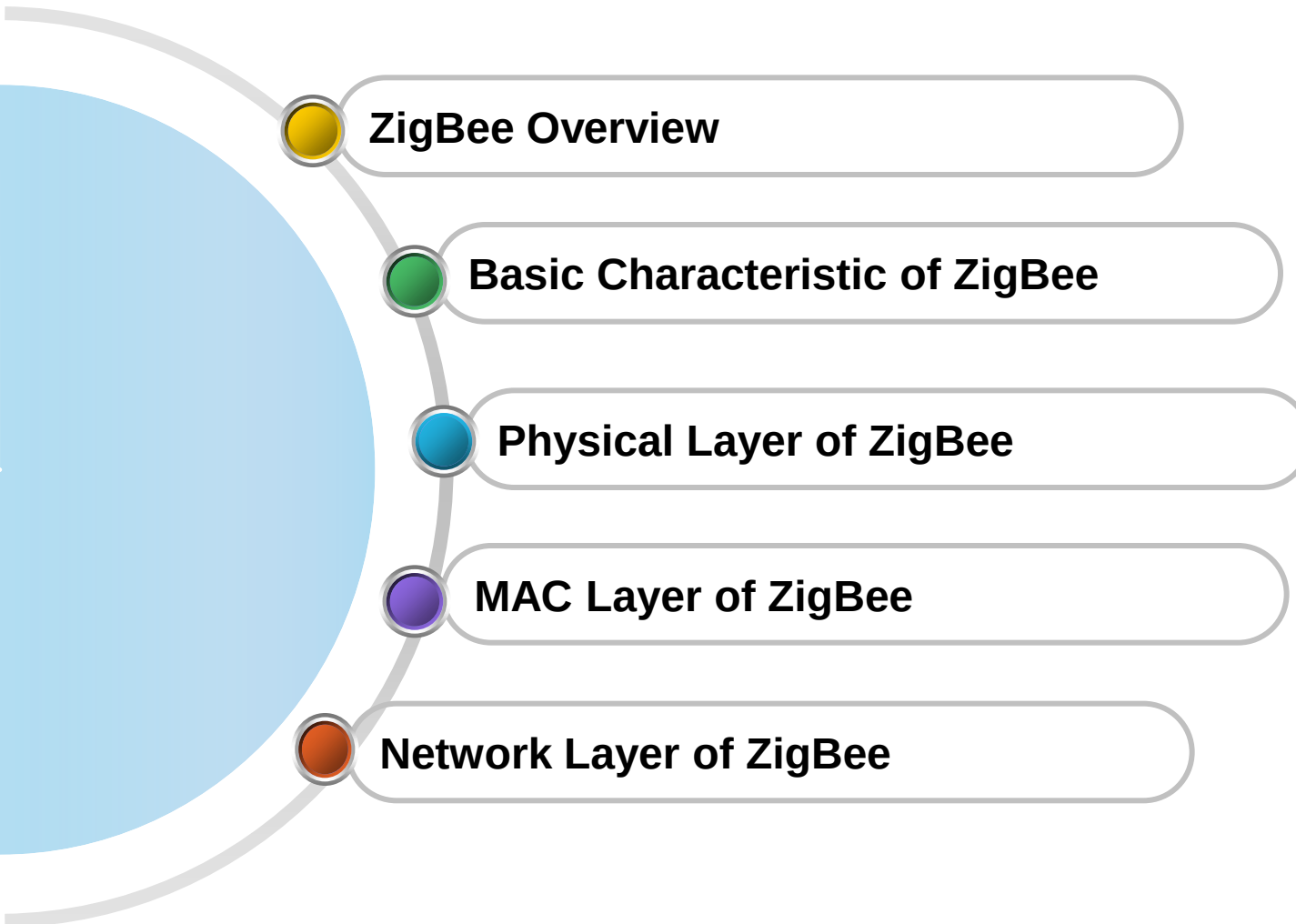


Chapter 5

ZigBee

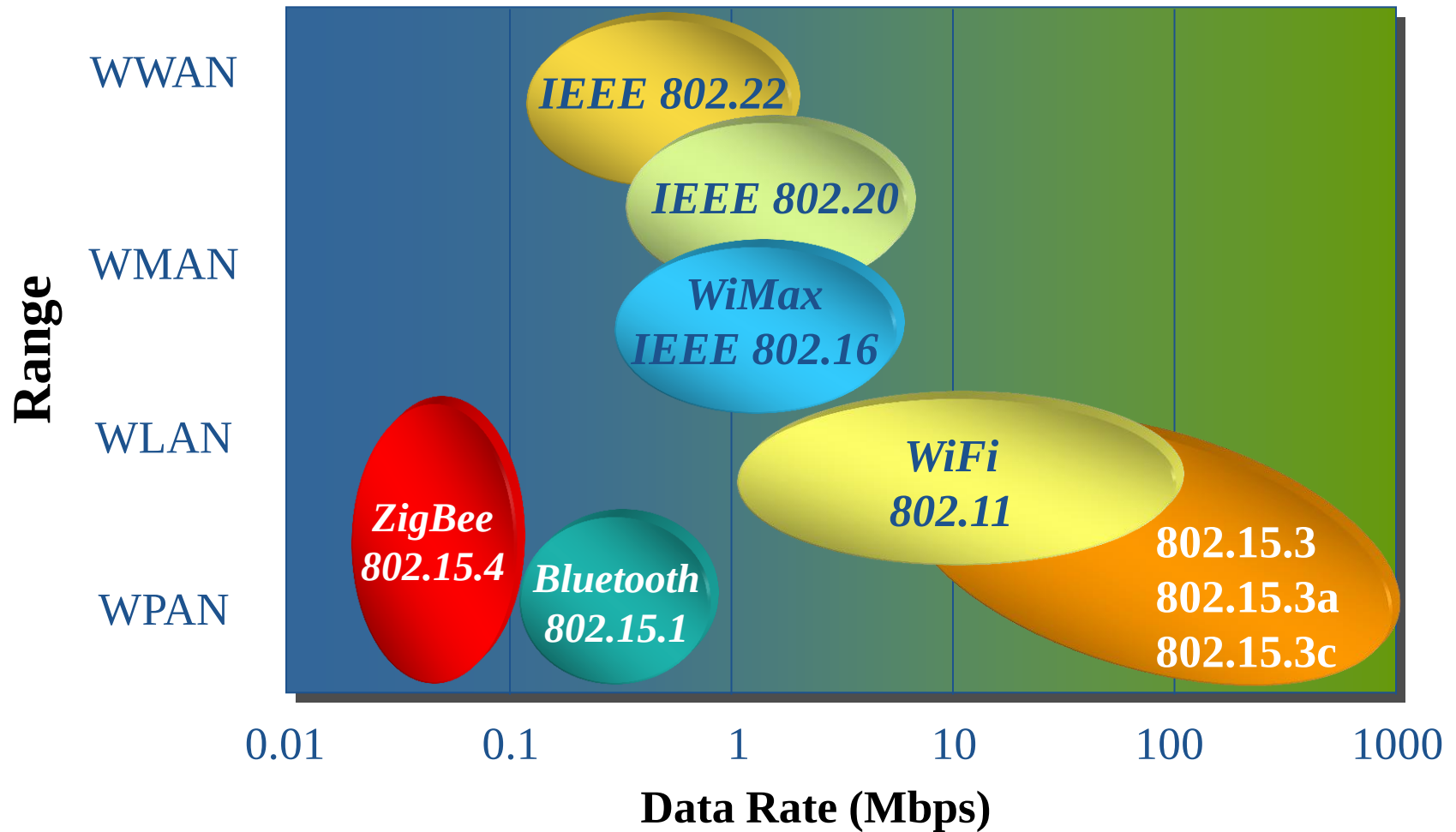
Dr K. F. Tsang
EE4036



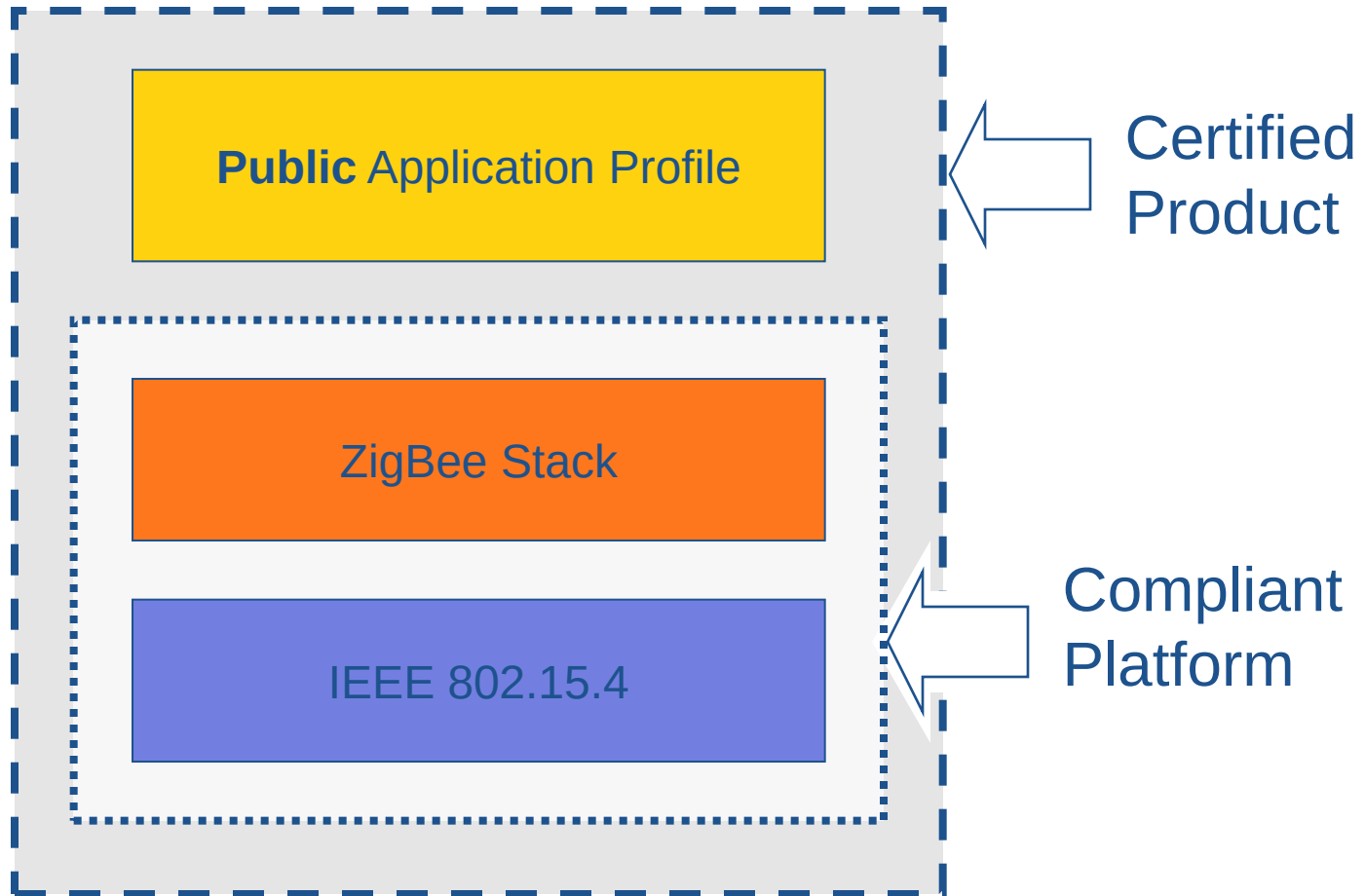
Overview

***Chapter 1: Introduction,
ZigBee: From Design to Applications,
(Prentice Hall)***

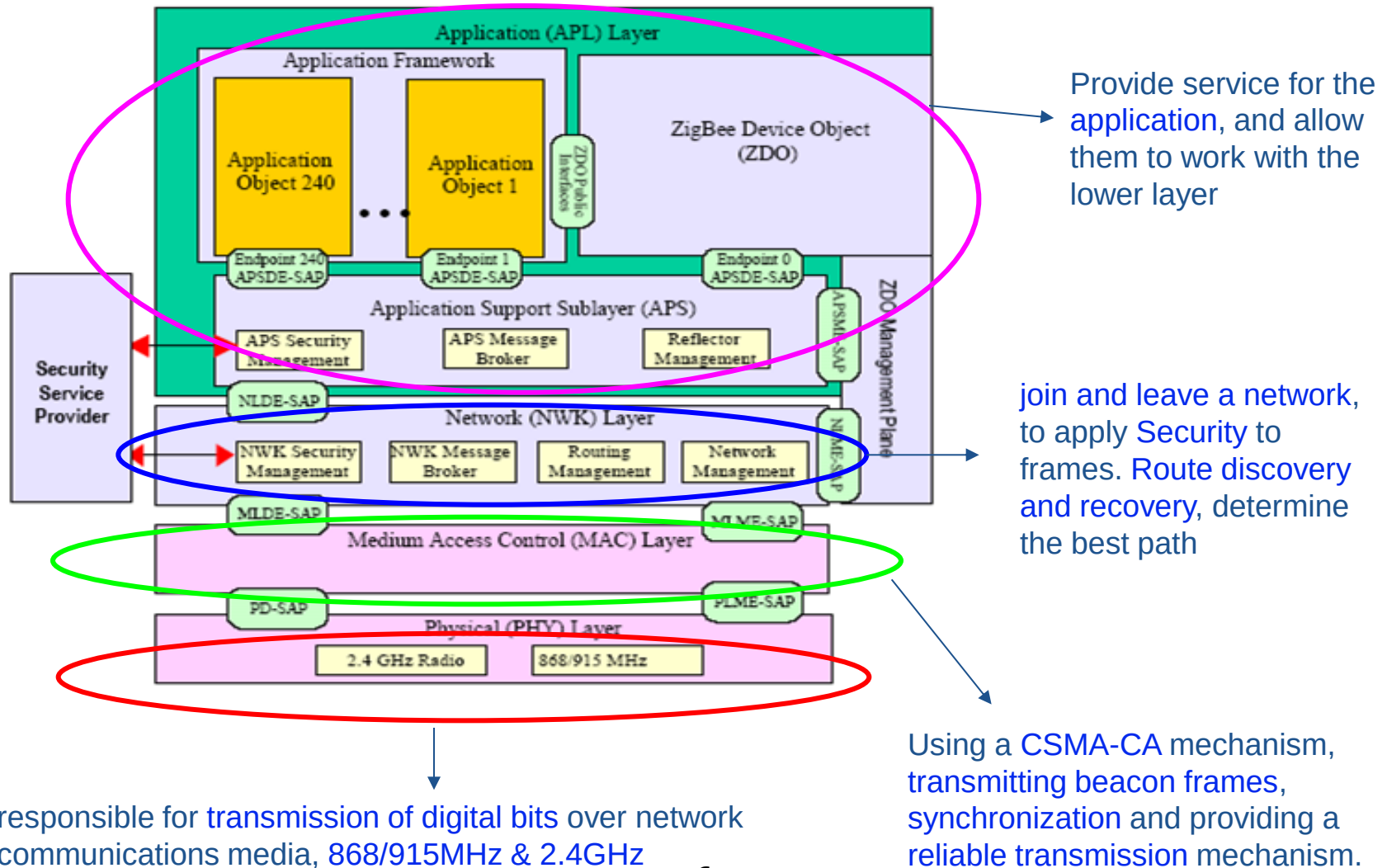
The 802 Wireless Space



The ZigBee Platform



Stack overview



Differences between ZigBee and Bluetooth

ZigBee and Bluetooth

Optimized for different applications

❖ ZigBee

- Smaller packets over large network
- Mostly Static networks with many, infrequently used devices
- Home automation, toys, remote controls, etc.

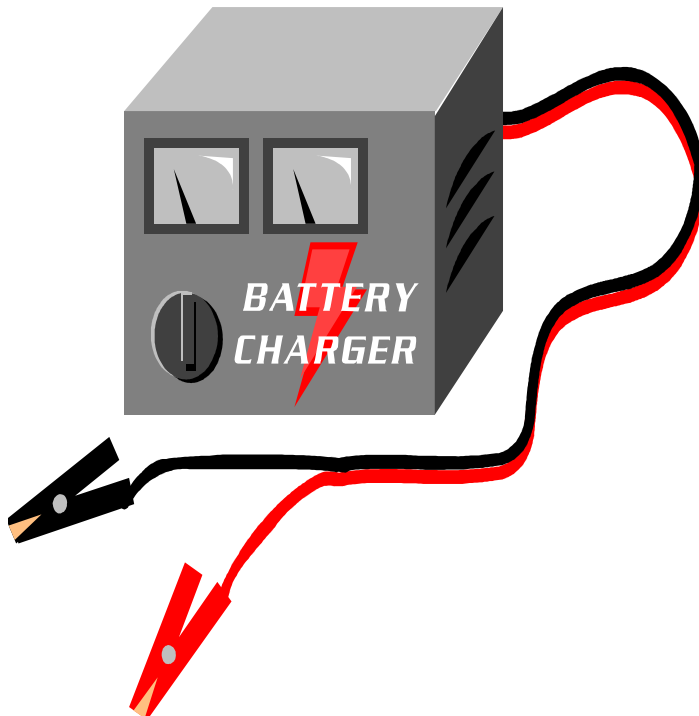
❖ Bluetooth

- Larger packets over small network
- Ad-hoc networks
- File transfer
- Screen graphics, pictures, hands-free audio, Mobile phones, headsets, PDAs, etc.



ZigBee and Bluetooth

Address Different Needs



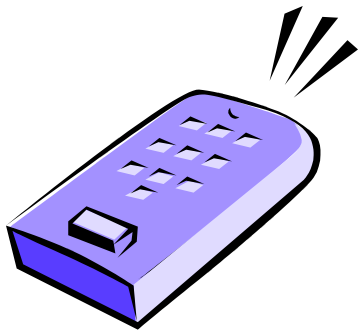
- ❖ Bluetooth is a cable replacement for items like Phones, Laptop Computers, Headsets
- ❖ Bluetooth expects regular charging
 - Target is to use <10% of host power

ZigBee and Bluetooth

Address Different Needs

❖ ZigBee is better for devices
Where the battery is 'rarely'
replaced

- Targets are :
 - Tiny fraction of host power
 - New opportunities where wireless not yet used

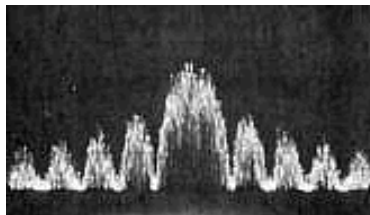


ZigBee and Bluetooth

Air interface

ZigBee

- ❖ DSSS
- ❖ 62.5 K symbols/s
- ❖ 4 Bits/ symbol
- ❖ Peak Information Rate
~128 Kbit/second

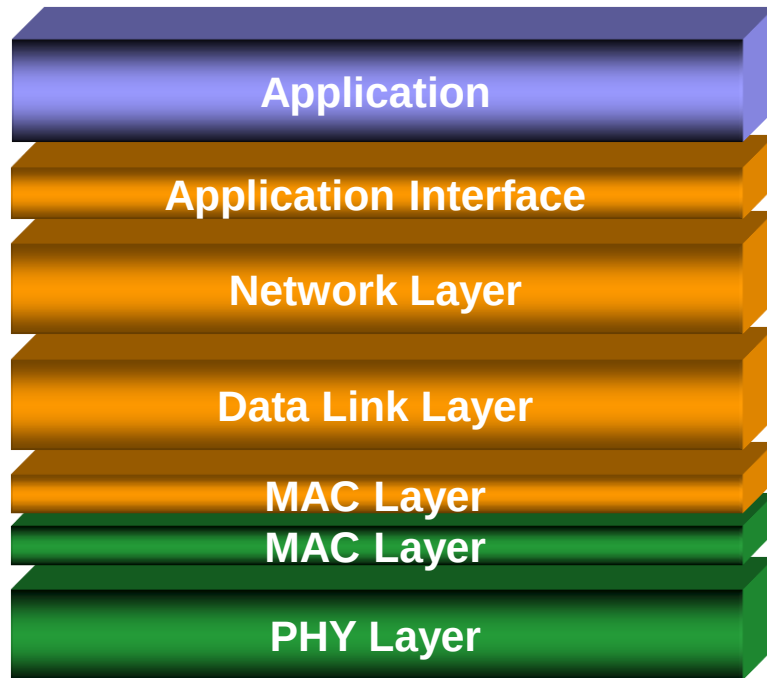


Bluetooth

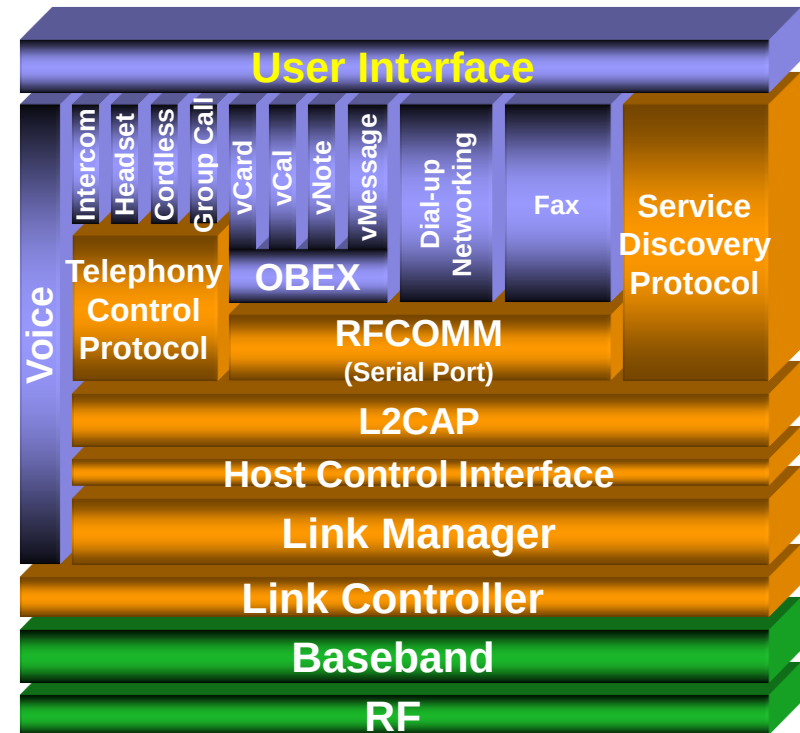
- ❖ FHSS
- ❖ 1 M Symbol / second
- ❖ Peak Information Rate
~720 Kbit / second



ZigBee and Bluetooth



Zigbee



Bluetooth

Protocol Stack Comparison

ZigBee and Bluetooth

Comparison Overview

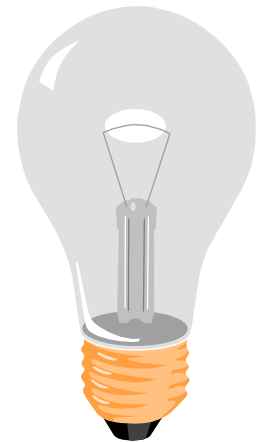
	Bluetooth	ZigBee
Air Interface	FHSS	DSSS
Protocol Stack	250kb	28kb
Device / Cluster	8	255
Link Rate	1Mbps	250kbps
Range	~10 meter (w/o pa)	~100 meters

An Application Example

Battery Life & Latency in a Light Switch



- ❖ **Wireless Light switch –**
 - Easy for Builders to Install
- ❖ **A Bluetooth Implementation would either :**
 - keep a counter running so that it could predict which hop frequency the light would have reached or
 - use the inquiry procedure to find the light each time the switch was operated.



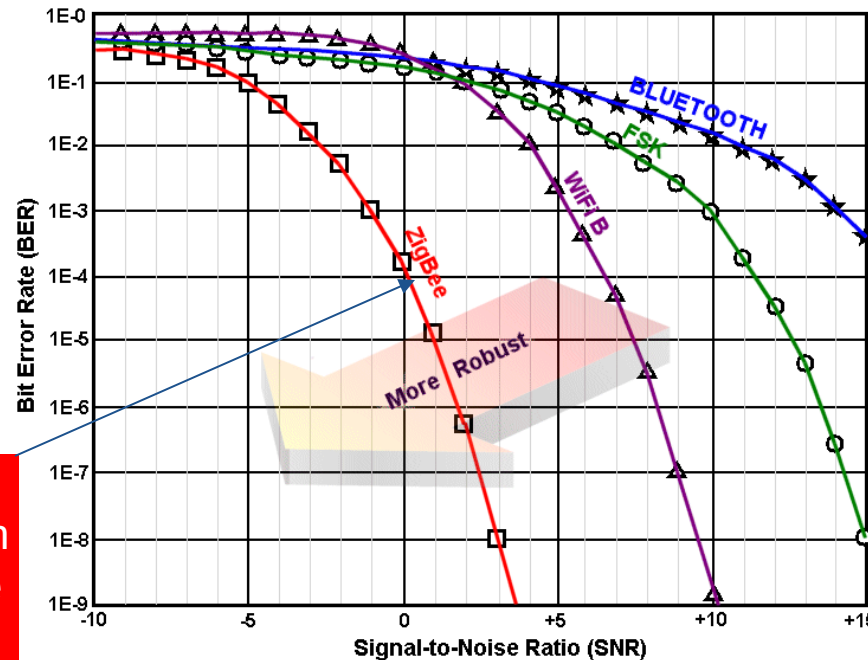
Physical Layer

***Chapter 3: The Physical Layer,
ZigBee: From Design to Applications,
(Prentice Hall)***

What is ISM Band

- ❖ stands for the industrial, scientific and medical (ISM) radio bands
- ❖ reserve internationally for the use of RF electromagnetic fields for industrial, scientific and medical purposes other than communications
- ❖ In general, communications equipment must accept any interference generated by ISM equipment

Basic Radio Characteristics



ZigBee technology relies upon IEEE 802.15.4, which has excellent performance in low SNR environments

Frequency Band	License Required?	Geographic Region	Data Rate	Channel Number(s)
868.3 MHz	No	Europe	20kbps	0
902-928 MHz	No	Americas	40kbps	1-10
2405-2480 MHz	No	Worldwide	250kbps	11-26

Possible Interference in 2.4GHz

❖ possible users and possible interferers includes:

- 802.11b/g/n networks
- Bluetooth Pico-Nets
- 802.15.4-based Personal Area Network (PAN)
- Cordless Phones
- Home Monitoring Cameras
- Microwave ovens
- Wireless headsets

Basic Radio Characteristics

PHY	Frequency Band	Channel Numbering	Spreading Parameters		Data Parameters		
			Chip Rate	Modulation	Bit Rate	Symbol Rate	Modulation
868/ 915 MHz	868- 870MHz	0	300 kchip/s	BPSK	20 kb/s	20 ks/s	BPSK
	902- 928MHz	1 to 10	600 kchip/s	BPSK	40 kb/s	40 ks/s	BPSK
2.4G Hz	2.4- 2.4835GHz	11 to 26	2.0 Mchip/s	O-QPSK	250 kb/s	62.5ks/ s	16-ary Orthogonal

Offset Quadrature phase-shift keying

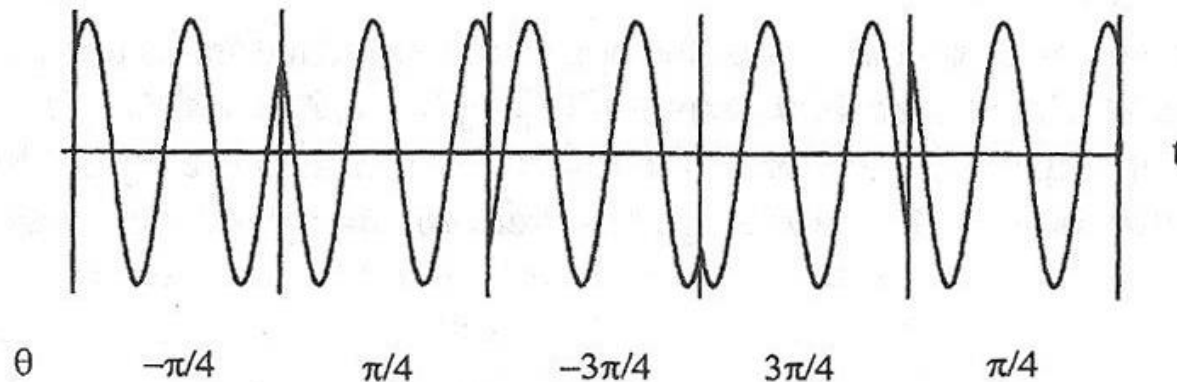
❖ Offset quadrature phase-shift keying (O-QPSK) is essentially the same as QPSK except that the I- and Q-channel pulse trains are staggered

❖ OQPSK Signal

$$s(t) = \frac{A}{\sqrt{2}} I(t) \cos 2\pi f_c t - \frac{A}{\sqrt{2}} Q\left(t - \frac{T}{2}\right) \sin 2\pi f_c t \quad -\infty < t < \infty$$

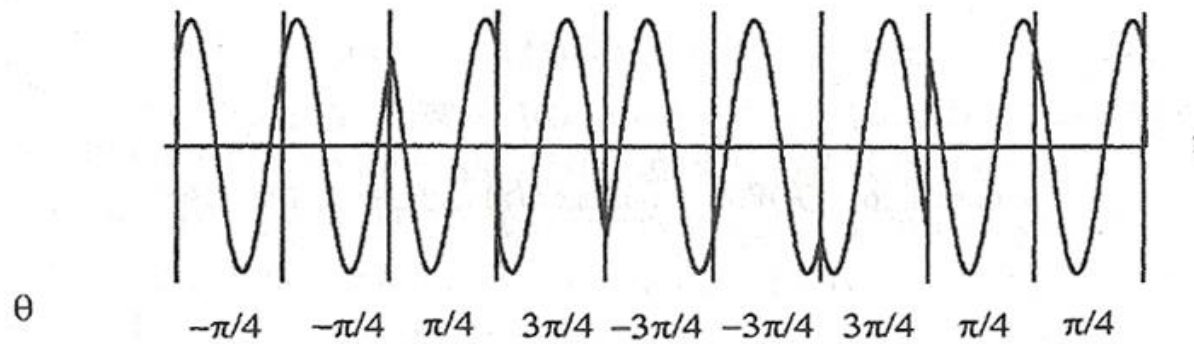
Offset Quadrature phase-shift keying

$$s(t) = I(t)\cos 2\pi f_c t - Q(t)\sin 2\pi f_c t$$



QPSK Signal

$$I(t)\cos 2\pi f_c t - Q(t - \frac{T}{2})\sin 2\pi f_c t$$

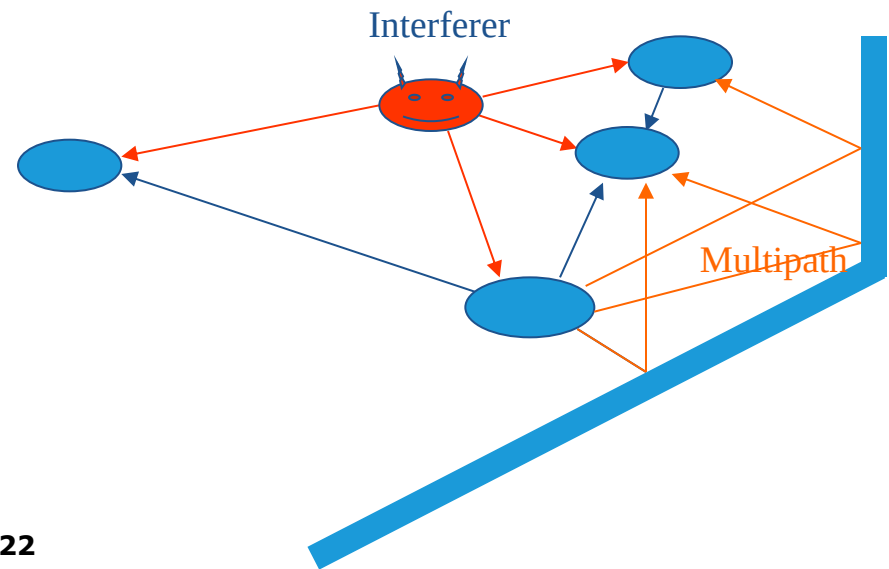


O-QPSK Signal

Reliability in PHY Layer

❖ Problem faces:

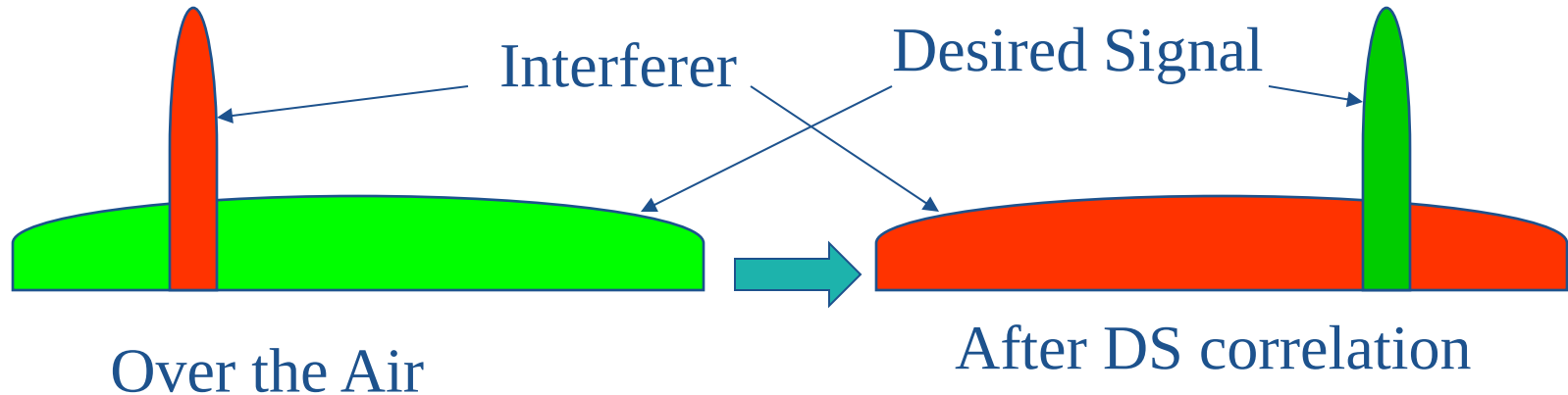
- Dispersion
- Multipath
- Interference
- Frequency dependent fading



❖ Solution:

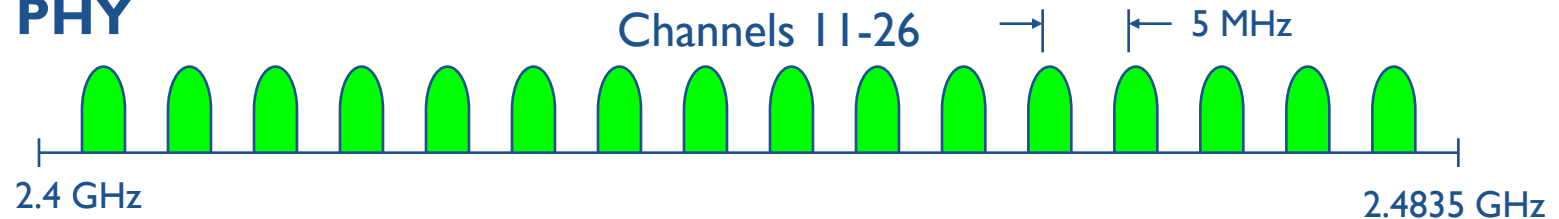
- Direct sequence: allows the radio to reject multipath and interference by use of a special “chip” sequence. The more chips per symbol, the higher its ability to reject multipath and interference.

Direct Sequence and Frequency Agility



2.4 GHz

PHY



Medium Access Control Layer

***Chapter 4 The Media Access Control
Layer,
ZigBee: From Design to Applications,
(Prentice Hall)***

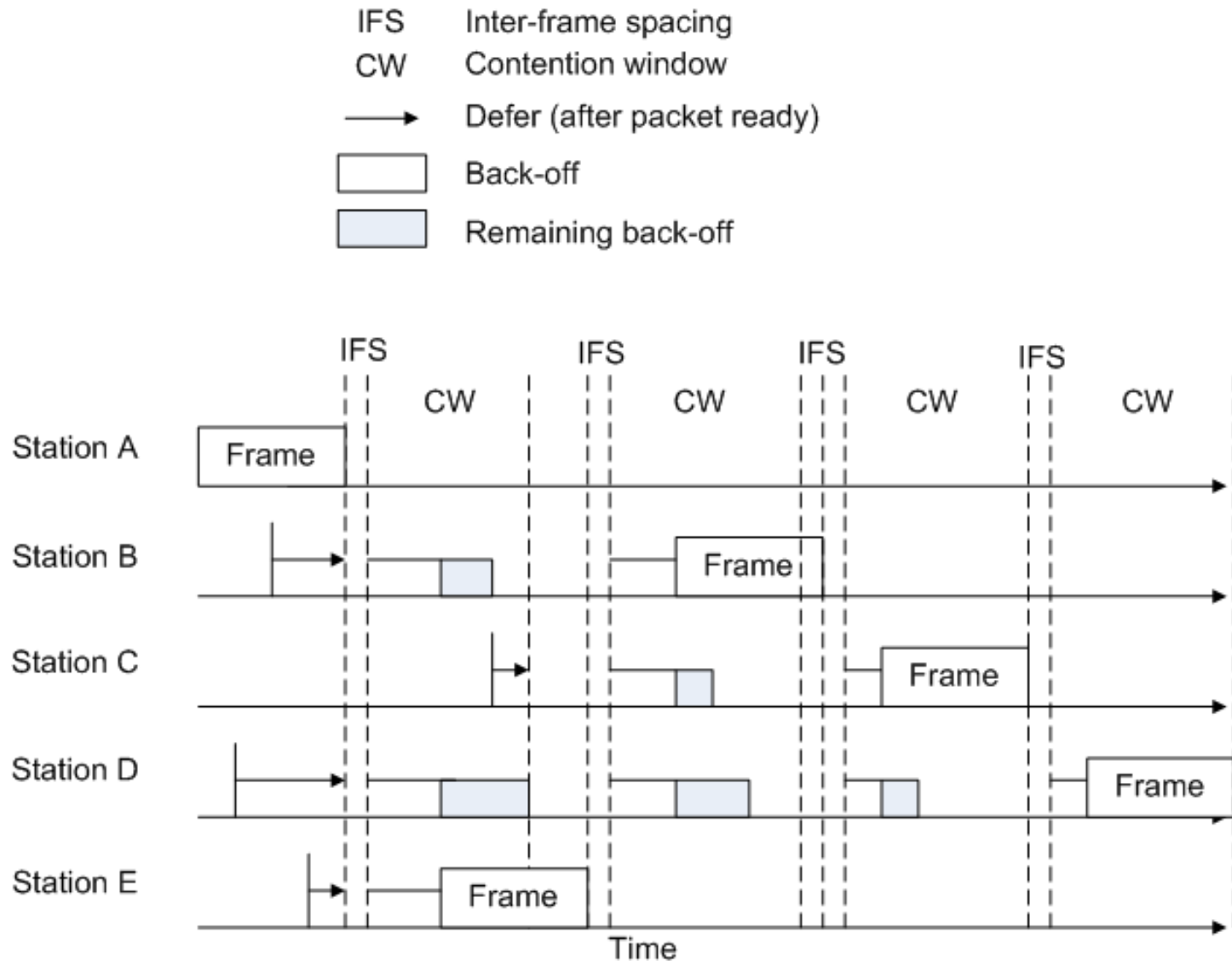
Overview of MAC Layer

- Over-the-air data rates of 250kb/s, 40kb/s, and 20kb/s
- Star or peer-to-peer operation
- Allocated 16bit short and 64 bit extended address
- Allocation of guaranteed time slots (Beacon Mode: power saving)
- CSMA-CA channel access (Non-Beacon Mode)
- Fully acknowledged protocol: high reliability

Overview of MAC Layer (Con't)

- Channel Selection
 - Energy detection (ED)
 - Link quality indication (LQI)
- 16 channels in the 2450 MHz band, 10 channels in the 915 MHz band, and 1 channel in the 868 MHz band

Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)



Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)

1. Station A has a frame in the air when stations B, D, and E sense the channel and finds it busy
2. Each of the three stations will run its random number generator to get a back-off time by random
3. Station E followed by B and D draws the smallest number
4. All three terminal persists on sensing the channel and defer their transmission until the transmission of terminal A is completed
5. After completion, all three terminals wait for the inter-frame spacing (IFS) and start their counters immediately afterward
6. As soon as E's backoff timer expires, it starts transmission of its frame

Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)

7. When E starts transmitting, B and D freeze their counters
8. After E has completed its transmission and another period IFS has elapsed, B and D resumes their counters
9. B will finish its counter first and starts transmission. Then C and E transmit
10. The advantage of this back-off strategy over the exponential back-off is that the waiting time is fairly distributed in a way that on average enforces a first-come, first serve policy

Channel Access Options

Two channel access mechanisms:

- ❖ Non-beacon network
 - A simple, traditional multiple access system used in simple peer and near-peer networks
 - Standard CSMA-CA communications
 - Positive acknowledgement for successfully received packets
- ❖ Beacon-enabled network (Slotted CSMA-CA)
 - Superframe structure- network coordinator transmits beacons at predetermined intervals
 - Dedicated bandwidth and low latency
 - Low Power Consumption mode for Coordinator

The Function of Superframe (Beacon Frame)

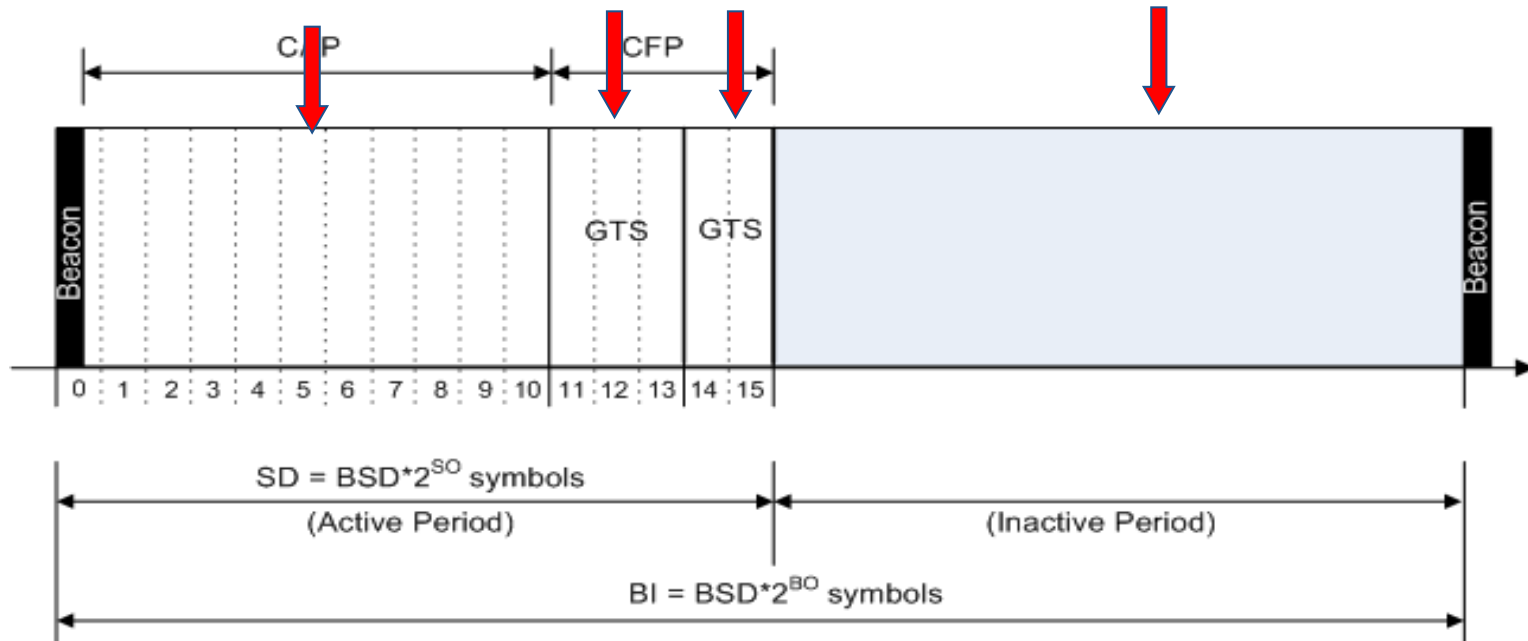
- To synchronize the attached device

Node send message to
coordinator for requesting
time slot



Is data

All nodes sleep



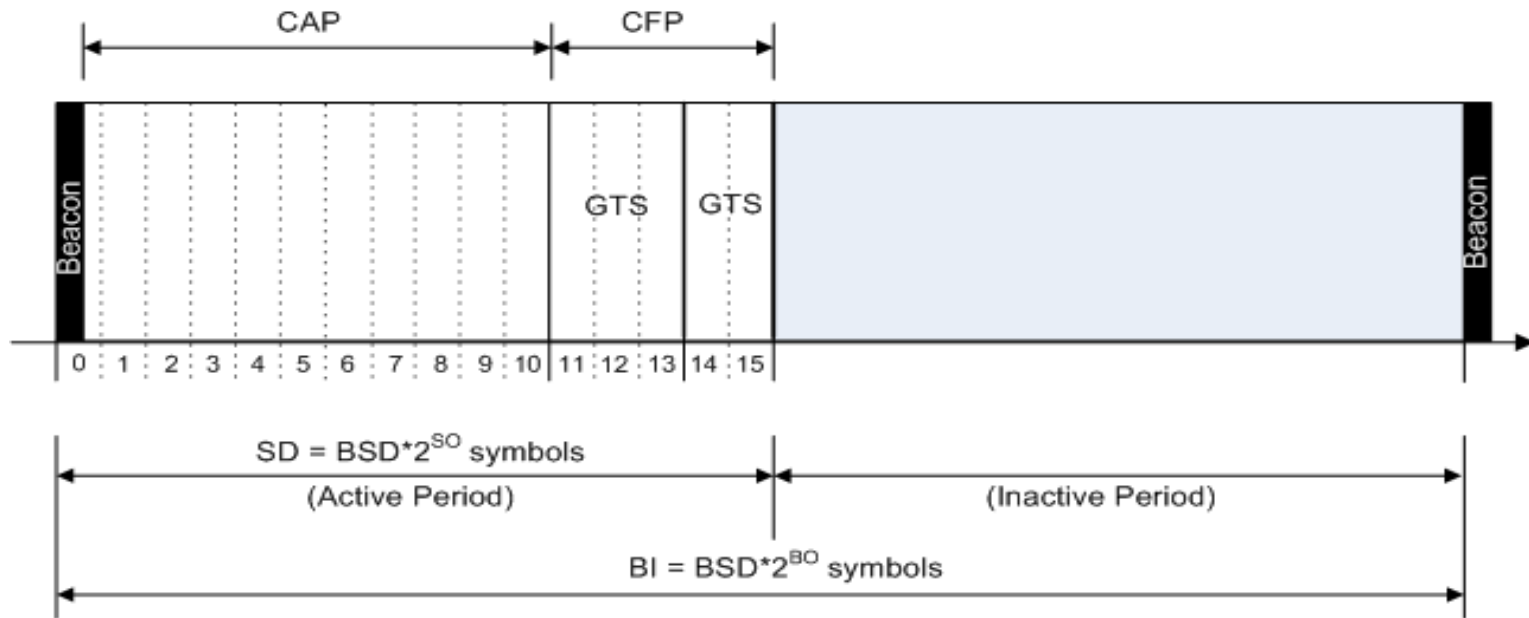
BO: *BeaconOrder* $0 \leq BO \leq 14$

SO: *SuperframeOrder* $0 \leq SO \leq BO \leq 14$

BI : beacon interval

SD : superframe duration

The Function of Superframe (Beacon Frame)



O-QPSK symbol time (s) = $1/(62500) = 1.6 \times 10^{-5}$

BSD = BaseSlotDuration x NumSuperframeSlots = 60 x 16
(from IEEE 802.15.4 specification)

BI = BSD x 2^{BO}

If $BO = 0$, $BI = 0.15$ s

If $BO = 14$, $BI = 252$ s

Slotted CSMA-CA

- The backoff slots are aligned with the start of the beacon transmission
- Device want to transmit data frame in CAP -> locate the boundary of next backoff slot -> wait for a random number of backoff slots

If the channel is busy -> follow the backoff -> wait for another random period

Else, begin transmission on the next available backoff slot boundary

Example of Beacon Network

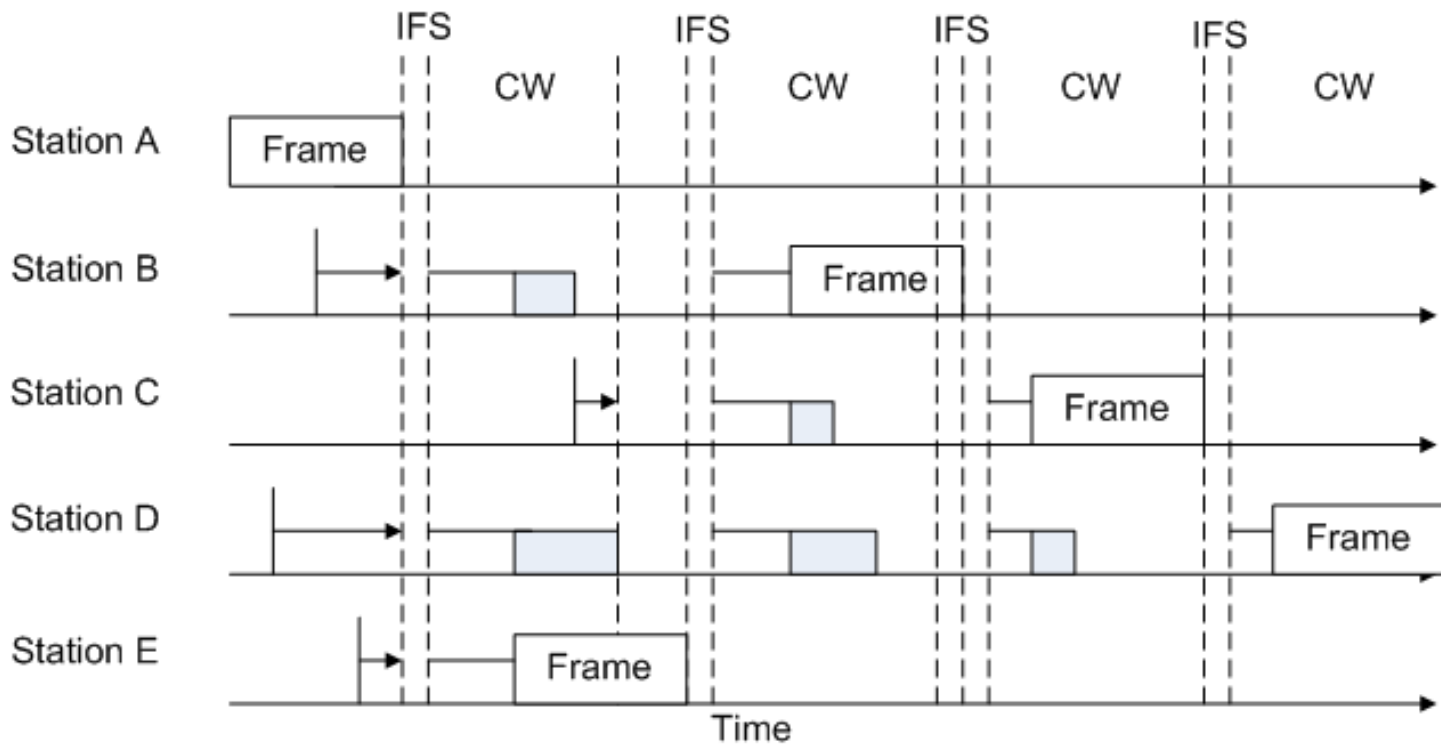
- ❖ Now make the ZigBee Coordinator battery-operated also
 - All units in system are now battery-operated
 - Client registration to the network
 - Client unit when first powered up listens to the ZigBee Coordinator's network beacon (interval between 0.015 and 252 seconds)
 - Register with the coordinator and look for any messages directed to it
 - Return to sleep, awaking on a schedule specified by the ZigBee Coordinator
 - Once client communications are completed, ZigBee coordinator also returns to sleep

Example of Beacon Network

- ❖ -This timing requirement potentially impacts the cost of the timing circuit in each end device
- ❖ *Longer intervals of sleep mean that the timer must be more accurate or
- ❖ *Turn on earlier to make sure that the beacon is heard, increasing receiver power consumption, or
- ❖ *Improve the quality of the timing oscillator circuit (increase cost) or
- ❖ *Control the maximum period of time between beacons to not exceeding 252 seconds, keeping oscillator circuit costs low

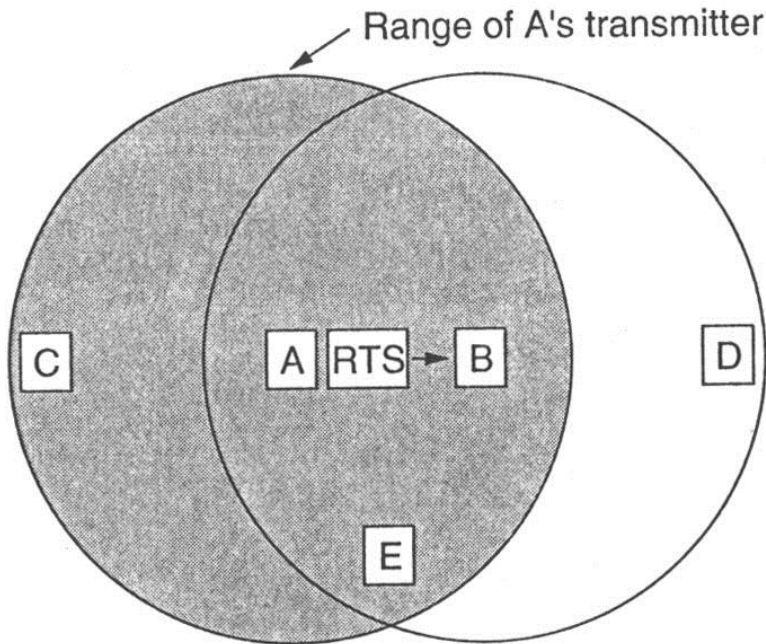
Non beacon-enabled model

IFS Inter-frame spacing
CW Contention window
→ Defer (after packet ready)
Back-off
Remaining back-off

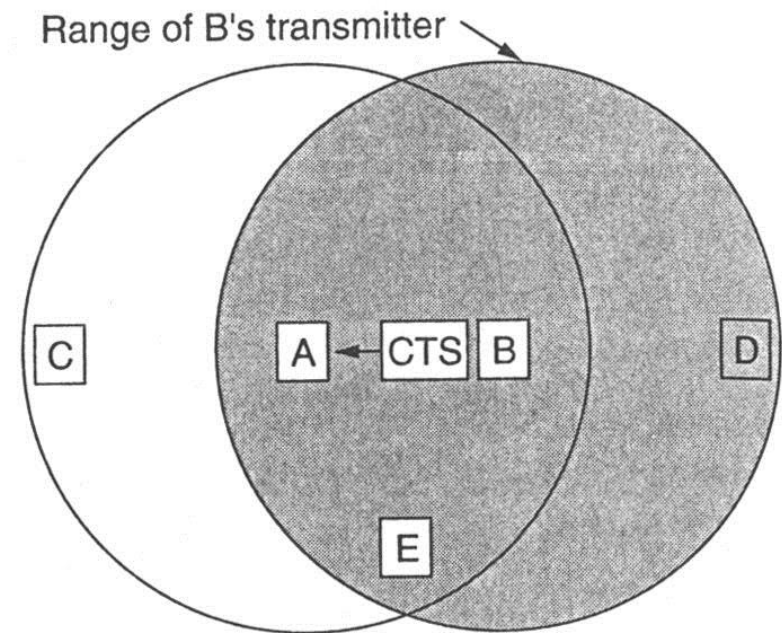


Non beacon-enabled model

- ❖ Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- ❖ It does solve Hidden Terminal Problem



(a)

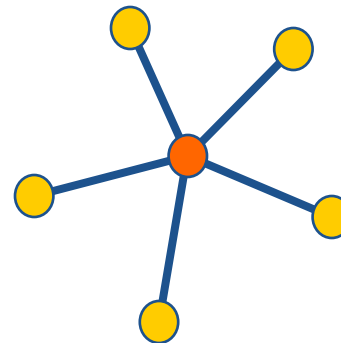


(b)

Example of Non-Beacon Network

❖ Commercial or home security

- Client units (intrusion sensors, motion detectors, glass break detectors, standing water sensors, loud sound detectors, etc)
 - Sleep 99.999% of the time
 - Wake up on a regular yet random basis to announce their continued presence in the network (“12 o’clock”)
 - When an event occurs, the sensor wakes up instantly and transmits the alert (“Somebody’s on the front porch”)



Example of Non-Beacon Network

- ❖ The ZigBee Coordinator, mains powered, has its receiver on all the time and so can wait to hear from each of these stations
- ❖ *Since ZigBee Coordinator has “infinite” source of power it can allow clients to sleep for unlimited periods of time to allow them to save power

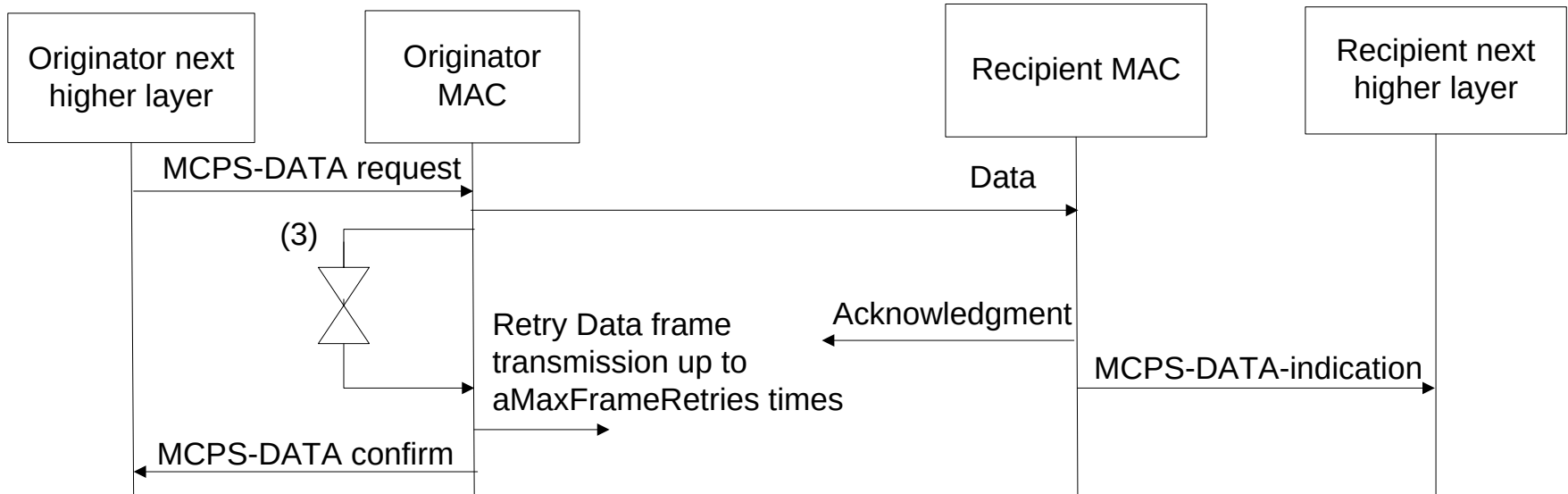
❖ Problem faces:

- Sleeping nodes
- Hidden nodes (solved by CSMA/CA)

MAC:

- ❖ Coordinator buffering is where the network coordinator buffers messages for sleeping nodes until they wake again
- ❖ ARQ (acknowledgement request) is where a successful transmission is verified by replying with an acknowledge (ACK). If the ACK is not received the transmission is sent again

Acknowledgement request (ARQ)



Network Layer

***Chapter 5: The Network Layer,
ZigBee: From Design to Applications,
(Prentice Hall)***

Goals of Network Layer

- ❖ Enable low-cost, low-power embedded networking.
 - “Low Cost” basically means low memory footprint.
 - “Low Power” means low radio power as well as long battery life.
- ❖ Support a wide variety of technical requirement and design tradeoffs.
 - Battery life vs. throughput/latency.
 - Latency vs. spatial coverage.
- ❖ Support stack profile-driven modularity.

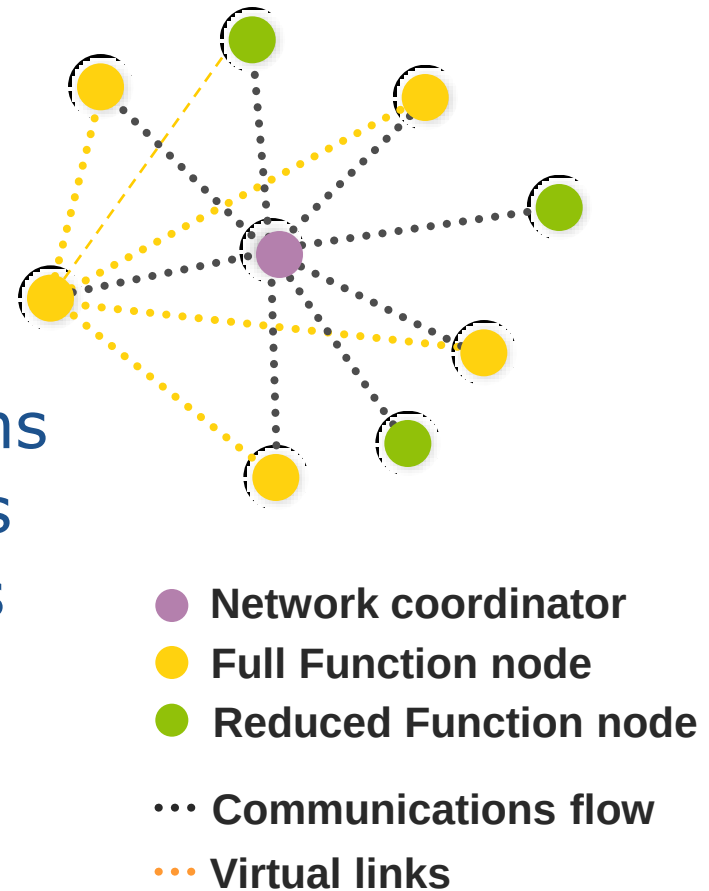
ZigBee Device Types

- ❖ ZigBee Coordinator (ZC)
 - One and only one required for each ZB network.
 - Initiates network formation.
 - Acts as 802.15.4 PAN coordinator (FFD).
 - May act as router once network is formed.
- ❖ ZigBee Router (ZR)
 - Optional network component.
 - May associate with ZC or with previously associated ZR.
 - Acts as 802.15.4 coordinator (FFD).
 - Participates in multihop routing of messages.
- ❖ ZigBee End Device (ZED)
 - Optional network component.
 - Shall not allow association.
 - Shall not participate in routing.

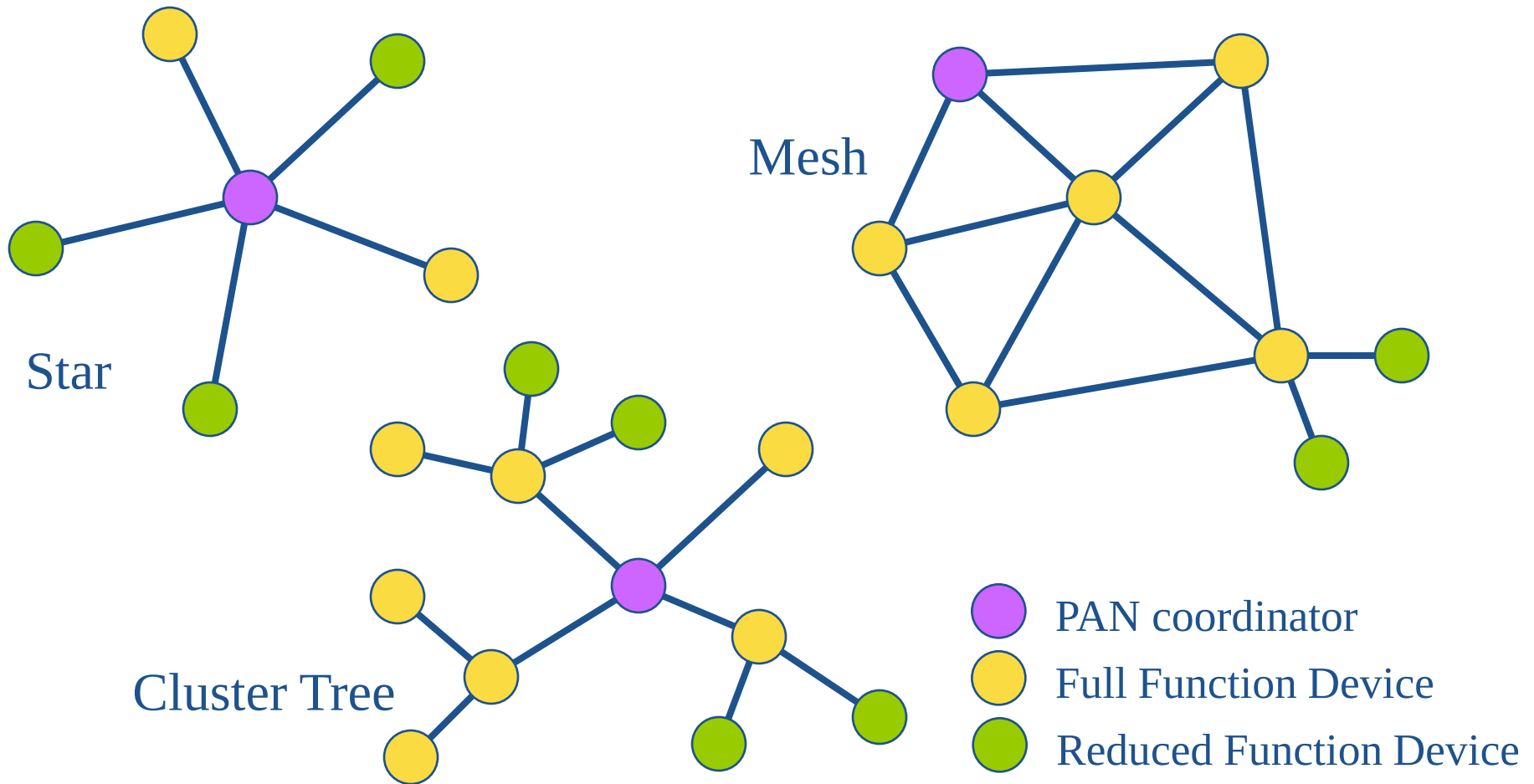
Basic Network Characteristics

- 65,536 network (client) nodes
- Optimized for timing-critical applications and power management
 - Time to Join Network: $\sim 500\text{ms}$
 - Sleeping to active: $< 15\text{ms}$
 - Channel access time: $< 15\text{ms}$

- Full Mesh Networking Support



ZigBee Network Topologies



Address assignment

- ❖ When a device joins the network, it is given a 16-bit short address (network address).
- ❖ Such address is a unique address in the ZigBee network.
- ❖ Two distributed addressing schemes are available in ZigBee Network
 - Tree Address Assignment Scheme
 - Stochastic Address Assignment Scheme.

Tree Address Assignment Scheme

- ❖ Design to provide every potential parent with a finite sub-block of network addresses

$$CSkip(d) = \begin{cases} 1 + C_m \cdot (L_m - d - 1), & \text{if } R_m = 1 \\ \frac{1 + C_m - R_m - C_m \cdot R_m^{L_m - d - 1}}{1 - R_m}, & \text{otherwise} \end{cases}$$

$CSkip(d)$, essentially the size of the address sub-block being distributed by each parent at that depth to its router-capable child devices for a given network depth

C_m : maximum number of children a parent may have

L_m : the maximum depth in the network

R_m : the maximum number of routers a parent may have as children

Tree Address Assignment Scheme

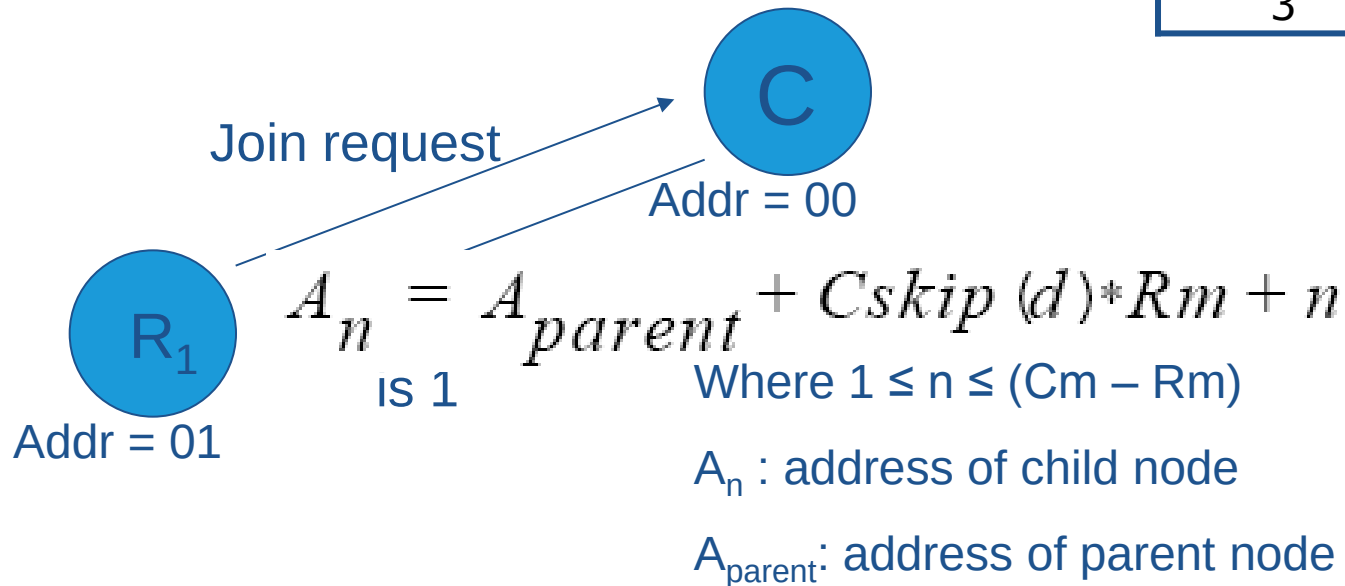
- ❖ Network addresses shall be assigned to end devices in a sequential manner with the n th address, A_n , given by

$$A_n = A_{parent} + Cskip(d) \cdot Rm + n$$

Example of Tree Address Assignment

When allowing a node to join, the coordinator assigns a 16-bit short address to new nodes. The address is calculated by the following formula

Tree level , d	CSkip(d)
0	31
1	7
2	1
3	0



If a new node joins into this network with the same level as R_1 , coordinator assigns the address as

$$A_2 = 0 + 31 + 1$$

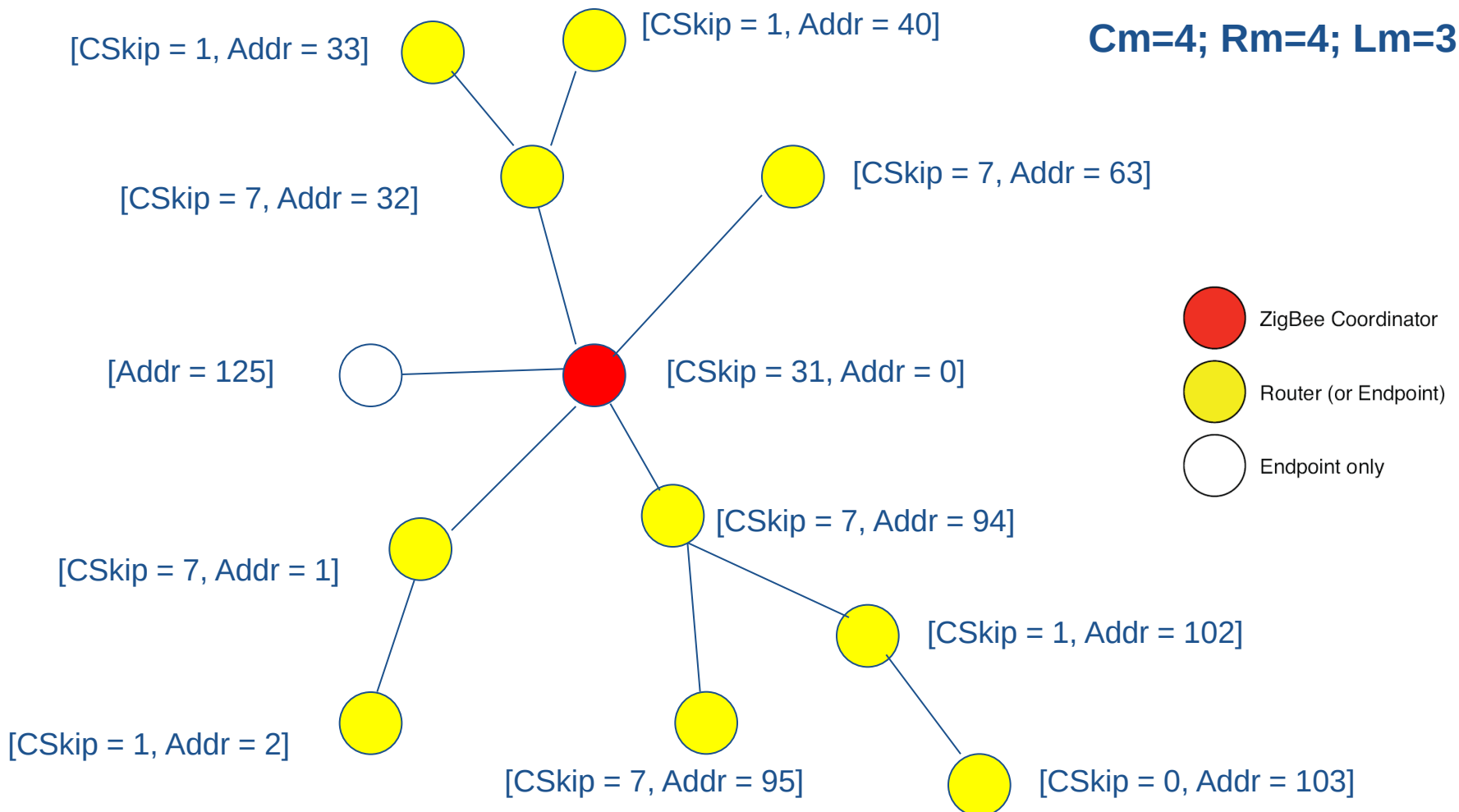
Tree level , d	CSkip(d)
0	31
1	7
2	1
3	0



Example

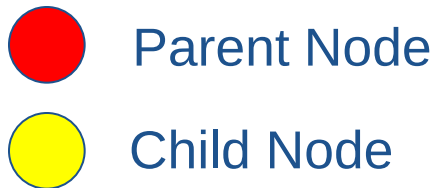
Setting:

Cm=4; Rm=4; Lm=3



Stochastic Address Assignment Mechanism

❖ Network addresses shall be chosen at random



Stochastic Address Assignment Scheme

❖ Advantage

- No 16-bit short address would be wasted

❖ Disadvantage

- The probability of duplicate short address increase when the number of nodes increase in the same network

Routing Algorithm in ZigBee

- ❖ ZigBee network could contain 65,536 network (client) nodes
- ❖ Multi-hop communication is very often in ZigBee network
- ❖ Therefore, routing is required

Basic knowledge of Routing protocol

- ❖ Routing Cost – a link cost associates with each link in the path
- ❖ Routing table - an electronic table (file) or database stores the routes to particular network destinations (node)

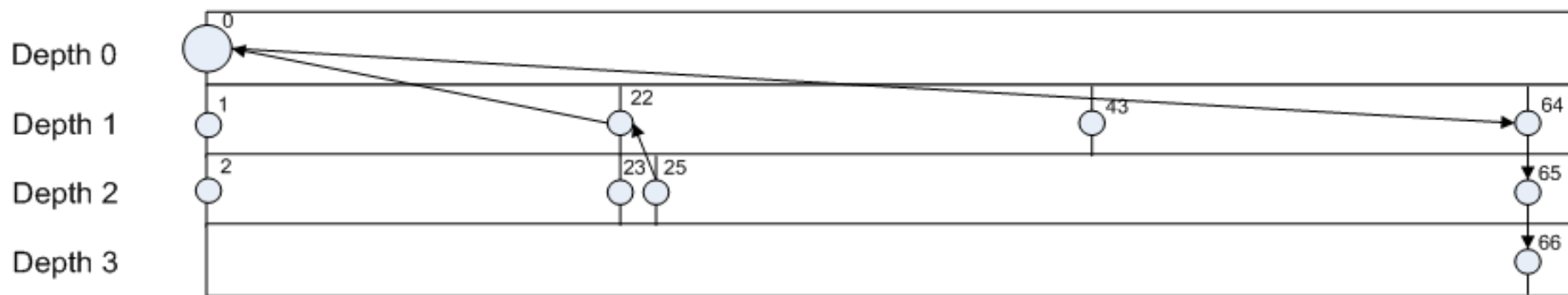
Routing Algorithm in ZigBee

- ❖ ZigBee provides two different routing algorithms
 - Tree Routing (Hierarchical Routing)
 - Mesh Network Routing (Table driven routing)

Tree Routing

- ❖ Simple and less resource requirement routing method
- ❖ based on the tree address assignment mechanism,
- ❖ Example: Node 25 sends a message to Node 66

Address

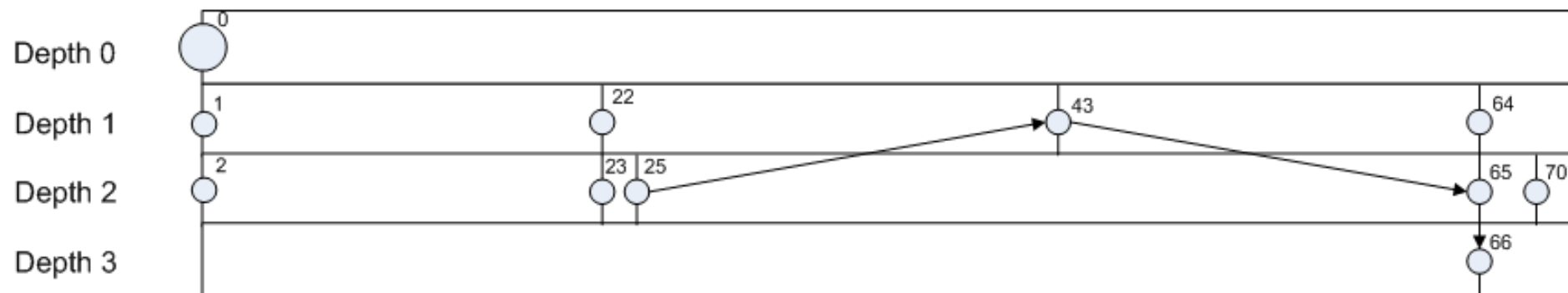


Obviously not necessarily the most efficient route

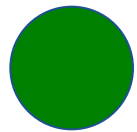
Mesh Network Routing

- ❖ Routes are established on-demand using a route discovery process in which the originating device broadcasts a route request command and the destination device sends back a route reply
- ❖ Find the path with the minimum routing cost
- ❖ Example: Node 25 sends a message to Node 66

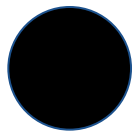
Address



Mobile Routing



Wireless Router



Destination (Lamp)

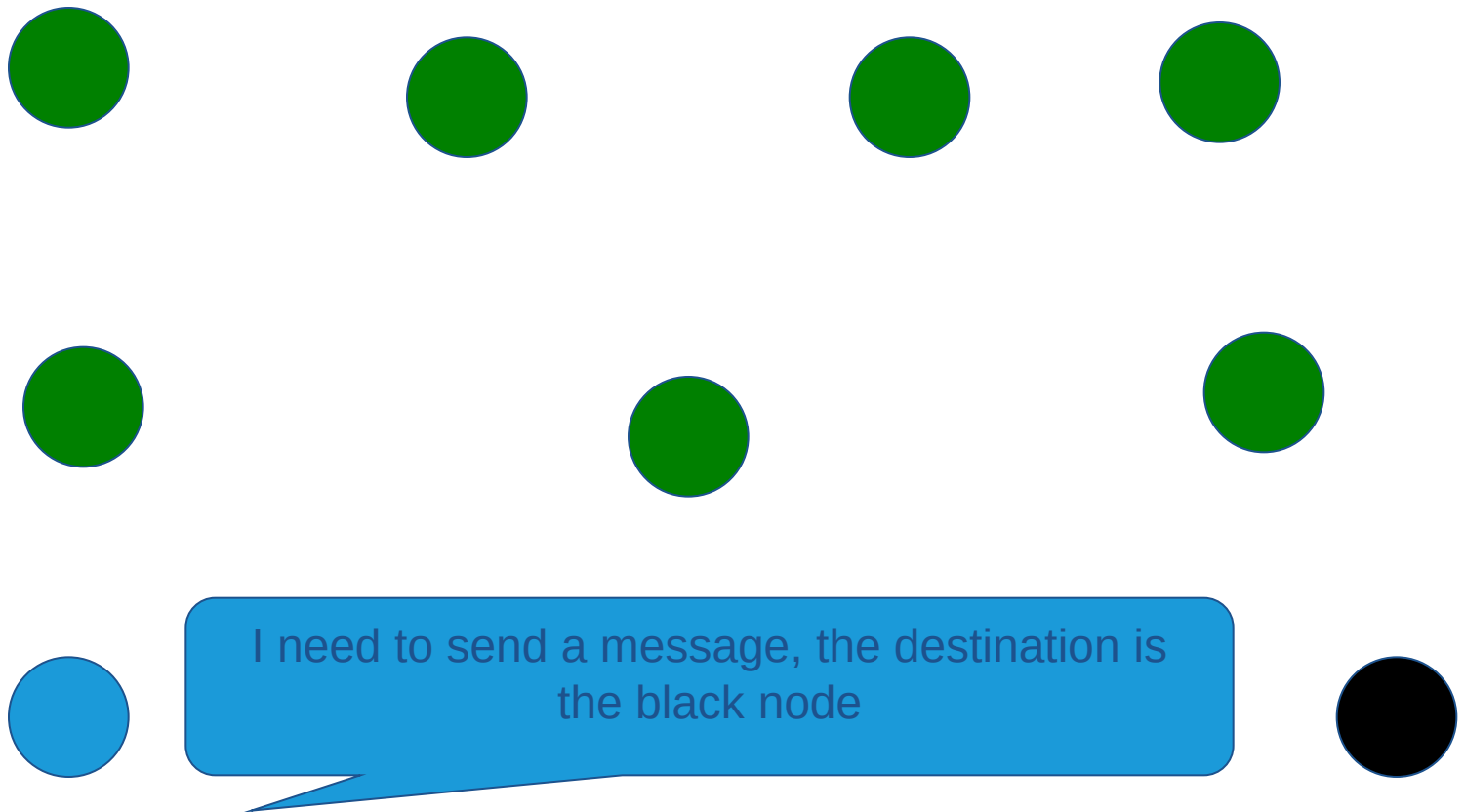


Source (Switch)

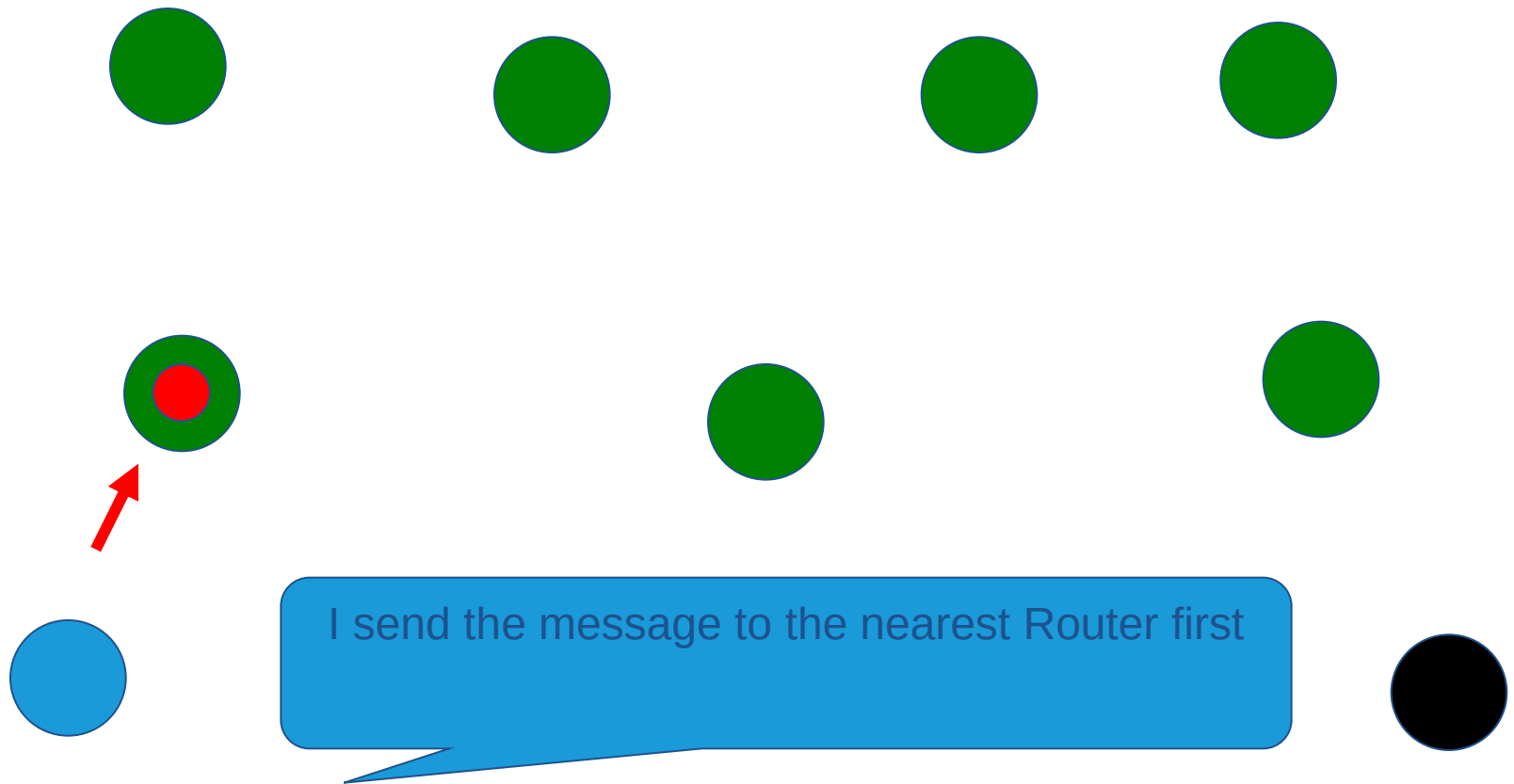
Assumption:

The link cost between each node is the same

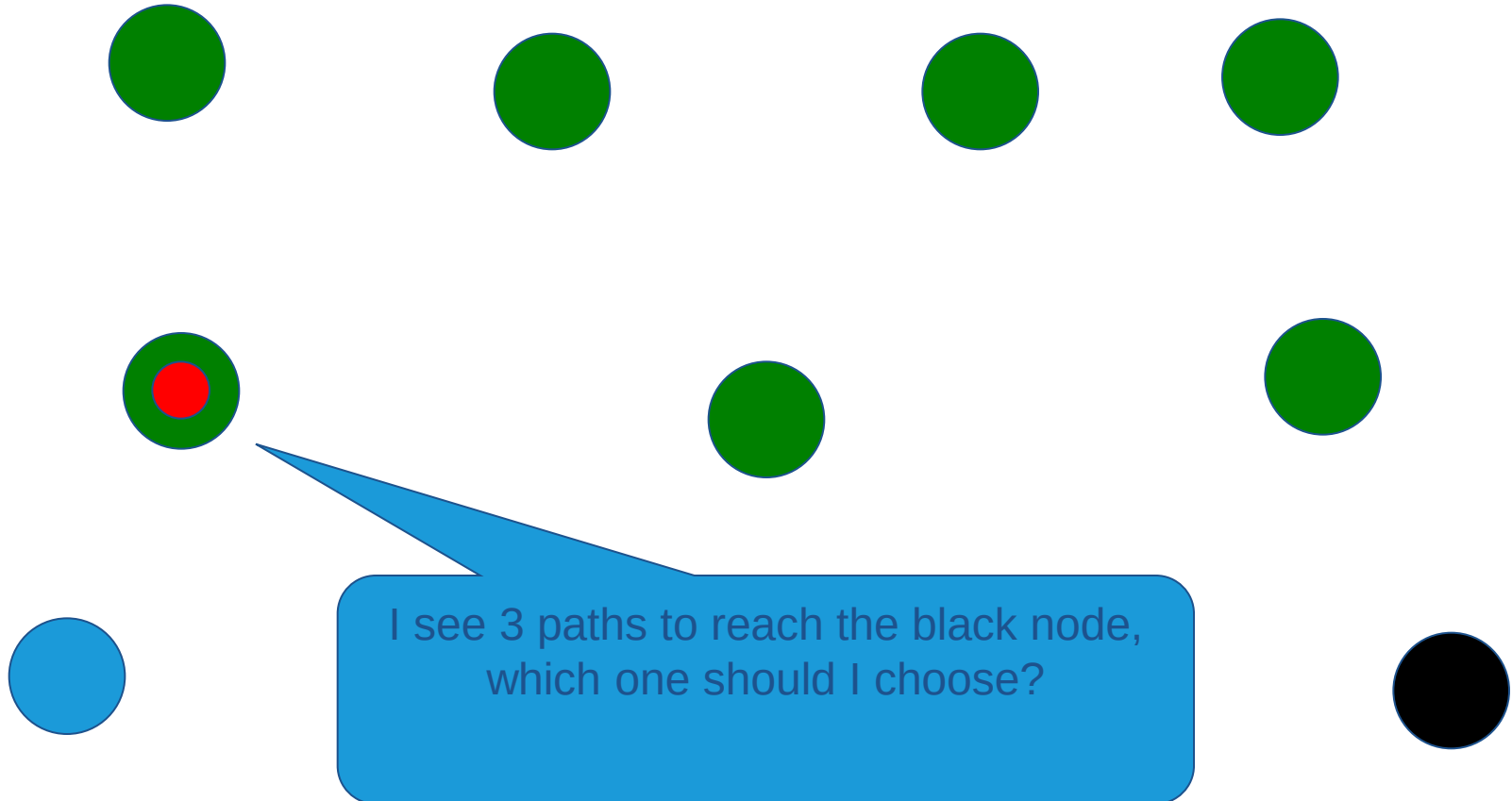
Reliability: Mesh Networking



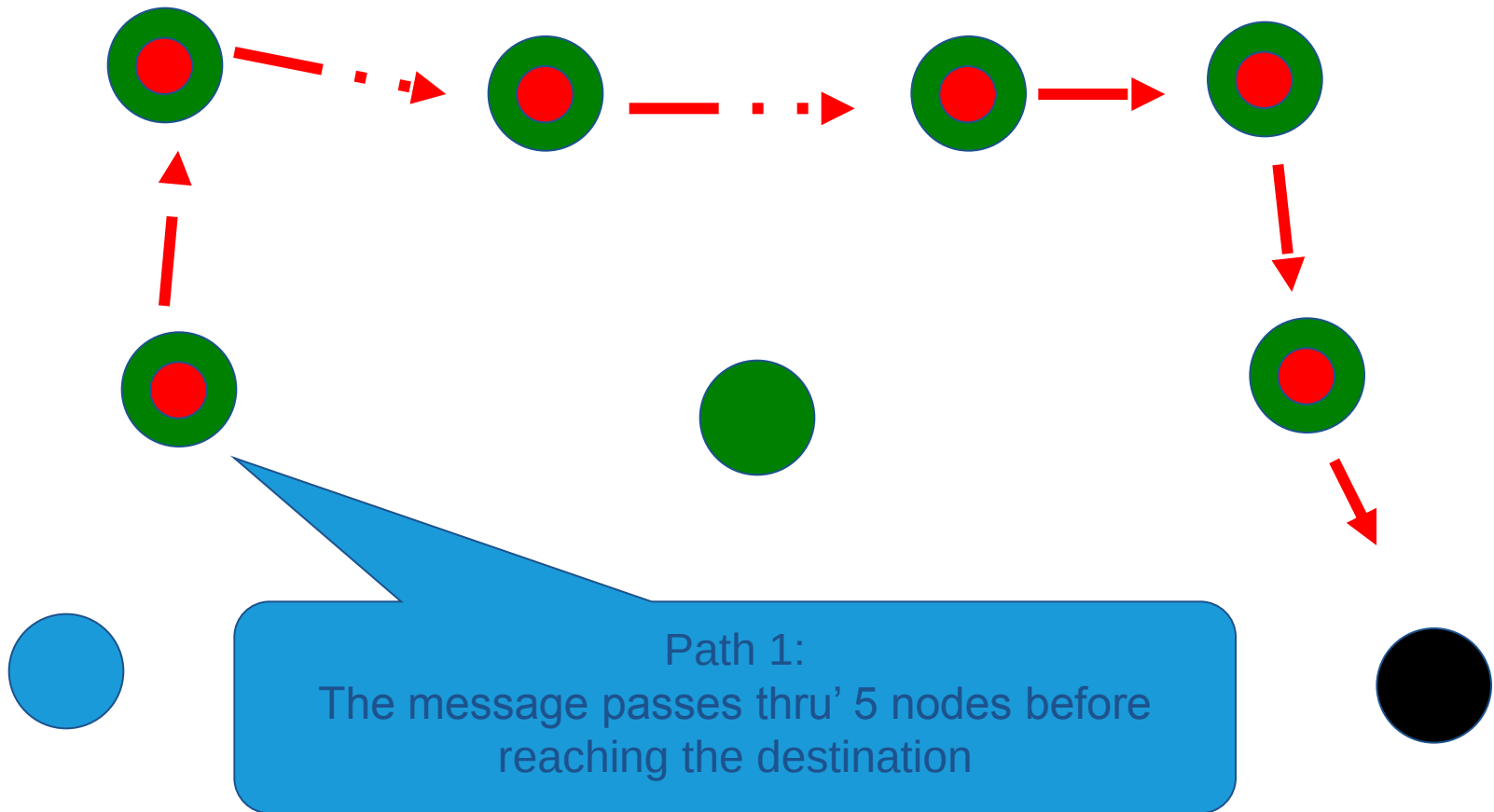
Reliability: Mesh Networking



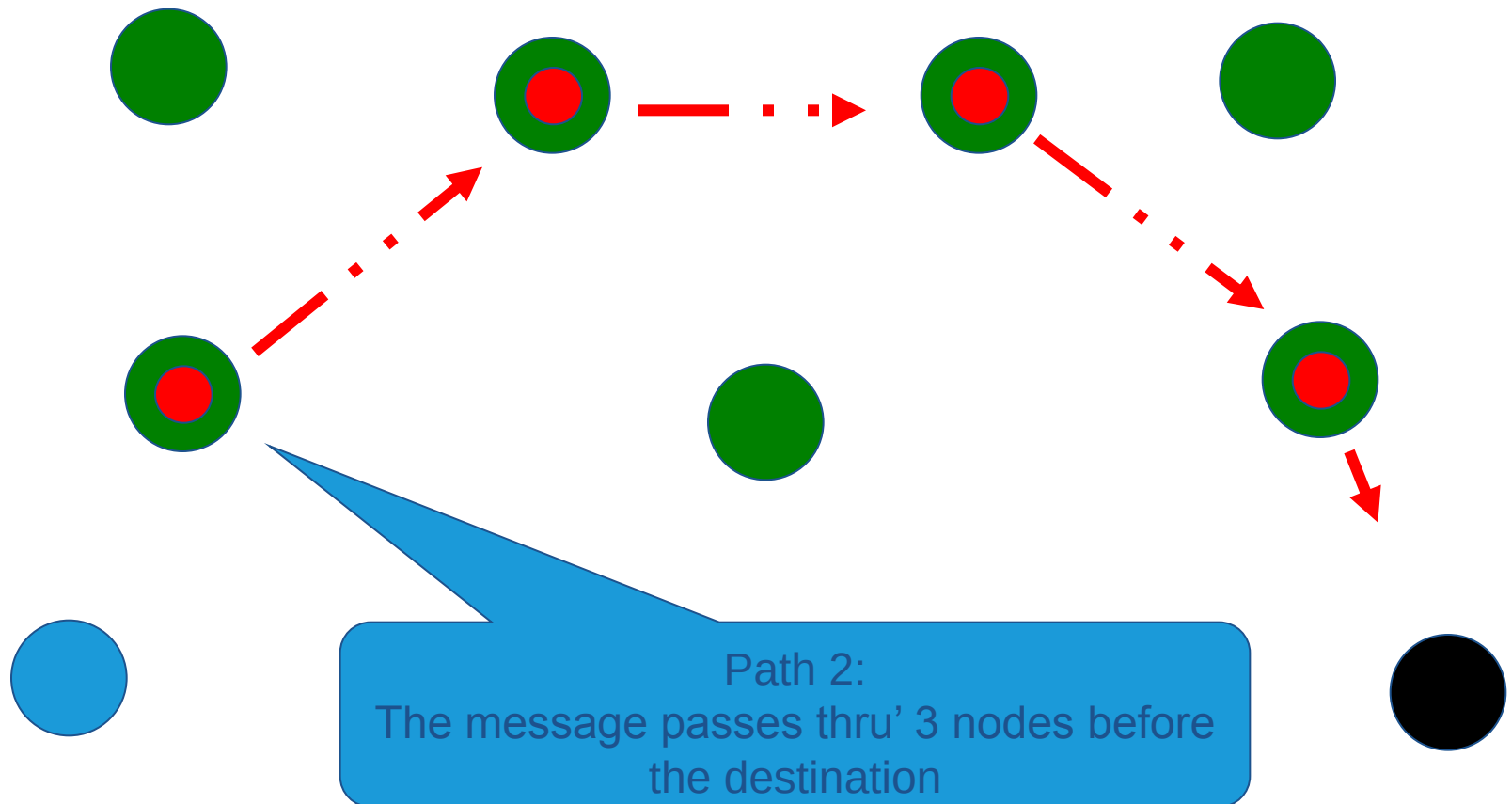
Reliability: Mesh Networking



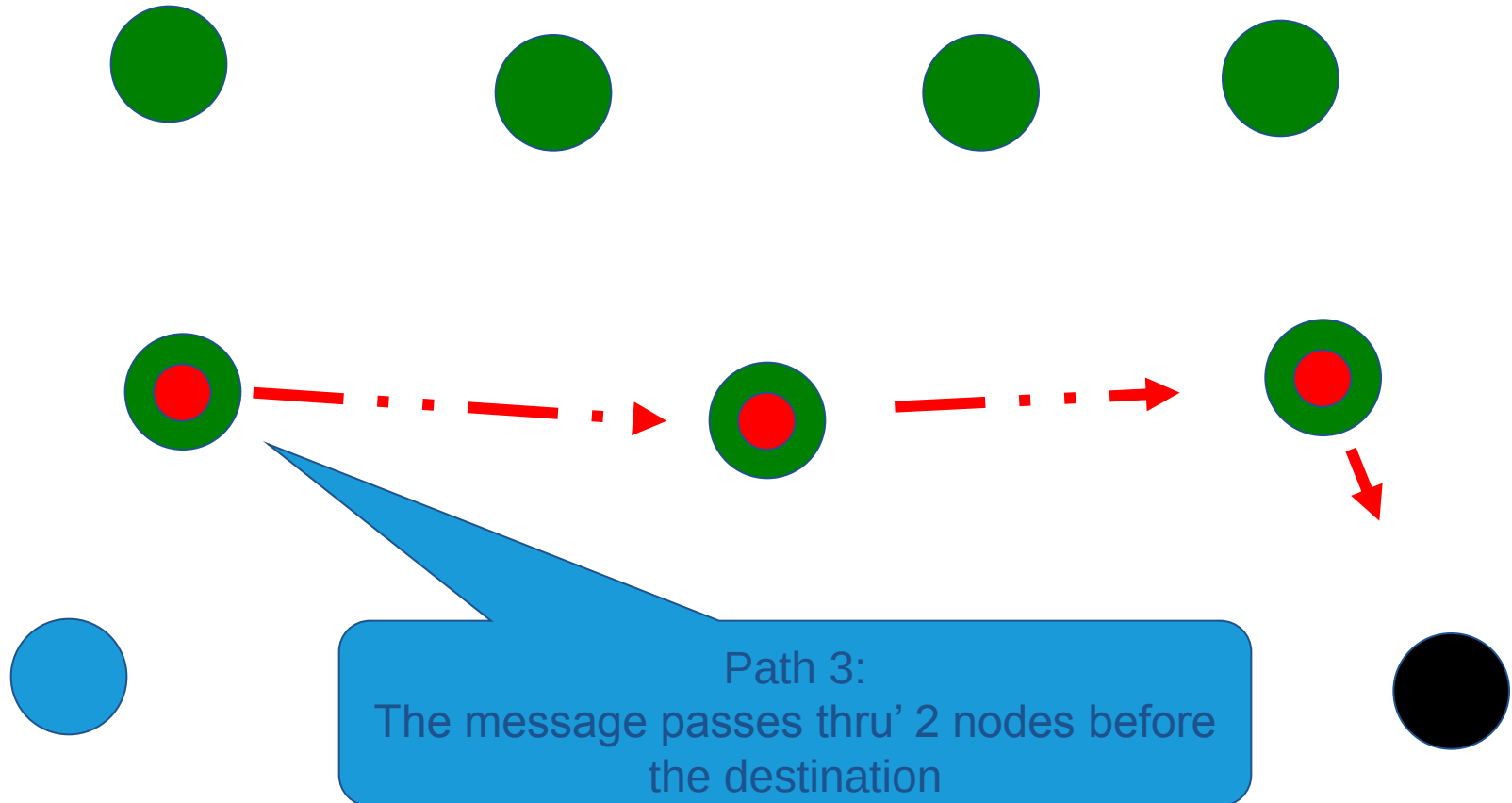
Reliability: Mesh Networking



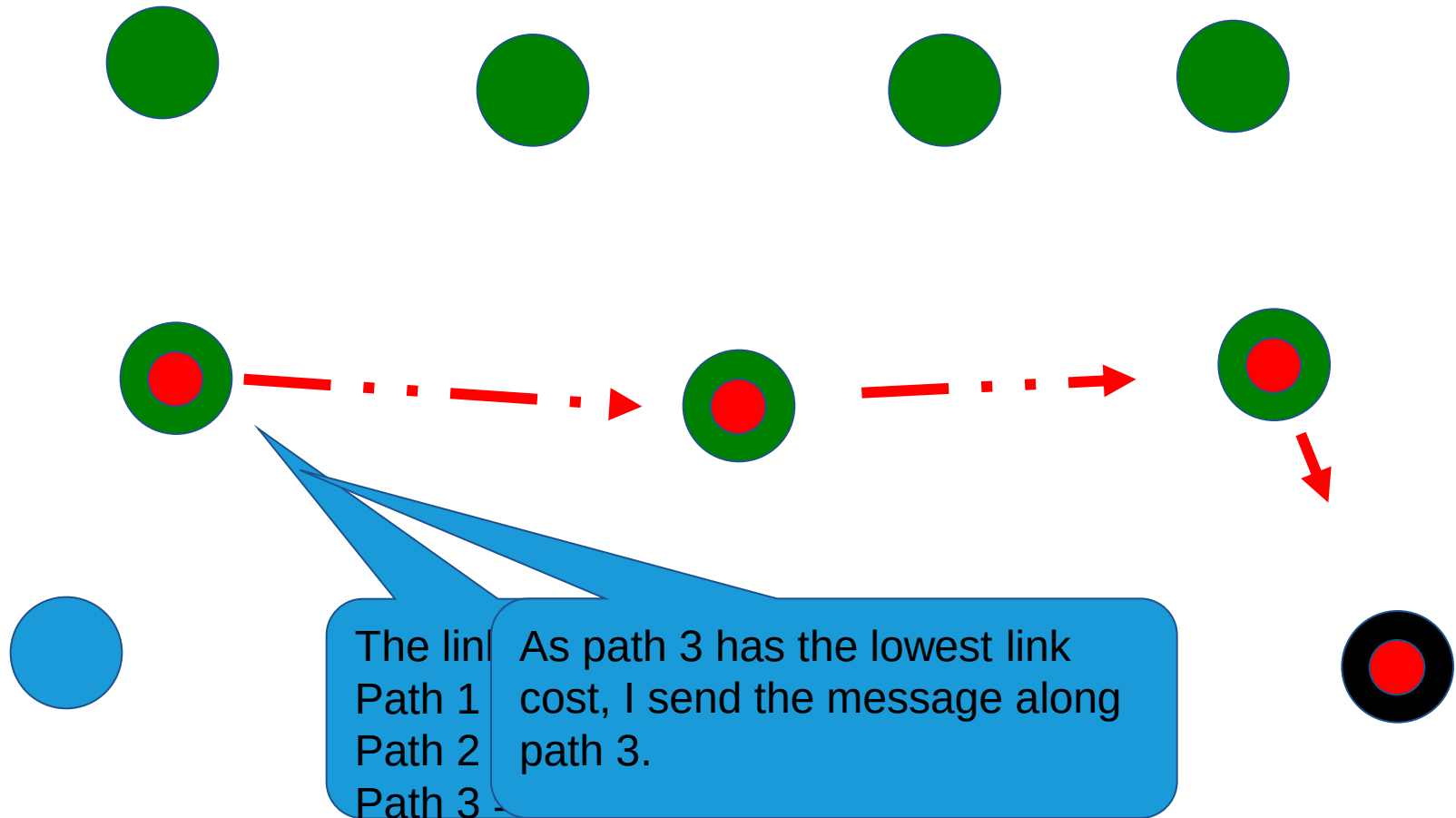
Reliability: Mesh Networking



Reliability: Mesh Networking



Reliability: Mesh Networking



- ❖ ZigBee provides an open standard platform for application development
- ❖ ZigBee is a reliable protocol, supporting a large number of nodes

END