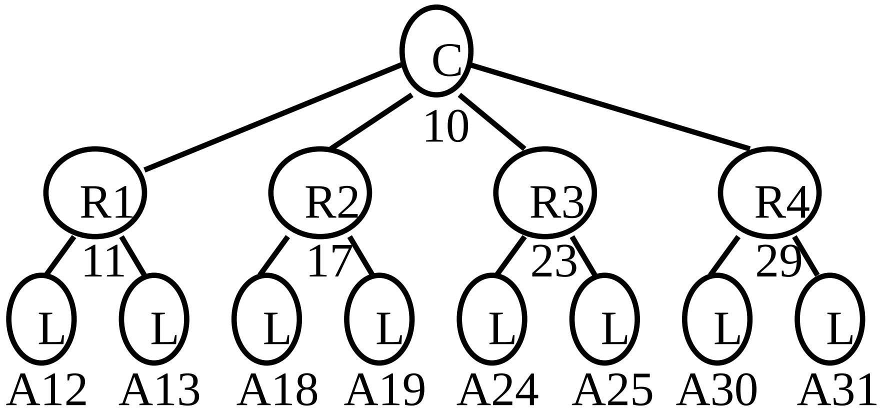
Feature	DSR	AODV
Routing Table	Route	Next Hop
Packet	Route	No route
Replies	Multiple	First only
Route Deletion	Fast Local	Slow Global

Ref: K. Garg, "Mobile Computing: Theory and Practice," Pearson, 2010, ISBN: 81-3173-166-9, 232 pp., Safari Book.

Student Questions

Tree Hierarchical Routing

- All leaf nodes send the packet to their parent
- Each parent checks the address to see if it is in its subrange.
  - If yes, it sends to the appropriate child.
  - If not, it sends to its parent
- Example: A12 to A30. A12 → R1 → Coordinator → R4 → A30



Student Questions

- What does "A" mean in the example?

A=Address

- Why, in this example we skipped 4 addresses for each router?

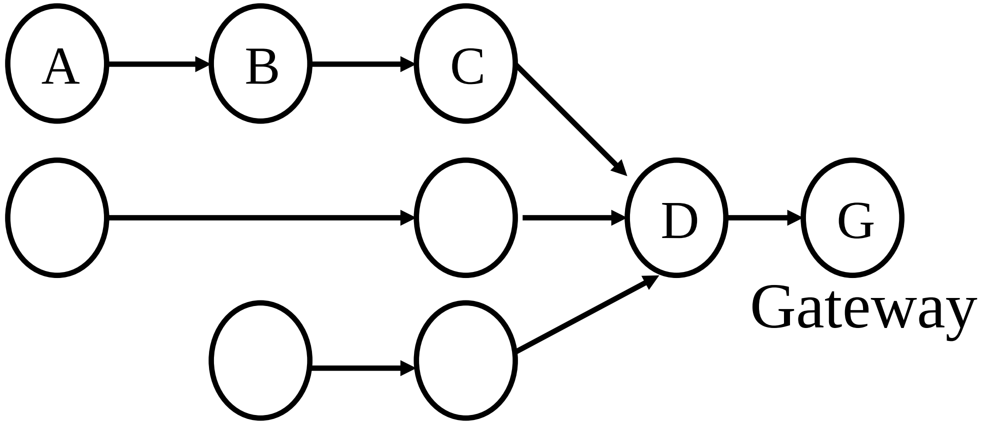
Address assignment was done with C=5 to allow 5 children per router. We can add 3 more devices to each router in future.

- What are the implications of setting specific subranges of addresses per router? How does this affect scalability?

It simplifies address assignment and downward routing.

Many-to-One Routing

- Used for sensor data collection. All data goes to a concentrator or a gateway
- Gateway has a large memory and can hold complete routes to all nodes
- But each node only remembers the next hop toward gateway



Student Questions

- Is Many-to-One Routing the same as Source Routing?

No. Source routing = Complete route stored in each packet. Many-to-one is the opposite of multicast, which is one-to-many.

- Is many-to-one routing still a type of tree routing?

Routing is not tree. The topology is.

Zigbee RF4CE

- Radio Frequency for Consumer Electronics (RF4CE) consortium developed a protocol for remote control using wireless (rather than infrared, which requires line of sight)
- RF4CE merged with Zigbee and produced the Zigbee RF4CE protocol
- Operates on channels 15, 20, and 25 in the 2.4 GHz band
- Maximum PHY payload is 127 bytes
- Two types of devices: Remotes and Targets (TVs, DVD Player,…)
- **Status Display**: Remote can show the status of the target
- **Paging**: You can locate the remote control using a paging button on the target
- **Pairing**: A remote control works only with certain devices

Ref: CSA, "White paper – Understanding Zigbee Rf4ce," https://csa-iot.org/developer-resource/white-paper-understanding-zigbee-rf4ce/

Student Questions

- Is the pairing process done on the MAC layer?

Pairing is an application.

- What are channels 15, 20, and 25 in 2.4 GHz? are they known?

The 2.4 GHz band is divided into 1 MHz channels for frequency hopping.

- Is there any reason why it can operate on channels 15, 20, 25 in the 2.4 GHz band?

Some one's observation that these center channels are less used. Also, limited possibilities simplifies the electronics and lowers cost.

Zigbee 2030.5

- Formerly known as "Zigbee Smart Energy 2."
- Monitor, control, and automate the delivery and use of energy and water
- Adds plug-in vehicle charging, configuration, and firmware download
- Developed in collaboration with other smart grid communication technologies: HomePlug, WiFi, …
- IP based ⇒ Incompatible with previous Zigbee

Student Questions

Zigbee IP

- Uses standard IPv6 frame format.
  ⇒ Allows connecting sensors directly to the Internet w/o gateways
- Uses 802.15.4 PHY, MAC and Zigbee 2030.5
- IPv6 headers are compressed using **6LowPAN**
- **RPL** Routing to discover the topology
- All Internet protocols: UDP, TCP, HTTP, … can be used
- Multicast forwarding and Service discovery using multicast DNS (mDNS) and DNS Service Discovery (DNS-SD)
- Security using standard protocols: TLS (Transport Layer Security), EAP (Extensible Authentication Protocol), PANA (Protocol for carrying Authentication for Network Access)
- Not compatible with other versions of Zigbee since they use a different network layer frame format
  ⇒ Need a gateway between Zigbee and Zigbee IP.

Student Questions

- Since Zigbee uses IPv6, does this mean that there are not many applications/uses in the United States?

All computers now come with IPv6 worldwide. IPv4 nodes can talk to IPv6 nodes through a router.

Z-Wave

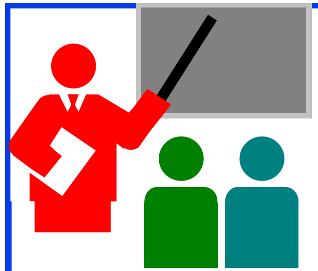
- No relationship to Zigbee but competes with it in many applications and so often confused with it
- Search for Zigbee devices on Amazon shows many products that support only Z-Wave, not Zigbee
- Originally a proprietary protocol developed for remote control. Now used for IoT.
- Now standardized by Z-Wave Alliance
- Uses 915/868 MHz band
- Many IoT hubs support Z-Wave along with Zigbee

Ref: Wikipedia, "Z-Wave," https://en.wikipedia.org/wiki/Z-Wave
Ref: Z-Wave Alliance, https://z-wavealliance.org/

Student Questions

- Is there an advantage to using Z-Wave over Zigbee or the other way around?

Zigbee is standard.



Summary

1. Zigbee is an IoT protocol for sensors, industrial automation, and remote control using IEEE 802.15.4 PHY and MAC
2. Zigbee PRO supports stochastic addressing, many-to-one routing, fragmentation, and mesh topologies.
3. Several application profiles have been defined with control and management provided by ZDOs.
4. Application Support layer provides data and command communication between application objects
5. Network layer provides addressing and routing. Addressing can be assigned using distributed or stochastic schemes. Routing is via AODV, DSR, Tree Hierarchical, or many-to-one routing.
6. Zigbee RF4CE and Zigbee SEP2 are Zigbee protocols designed specifically for remote control and smart grid, respectively.

Student Questions

- I think it would be beneficial to go over slides 3-6, as the delayed audio made it a bit more difficult to follow.

Slides were discussed 2,4,5,6,3 but inserted 2,3,4,5,6. A corrected version has been uploaded.

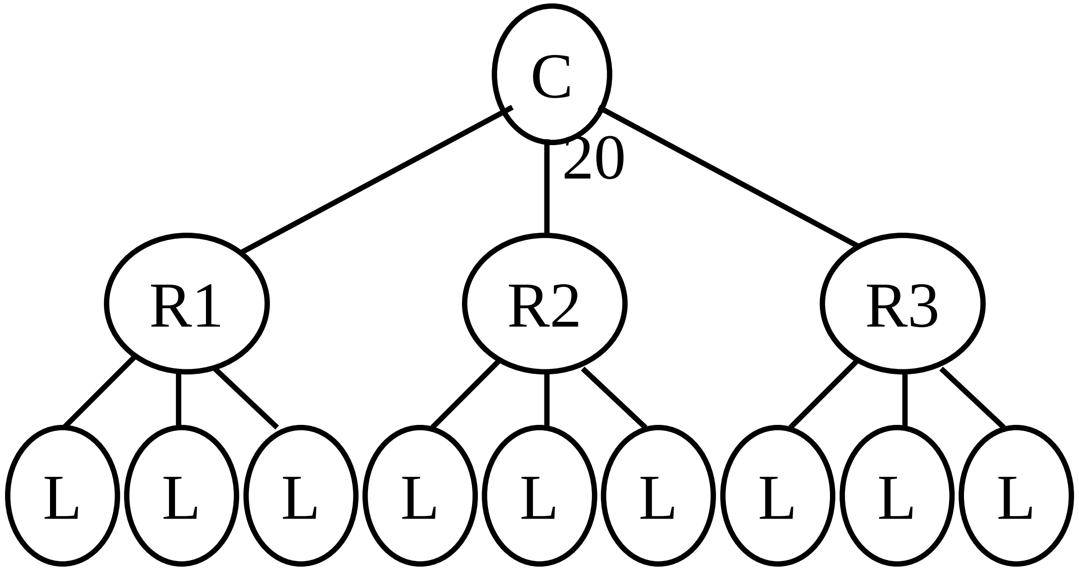
- I was wondering when did they publish the latest Zigbee standard. Because I see the Zigbee alliance changed its name to Connectivity Standards Alliance.

Starting in 2019, they started work on Matter protocol. Matter 1.0 was released on October 4, 2024. Allows working with Amazon Alexa, Apple Home, Google Home, etc.

- Some links are invalid because they point to the old name.

All links have been updated today.

Homework 13A

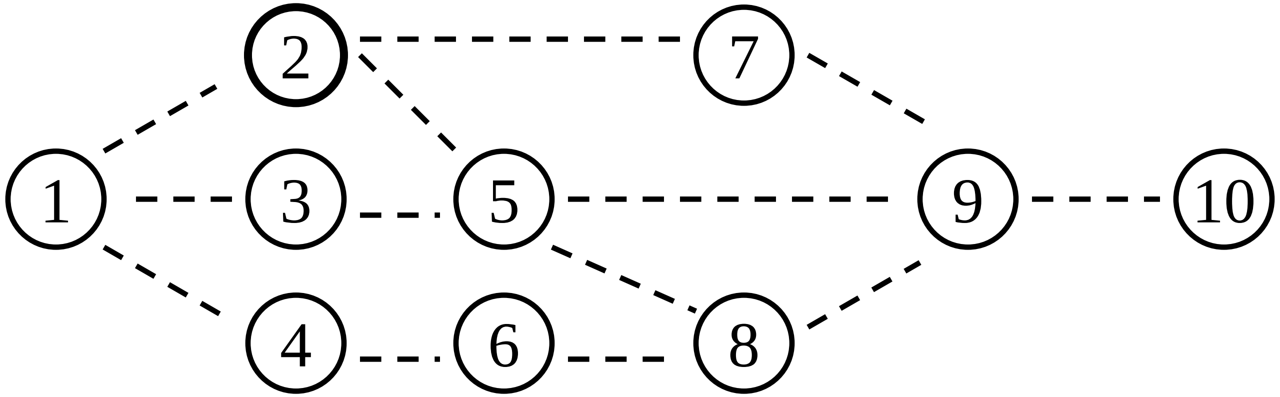


- Assuming that IEEE 802.15.4 network is being planned with a maximum of 5 children per node to a depth of 2 levels and a maximum of 4 routers. Compute sub-ranges to be assigned to each router and the addresses assigned to each node in the network, assuming the coordinator has an address of 20.

Student Questions

Homework 13B

- Write the sequence of messages sent in the following network when node 2 tries to find the path to node 10 in the AODV example.



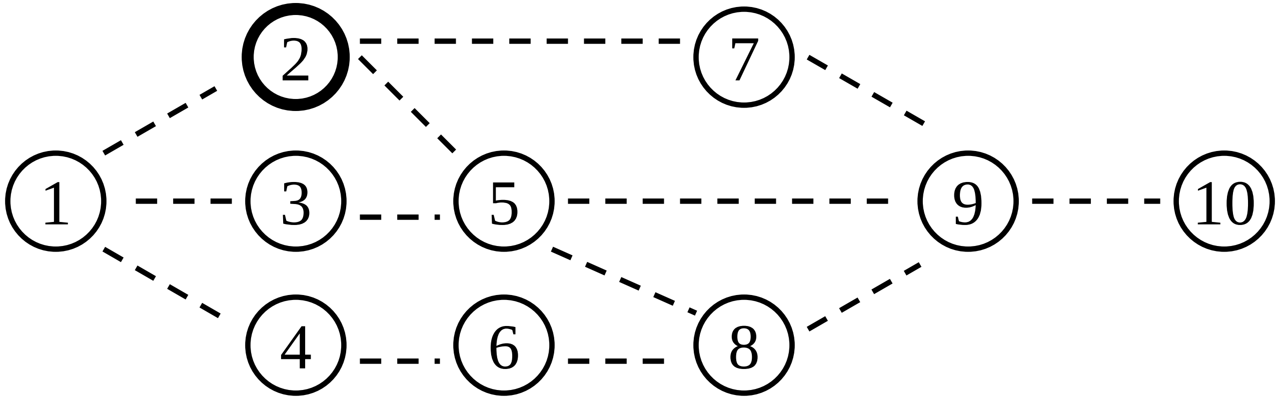
Student Questions

- For this question, are we going to create the whole table like slide 24?

Yes.

Homework 13C

- Write the sequence of messages sent in the following network when node 2 tries to find the path to node 10 in the DSR example.



Student Questions

Reading List

- A. Elahi and A. Gschwender, "Zigbee Wireless Sensor and Control Network," Prentice Hall, 2009, 288 pp., ISBN:0137134851, Safari Book, Chapters 2, 5, 6, 9
- K. Garg, "Mobile Computing: Theory and Practice," Pearson, 2010, ISBN: 81-3173-166-9, 232 pp., Safari Book, Sections 6.5-6.7
- R. Jain, "Networking Protocols for Internet of Things," (6LowPAN and RPL)," http://www.cse.wustl.edu/~jain/cse570-13/m_19lpn.htm

Student Questions

Related Wikipedia Pages

- http://en.wikipedia.org/wiki/Zigbee
- http://en.wikipedia.org/wiki/Ad_hoc_On-Demand_Distance_Vector_Routing
- http://en.wikipedia.org/wiki/Dynamic_Source_Routing
- http://en.wikipedia.org/wiki/Source_routing
- http://en.wikipedia.org/wiki/Loose_Source_Routing

Student Questions

References

1. D. A. Gratton, “The Handbook of Personal Area Networking Technologies and Protocols,” Cambridge University Press, 2013, 424 pp., ISBN:9780521197267, Safar Book.
2. O. Hersent, et al., “The Internet of Things: Key Applications and Protocols,” Wiley, 2012, 370 pp., ISBN:9781119994350, Safari Book.
3. N. Hunn, “Essentials of Short Range Wireless,” Cambridge University Press, 2010, 344 pp., ISBN:9780521760690, Safari book.
4. D.Gislason, “Zigbee Wireless Networking,” Newnes, 2008, 288 pp., ISBN:07506-85972, Safari book.
5. S. Farahani, “Zigbee Wireless Network and Transceivers,” Newnes, 2008
6. J. Gutierrez, E. Gallaway, and R. Barrett, “Low-Rate Wireless Personnel Area Networks,” IEEE Press Publication, 2007
7. H. Labiod, H. Afifi, C. De Santis, "Wi-Fi, Bluetooth, Zigbee and WiMax," Springer, Jun 2007, 316 pp., ISBN:1402053967.
8. I. Guvenc, et al., "Reliable Communications for Short-Range Wireless Systems," Cambridge University Press, March 2011, 426 pp., ISBN: 978-0-521-76317-2, Safari Book

Student Questions

References (Cont)

- Connectivity Standards Alliance, "Specifications Download Request," https://csa-iot.org/developer-resource/specifications-download-request/
- CSAWhitepapers, https://csa-iot.org/resources/developer-resources/page/4/
- CSA, Zigbee Specification R22 (V 1.0), https://csa-iot.org/developer-resource/specifications-download-request/
- Daintree Network, "Comparing Zigbee Specification Versions," www.daintree.net/resources/spec-matrix.php
- "How Does Zigbee Compare with Other Wireless Standards?" www.stg.com/wireless/Zigbee-comp.html

Student Questions

References (Cont)

- I., Poole, "What exactly is . . . Zigbee?", Volume 2, Issue 4, Pages: 44-45, IEEE Communications Engineer, 2004, http://ieeexplore.ieee.org/iel5/8515/29539/01340336.pdf?tp=&arnumber=1340336&isnumber=29539
- "Zigbee starts to buzz", Volume 50, Issue 11, Pages: 17-17, IEE Review, Nov. 2004 http://ieeexplore.ieee.org/iel5/2188/30357/01395370.pdf?tp=&arnumber=1395370&isnumber=30357
- C. Evans-Pughe,"Bzzzz zzz [Zigbee wireless standard]", Volume 49, Issue 3, Pages:28-31, IEE Review, March 2003
- Craig, William C. “Zigbee: Wireless Control That Simply Works,” Zigbee Alliance, 2003

Student Questions

Acronyms

AODV	Ad-Hoc On-Demand Distance Vector
APS	Application Support Sublayer
APSDE	Application Support Sublayer Data Entity
APSME	Application Support Sublayer Management Entity
CSMA/CA	Carrier Sense Multiple Access
DNS	Domain Name System
DSR	Dynamic Source Routing
DVD	Digital Video Disc
EP	End Point
GHz	Giga Hertz
ID	Identifier
IEE	Institution of Electrical Engineers (UK) now IET
IEEE	Institution of Electrical and Electronic Engineers
IET	Institution of Engineering and Technology
IoT	Internet of Things
IP	Internet Protocols

Student Questions

Acronyms (Cont)

❑	ISM	Instrumentation, Scientific, and Medical
❑	kB	Kilo byte
❑	MAC	Media Access Control
❑	MHz	Mega Hertz
❑	NPDU	Network Protocol Data Unit
❑	NPDU	Network Service Data Unit
❑	PHHC	Personal, Home, and Hospital Care
❑	PHY	Physical Layer
❑	RF4CE	Radio Frequency for Consumer Electronics
❑	RFC	Request for Comment
❑	RFID	Radio Frequency ID
❑	RREP	Route Reply
❑	RREQ	Route Request
❑	UWB	Ultra Wide-Band
❑	WiFi	Wireless Fidelity

Student Questions

Acronyms (Cont)

- WiMAX Worldwide Interoperability for Microwave Access
- WWAN Wireless Wide Area Network
- ZDO Zigbee Device Object

Student Questions

Scan This to Download These Slides

Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/cse574-24/j_13zgb.htm

Student Questions

Related Modules

CSE567M: Computer Systems Analysis (Spring 2013),
https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof

CSE473S: Introduction to Computer Networks (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcgy5e_10TiDw

Recent Advances in Networking (Spring 2013),
https://www.youtube.com/playlist?list=PLjGG94etKypLHyBN8mOgwJLHD2FFIMGq5

CSE571S: Network Security (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFJXumyyg93u

Video Podcasts of Prof. Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw

Student Questions