Wireless Protocols for Internet of Things: Part II – 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/cse574-14/

Overview

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 RF4CE and ZigBee Smart Energy V2

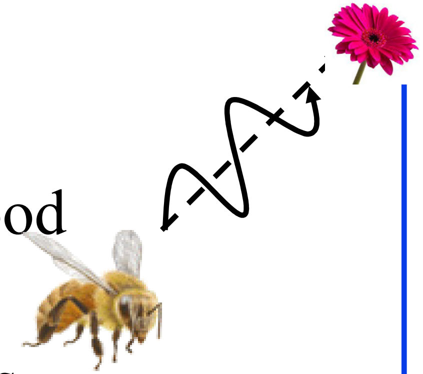
Note: This is the 3rd lecture in series of class lectures on IoT. Bluetooth, Bluetooth Smart, IEEE 802.15.4 were covered in the previous lectures..

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 reading, patient monitoring
- 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 915 MHz ISM band
  - One Channel at 20 kb/s in European 868 MHz band

ZigBee Overview (Cont)

- IEEE 802.15.4 MAC and PHY.
  Higher layer and interoperability by ZigBee Alliance
- Up to 254 devices or 64516 simpler nodes
- Named after zigzag dance of the honeybees
  Direction of the dance indicates the location of food
- Multi-hop ad-hoc mesh network

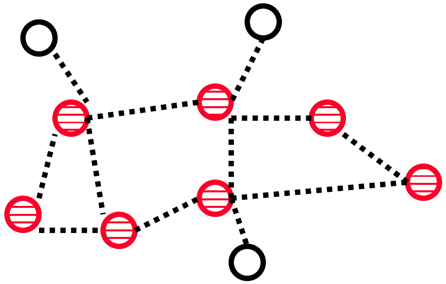


Multi-Hop Routing: message to non-adjacent nodes

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

Mesh Routing: End-nodes help route messages for others

Mesh Topology: Loops possible



Ref: ZigBee Alliance, http://www.ZigBee.org

PRO Features

- **Stochastic addressing**: A device is assigned a random address and announced. Mechanism for address conflict resolution. Parents don't need to maintain assigned address table.
- **Link Management**: Each node maintains quality of links to neighbors. Link quality is used as link cost in routing.
- **Frequency Agility**: Nodes experience interference report to 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

Recent New Features (Cont)

- **Power Management**: Routers and Coordinators use main power. End Devices use batteries.
- **Security**: Standard and High
  End-Devices get new security key when they wake up.

ZigBee Versions

- ZigBee 2004: Original spec for home lighting control
  No longer supported
- ZigBee 2006
- ZigBee 2007
- ZigBee PRO

ZigBee Version Features

Feature	**ZigBee 2006**	**ZigBee Feature Set**	**ZigBee PRO**
Coordinator can change channel during operation	No	Yes	Yes
Distributed Address Assignment	Yes	Yes	No
Stochastic Address Assignment	No	No	Yes
Group Addressing	Yes	Yes	Yes
Many-to-One Routing	No	No	Yes
AES-128	Yes	Yes	Yes
Trust Center	Coordinator	Coordinator	Any device
Network scale limited by address assignment scheme	Yes	Yes	No
Fragmentation and Reassembly	No	Yes	Yes
Commissioning Tool	Yes	Yes	Yes
Keep Neighbor Link Quality	No	No	Yes
High-Security Mode	No	No	Yes
Topologies	Tree and Mesh	Tree and Mesh	Mesh

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

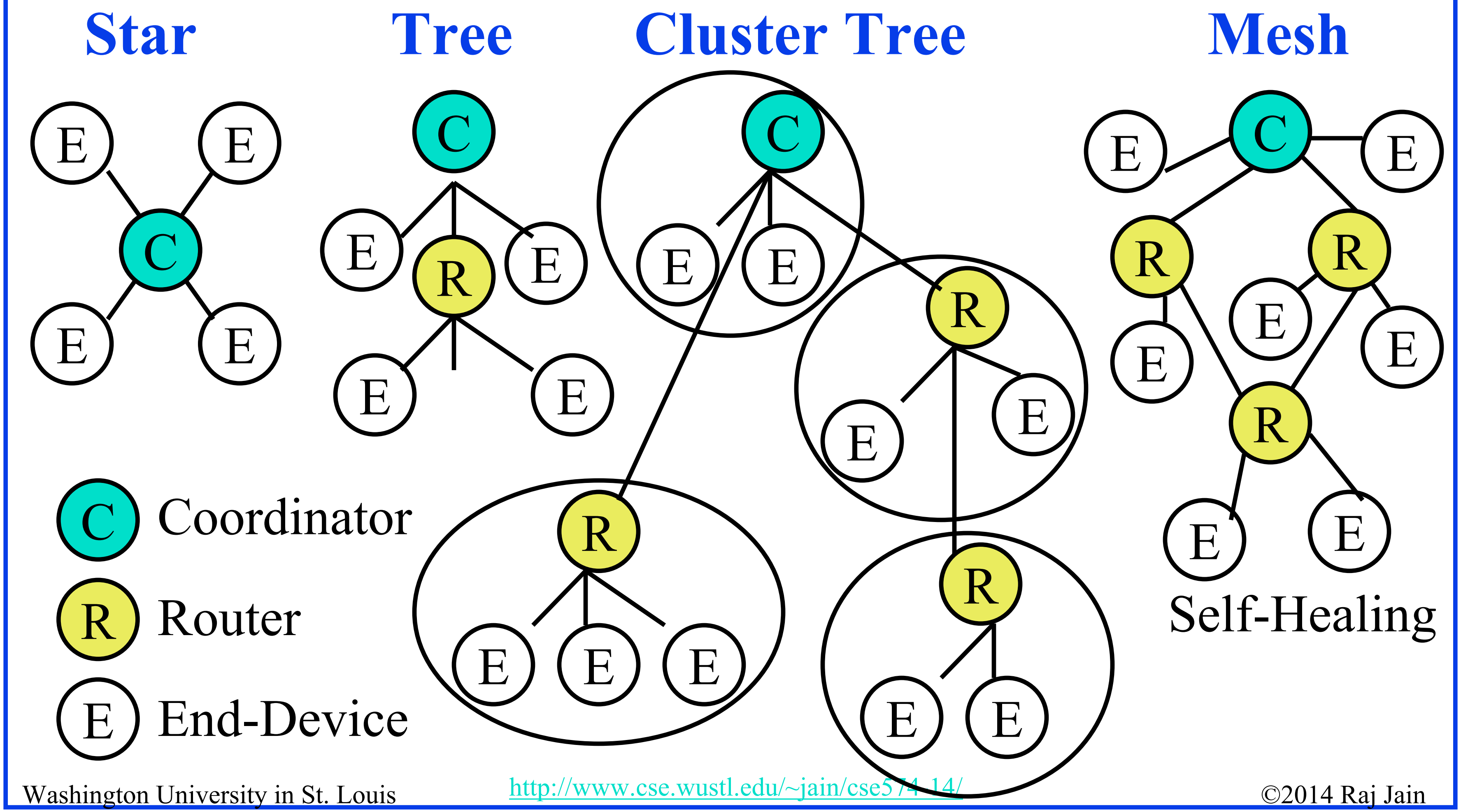
ZigBee Versions Compatibility

- The specs are only "edge compatible"
  ⇒ A node can join as an end-device (leaf) in another network
  - ZigBee devices join as end-devices in ZigBee PRO network
  - ZigBee Pro devices join ZigBee network as end-devices
  - ZigBee 2006 devices join ZigBee network as end-devices

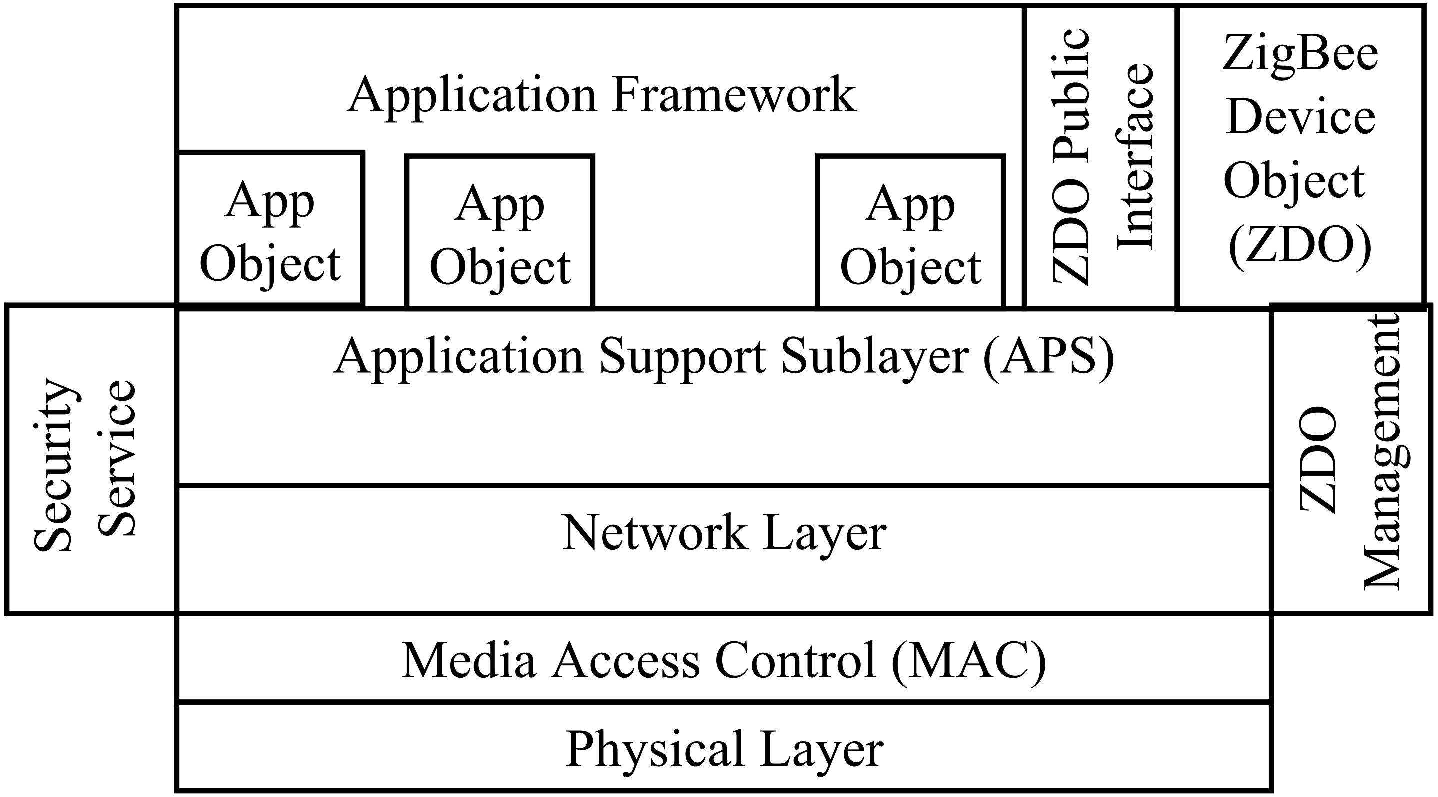
ZigBee Device Types

- **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 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

ZigBee Topologies

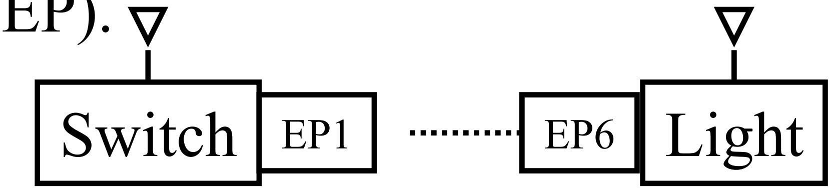


ZigBee Protocol Architecture



ZigBee Protocol Architecture (Cont)

- **Application Objects**: e.g., Remote control application. 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

ZigBee Application Layer

- Application layer consists of application objects (aka end points) 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 a number of profiles.
  Users can develop other profiles
- **Attributes**: Each profile requires a number of data items. Each data item is called an "attribute" and is assigned an 16-bit "attribute ID" by ZigBee forum

ZigBee Application Layer (Cont)

- **Clusters**: A collection of attributes and commands on them. Each cluster is represented by a 16-bit ID. Commands could be read/write requests or read/write responses
- **Cluster Library**: A collection of clusters. ZigBee forum has defined a number of cluster libraries, e.g., General cluster library contains on/off, level control, alarms, etc.
- **Binding**: Process of 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 end points.
  - Uses network management commands for network discover, route discovery, link quality indication, join/leave requests

ZigBee Application Profiles

- **Smart Energy**: Electrical, Gas, 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

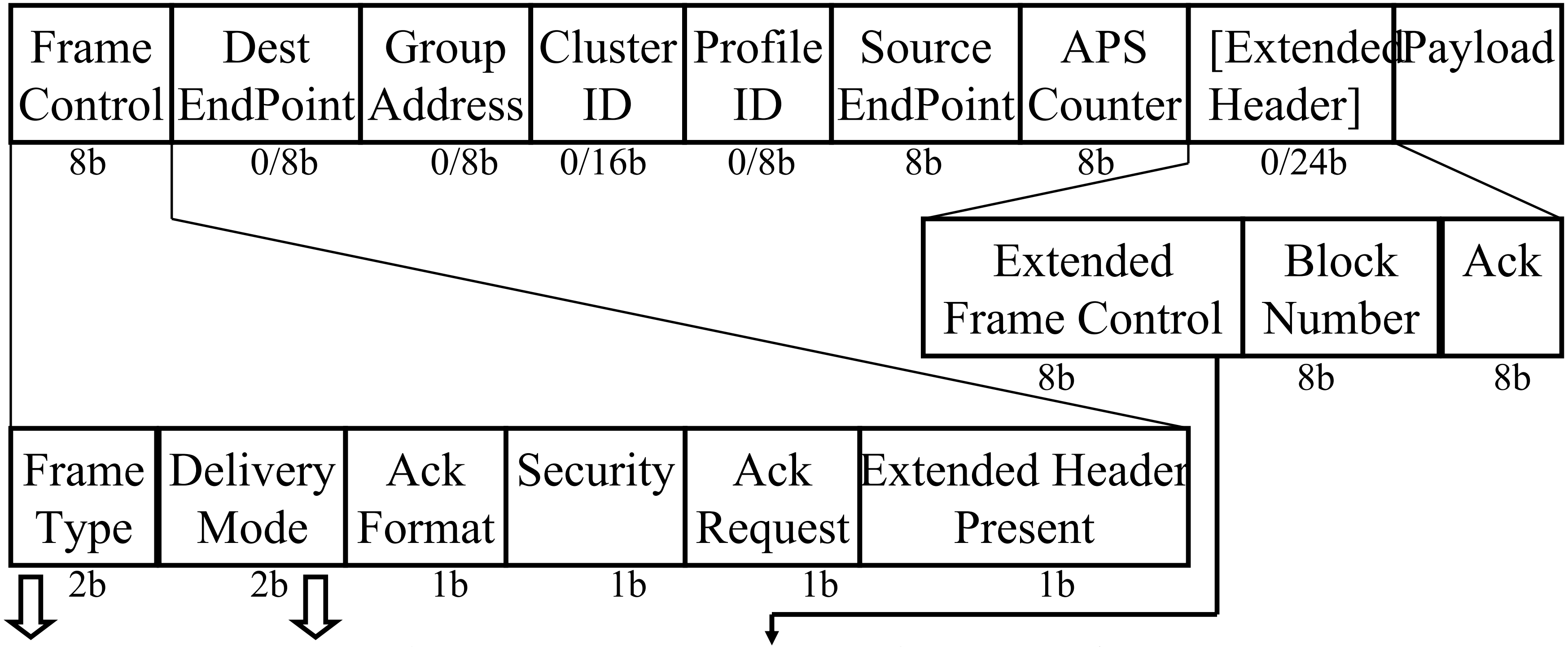
Ref: A. Elahi and A. Gschwender, "ZigBee Wireless Sensor and Control Network," Prentice Hall, 2009, 288 pp., ISBN:0137134851, Safari Book

ZigBee Application Support Layer

Components:

- APS Data Entity (APSDE)
- APS Management Entity (APSME)
- APS Information Base (AIB)

ZigBee APS Frame Format



Frame Control	Dest EndPoint	Group Address	Cluster ID	Profile ID	Source EndPoint	APS Counter	[Extended Header]	Payload
8b	0/8b	0/8b	0/16b	0/8b	8b	8b	0/24b	

Extended Frame Control	Block Number	Ack
8b	8b	8b

Frame Type	Delivery Mode	Ack Format	Security	Ack Request	Extended Header Present
2b	2b	1b	1b	1b	1b

00 Data	00 Unicast	00 Not fragmented
01 Command	01 Indirect addressing	01 first fragment, Block # is # of fragments
10 Ack	10 Broadcast	10 other fragments, Block # is fragment #
11 Reserved	11 Group addressing	11 Reserved

ZigBee APS Frame Format (Cont)

- **Ack Format**: 1⇒ Ack frame contains Cluster ID, profile ID, and source end point address
- **Security**: 1⇒ Enable security
- **Ack Request**: 1⇒ Please ack
- **Extended Header**: 1⇒ Extended header present
- **Ack**: Acknowledgment for a fragmented frame
- **Dest End Point**: Application # 0 through 240
- **Cluster ID**: 8-bit cluster in a profile
- **Profile ID**: Destination profile#
- **APS Counter**: APS Frame Sequence. All fragments have the same APS counter value.

ZigBee APS Frame Format (Cont)

- APS Ack frames do not have group address field, have extended header, and no payload.

Frame Control	Dest EndPoint	Cluster ID	Profile ID	Source EndPoint	APS Counter	Extended Header
8b	8b	0/16b	0/16b	8b	8b	24b

- APS Command frames are used for key establishment and switching, removing a device from the network.

Frame Control	Group Address	APS Counter	APS Command ID	APS Command Payload
8b	0/16b	8b	8b	

ZigBee Network Layer

Components:

1. Network Layer Data Entity (NLDE): Makes NPDU from NSDU
2. Network Layer Management Entity (NLME): Configure new device, neighbor discovery, route discovery, joining/leaving a network, …
3. Network Layer Information Base (NIB): Capabilities (RFD/FFD), Security level, protocol version, route discovery time, max retries for route discovery, neighbor table, …

ZigBee Network Layer Frame Format

Frame Control	Dest Addr	Src Addr	Radius	Seq #	Dest IEEE Addr	Src IEEE Addr	Multicast Control	**Source Route**	Payload
16b	16b	16b	8b	0/8b	0/64b	0/64b	0/8b	Variable	

Frame Type	Protocol Version	Discover Route	Multicast Flag	Security	Source Route	Dest IEEE Addr	Src IEEE Addr	Resvd
2b	4b	2b	1b	1b	1b	1b	1b	3b

00 Data
01 Command
10 or 11 Reserved

00 No discovery
01 If no route, discover
11 Force discovery

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

ZigBee Network Layer Frame Format (Cont)

- **Multicast Flag**: 1⇒ Multicast control present
- **Broadcast Frame Address**:
  FFFF=All devices, FFFD = Devices with receiver on
  FFFC = Coordinators/routers, FFFB = Low-Power Routers
- **Source Route**: Header contains route
- **Radius**: Hop limit
- **Destination/Source IEEE Address**: Address is an IEEE address
- **Security Field**: 1 ⇒ Secure outgoing frame
- Multicast Control Field

Neighbor Table

EUI-64	Short Address	Device Type	On while Idle	Relation	Transmission Failure	Link Quality	Cost	Hops from Coordinator	Permits new joins	Logical Channel

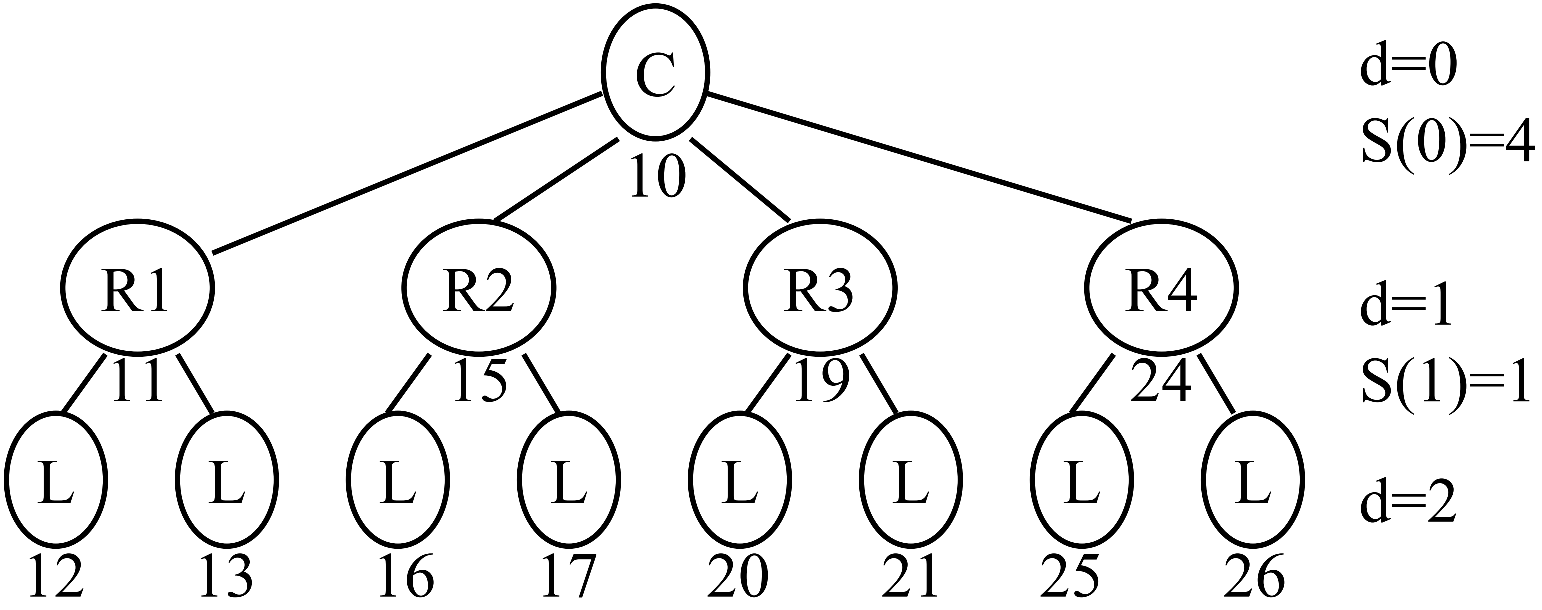
- 64-bit address, 16-bit address
- **Type**: 00 = Coordinator, 01=Router, 02=End device
- **On while Idle**: True ⇒ receiver always on
- **Relation**: 00=parent, 01=Child, 02=Sibling, 04=previous child, 05=unauthenticated child
- **Transmission Failure**: True=Previous transmission failed
- **Logical Channel**: Channel at which the neighbor is operating

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)

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

Distributed Scheme Example



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

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

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+6=17
- Address of R3 = 10+1+2*S(0) = 11+12 = 23
- Address of R3 = 10+1+3*S(0) = 11+18 =29
- 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 18 and 19

Stochastic Address Assignment

- Parent draws as 16 bit random number between 1 and 2^{16}-1 and assigns it to a new child
- Parent then advertises the number child to the network
- If another node has that address an address conflict message is returned and the parent draws another number and repeats

ZigBee Routing

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

AODV

- **A**d-hoc **O**n-demand **D**istance **V**ector Routing
- On-demand ⇒ Reactive ⇒ Construct a route when needed
- **Routing Table**: 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.

AODV (Cont)

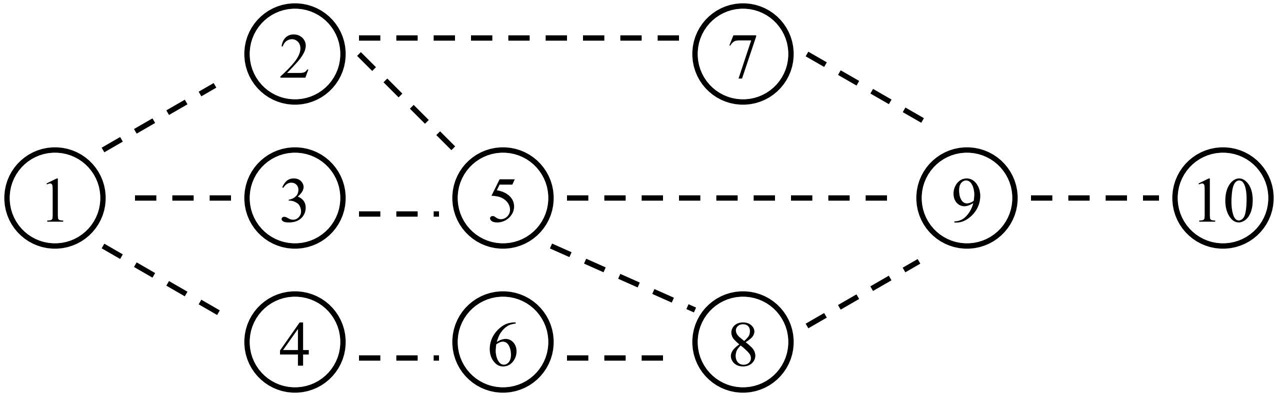
- Intermediate nodes can reply to RREQ only if they have a route to destination with higher destination sequence #
- ***Route reply*** **(RREP)** comes back "unicast" on the reverse path

Src Addr	Dest Addr	Dest Seq #	Hop Count	Life Time

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

AODV: Example

- Node 1 broadcasts RREQ to 2, 3, 4:
  "*Any one 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



AODV Example (Cont)

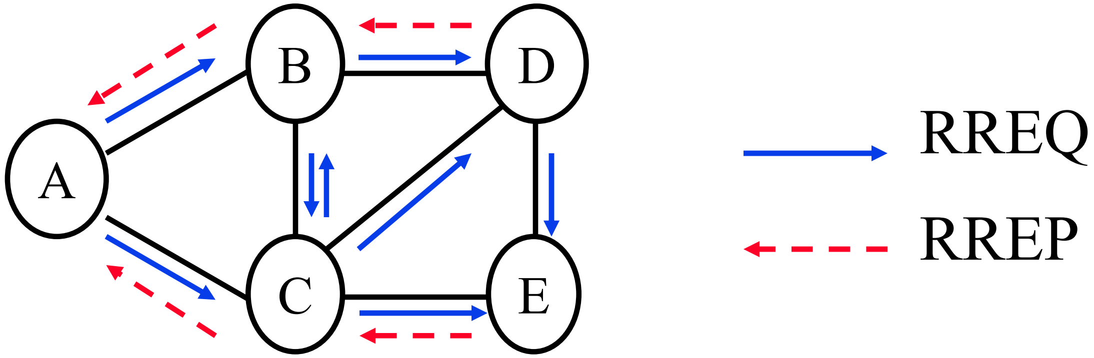
Pkt #	Pkt #				Req	Src	Dest			New Table Entry			
In	Out	From	To	Message	ID	Seq #	Seq #	Hops	Action at Receipient	Dest	Seq	Hops	Next
	1	1	2	RREQ	1	1	1	1	New RREQ. Broadcast	1	1	1	1
	2	1	3	RREQ	1	1	1	1	New RREQ. Broadcast	1	1	1	1
	3	1	4	RREQ	1	1	1	1	New RREQ. Broadcast	1	1	1	1
1	4	2	1	RREQ	1	1	1	2	Duplicate 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	6	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	1	1	4	9
12	22	9	10	RREQ	1	1	1	4	New RREQ. Respond	10	6	1	10
16	23	8	6	RREQ	1	1	1	3	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	2	9
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

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 member of the group, it sends a RREP message to the source and forwards to other neighbors. Intermediate nodes make a note of this and set up a forward path

Multicast Discovery Example

- D and E are members
- A concludes that the paths are ABD and ACE



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 an RERR, it starts route discovery with that sequence number.
- Disadvantage: Intermediate nodes may send more up-to-date but still stale routes.
- Ref: RFC3561

Dynamic Source Routing (DSR)

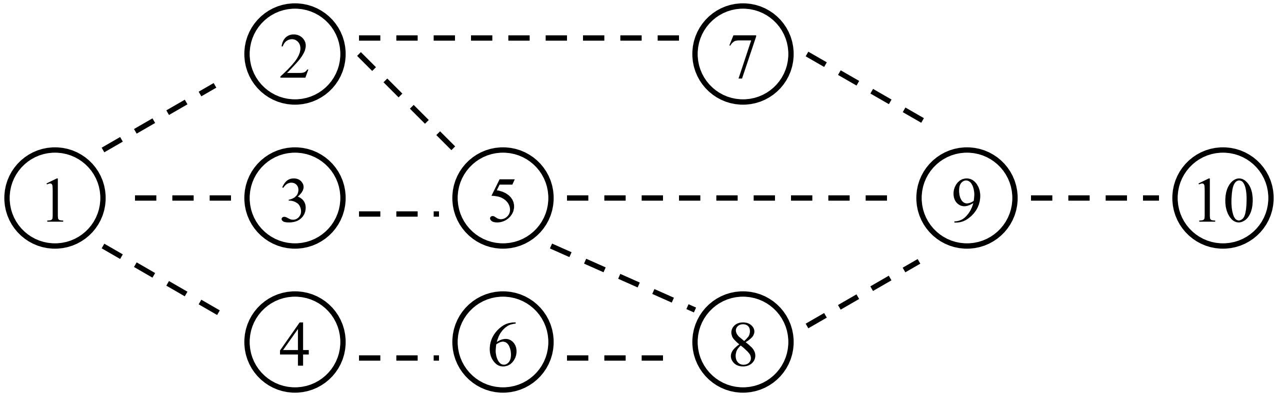
- On-Demand (reactive) routing using "Source Route“
- Source Route = List of routers along the path in the packet.
- **Routing database**: Complete route to recent destinations
- Each entry has an expiration period and is timed out
- If a route is not available, send "*route request*" to all neighbors

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

- Each neighbor adds itself to the route in the request and forward to all its neighbors (only first receipt). Does not change 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.

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



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	1-2-5-9-7
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)

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-initate 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

AODV vs. DSR

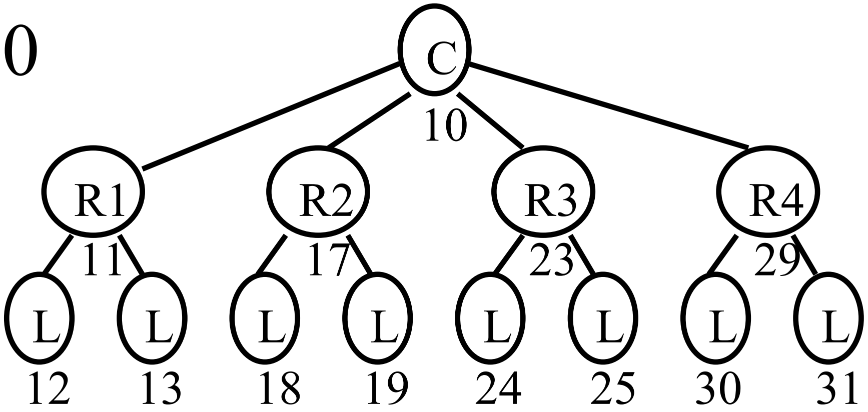
- In DSR a single RREQ can result in routes to several destination
- In DSR RERR messages are sent to the source not broadcast ⇒ Many nodes are unaware of failure
- In DSR, route discovery is delayed until all cached entries have been tried ⇒ Not good for high mobility

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

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

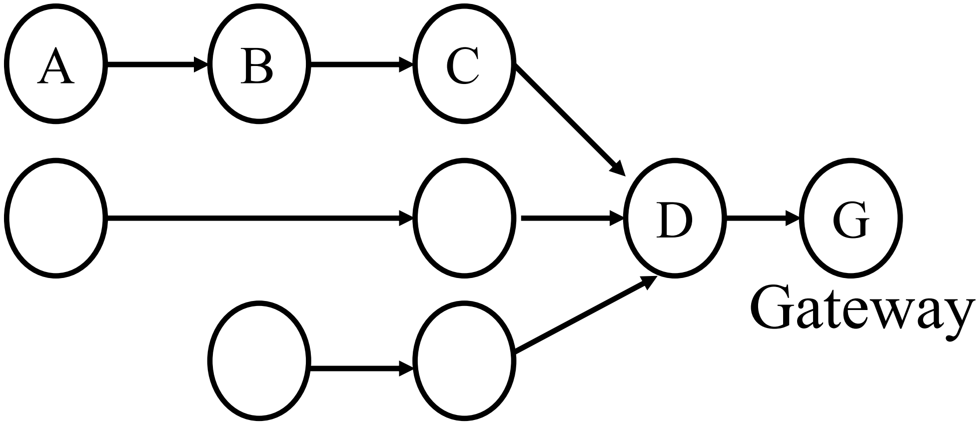
Tree Hierarchical Routing

- 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



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 towards gateway

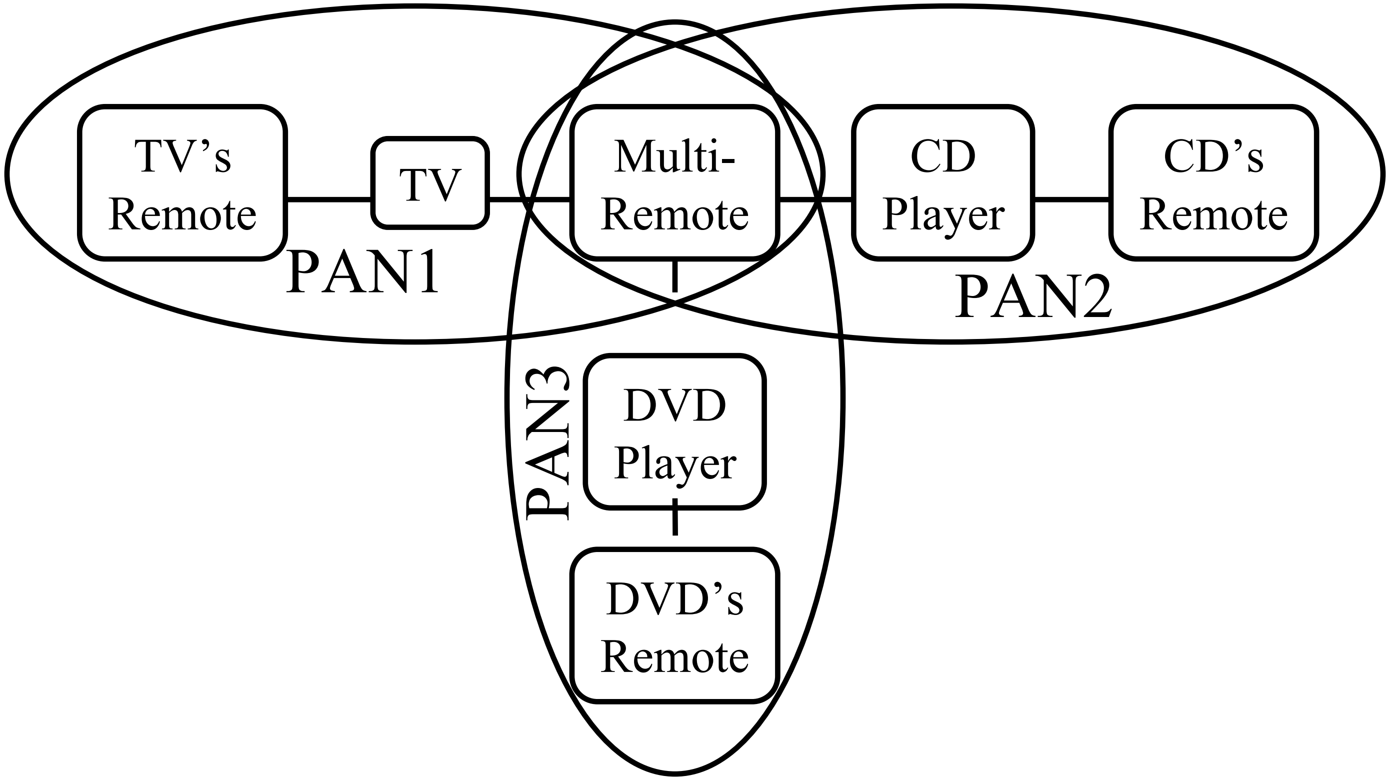


ZigBee RF4CE

- 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 ZigBee RF4CE protocol
- Operates on channels 15, 20, and 25 in 2.4 GHz
- 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**: Can locate remote control using a paging button on the target
- **Pairing**: A remote control works only with certain devices

RF4CE Multi-star Topology

- Each target device (TV, CD, …) forms a PAN with its remote
- Example: 3 PANs. Multi-function remote can control all 3 devices and is a member of all 3 PANs

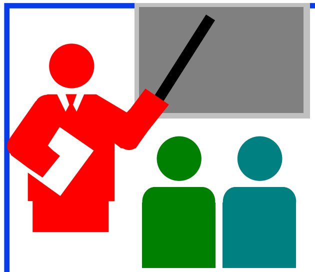


ZigBee RF4CE Pairing Process

- Allows a remote to be associated with the target
- Ensures specific remote will work with only specific TV
- Each remote and the target has a device ID, profiles that it supports, vendor ID
- When target receives a pairing command, it checks if the remote is listed in its pairing table. If yes, it accepts the pairing request.

ZigBee Smart Energy V2

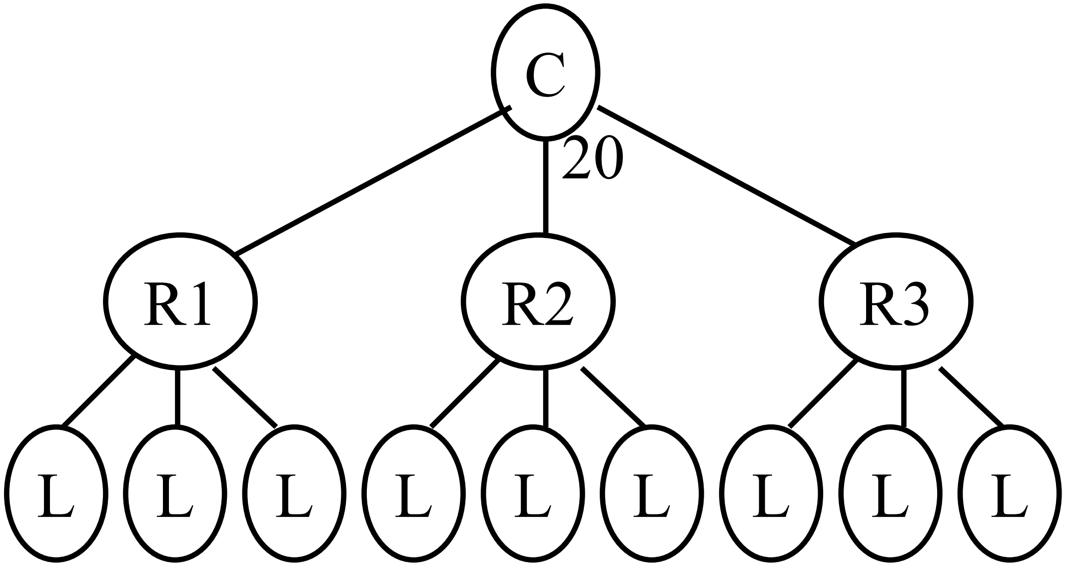
- Monitor, control, automate the delivery and use of energy and water
- Adds plug-in vehicle charging, configuration, and firmware download
- Developed in collaboration with other smart grid communication technologies: HomePlug, WiFi, …
- IP based ⇒ Incompatible with previous ZigBee



Summary

1. ZigBee is an IoT protocol for sensors, industrial automation, 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. A number of 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.

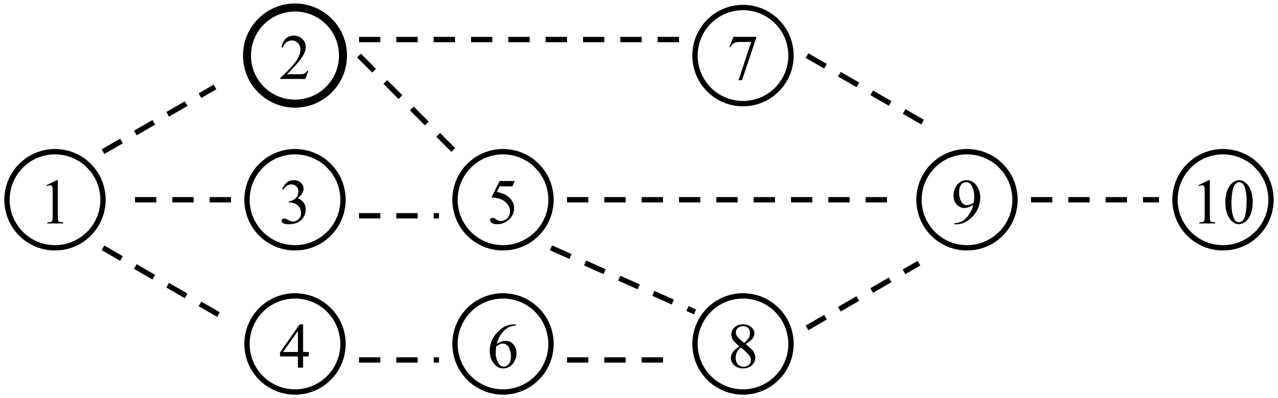
Homework 13A



- 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 maximum 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.

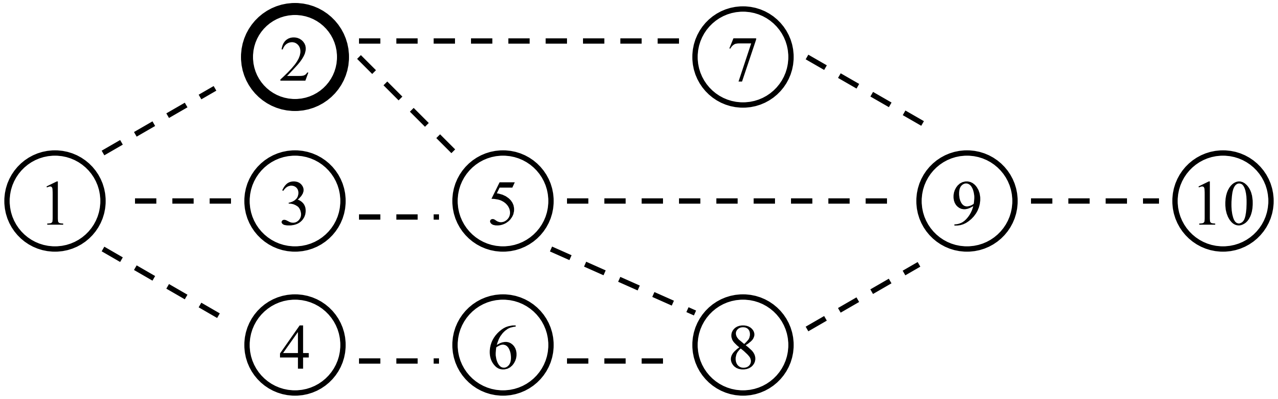
Homework 13B

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



Homework 13C

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



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

Related Wikipedia Pages

- http://en.wikipedia.org/wiki/ZigBee
- http://en.wikipedia.org/wiki/ZigBee_specification
- 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

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

References (Cont)

- ZigBee Alliance Technical Documents, http://www.zigbee.org/Products/TechnicalDocumentsDownload/tabid/237/Default.aspx
- ZigBee Alliance Whitepapers, http://www.zigbee.org/LearnMore/WhitePapers/tabid/257/Default.aspx
- ZigBee Alliance, ZigBee Specification Document 053474r17, 2008
- 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

References (Cont)

- ZigBee IEEE 802.15.4 Summary, http://www.eecs.berkeley.edu/~csinem/academic/publications/zigbee.pdf
- 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

Acronyms

AIB	Application Information Base
AODV	Ad-Hoc On-Demand Distance Vector
APS	Application Support Sublayer
APSDE	Application Support Sublayer Data Entity
APSME	Application Support Sublayer Management Entity
CD	Compact Disc
CSMA/CA	Carrier Sense Multiple Access
DSR	Dynamic Source Routing
DVD	Digital Video Disc
EP	End Point
FCC	Federal Communications Commission
GHz	Giga Hertz
HDTV	High Definition Television
ID	Identifier
IEEE	Institution of Electrical and Electronic Engineers
IoT	Internet of Things

Acronyms (Cont)

IP	Internet Protocols
ISM	Instrumentation, Scientific, and Medical
kB	Kilo byte
MAC	Media Access Control
MHz	Mega Hertz
NIB	Network Layer Information Base
NLDE	Network Layer Data Entity
NLME	Network Layer Management Entity
NPDU	Network Protocol Data Unit
NPDU	Network Service Data Unit
OFDM	Orthogonal Frequency Division Multiplexing
PAN	Personal Area Network
PHHC	Personal, Home, and Hospital Care
PHY	Physical Layer
RF4CE	Radio Frequency for Consumer Electronics
RFC	Request for Comment

Acronyms (Cont)

RFID	Radio Frequency ID
RREP	Route Reply
RREQ	Route Request
TV	Television
UWB	Ultra Wide-Band
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
ZDO	ZigBee Device Object