ZigBee

- Specification for a suite of high-level communication protocols used to create personal area networks (WPAN) built from small, low-power digital radios.
- Based on IEEE 802.15.4 standard.
- Though its low power consumption limits transmission distances to 10–100 meters, ZigBee devices can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones (multi-hop).

ZigBee

- ZigBee is typically used in low data rate applications that require long battery life and secure networking (support 128 bit encryption): home automation, healthcare, industrial control applications with short range and low bitrate.
- ZigBee has a defined rate of 250 Kbit/s, best suited for intermittent data transmissions from a sensor or input device.
- ZigBee uses the 2.4 GHz ISM frequency band and has 16 channels.
- Multi-level security (supports AES-128 security).
- Addressing space of up to 64 bit IEEE address devices.

ZigBee

The Xbee shield allows an Arduino board to communicate wirelessly using ZigBee.

The module can communicate up to 30 meters indoors or 100 meters outdoors (with line-of-sight).

It can be used as a serial/USB replacement, or you can put it into a command mode and configure it for a variety of broadcast and mesh networking options.

ZigBee – Characteristics

- Low cost
- Low power consumption
- Low data rate
- Relatively short transmissions range
- Scalability
- Reliability
- Flexible protocol design suitable for many applications

ZigBee – Device types

Uses notion of "logical devices" in a Personal Area Network (PAN):

ZigBee Coordinator Only one coordinator exists in each ZigBee PAN. Its function is to store information about the network and to determine the optimum transmission path between any two points of the network.

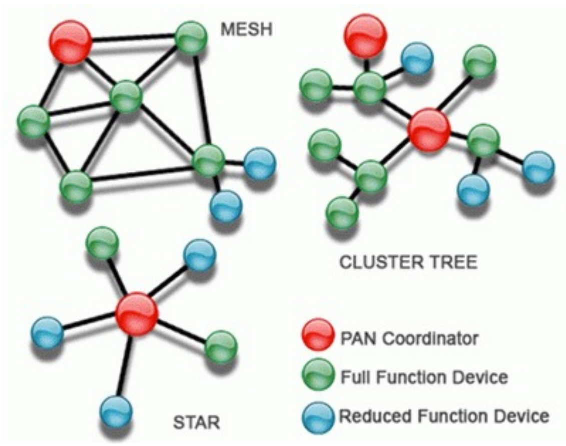
- Is responsible for initializing, maintaining and managing the network.

ZigBee Route (Full function device), for controlling the message routing between nodes (Router, Repeater). Act as an intermediate repeater that passes data from other devices.

ZigBee end-device, acts has the end point of the network. Also called Reduced Function Device. This device contains a minimal amount of functionality to enable it to talk to its parent node (either the coordinator or a router); it cannot relay data directly from other devices.

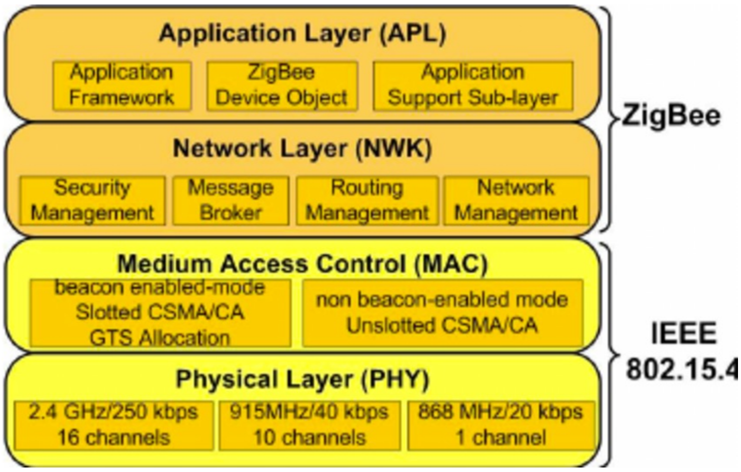
54

ZigBee - topologies



55

ZigBee Layers



SMCU 2021/2022 56

56

ZigBee vs Bluetooth

Bluetooth targets medium data rate continuous duty

- 1 Mbps.
- Larger packets over small network.
- File transfer, streaming telecom radio.
- Ad-hoc networks.

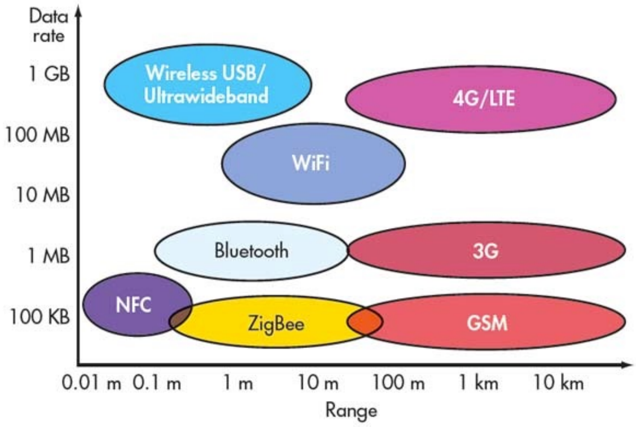
ZigBee targets low data rate, low duty cycle

- 250 Kbps (60-115 Kbps typical data transfer).
- Smaller packets over large network.
- More sophisticates networking, mostly static networks with many infrequently used devices .
- Long battery life (weeks to months).

SMCU 2021/2022 57

57

ZigBee vs Bluetooth



Wireless - Compare

Name	Bluetooth Classic	Bluetooth 4.0 Low Energy (BLE)	ZigBee	WiFi
IEEE Standard	802.15.1	802.15.1	802.15.4	802.11 (a, b, g, n)
Frequency (GHz)	2.4	2.4	0.868, 0.915, 2.4	2.4 and 5
Maximum raw bit rate (Mbps)	1-3	1	0.250	11 (b), 54 (g), 600 (n)
Typical data throughput (Mbps)	0.7-2.1	0.27	0.2	7 (b), 25 (g), 150 (n)
Maximum (Outdoor) Range (Meters)	10 (class 2), 100 (class 1)	50	10-100	100-250
Relative Power Consumption	Medium	Very low	Very low	High
Example Battery Life	Days	Months to years	Months to years	Hours
Network Size	7	Undefined	64,000+	255

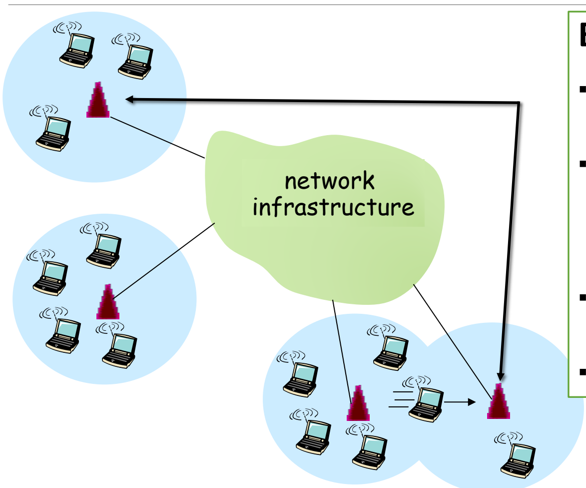
https://learn.sparkfun.com/tutorials/bluetooth-basics

Core Issues

Handoff of mobile devices

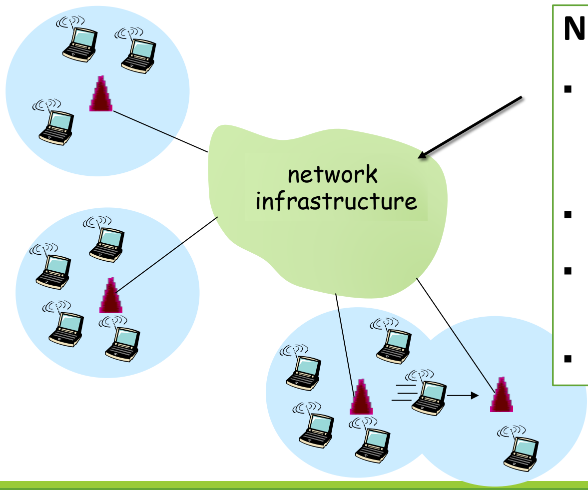
Communication over wireless links
- Medium Access Control (MAC)
- Ad-hoc Routing

Wireless Network: Infrastructure Mode



Base station
- Typically connected to wired network
- Relay responsible for sending packets between wired network and wireless host(s) in its “area”
- E.g., cell towers, WiFi access points
- May support “roaming”

Wireless Network



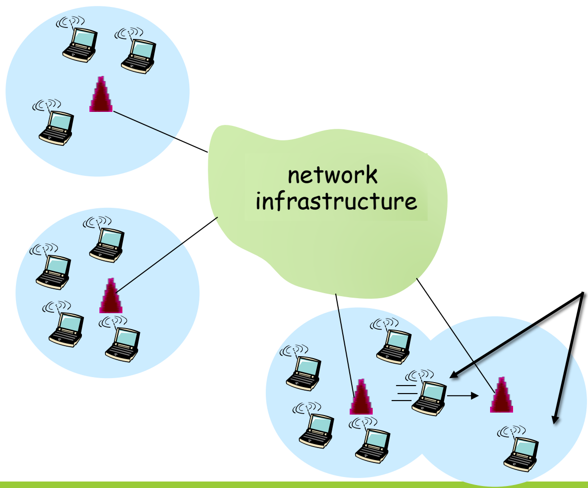
Network infrastructure

- Larger network with which a wireless host wants to communicate
- Typically a wired network
- Provides traditional network services
- May not always exist

SMCU 2021/2022 62

62

Wireless Network



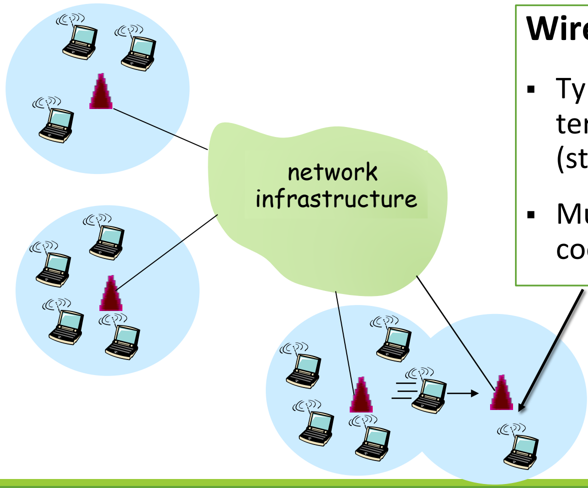
Wireless terminal

- Laptop, tablet, phone
- Run applications
- May be stationary (non-mobile) or mobile

SMCU 2021/2022 63

63

Wireless Network



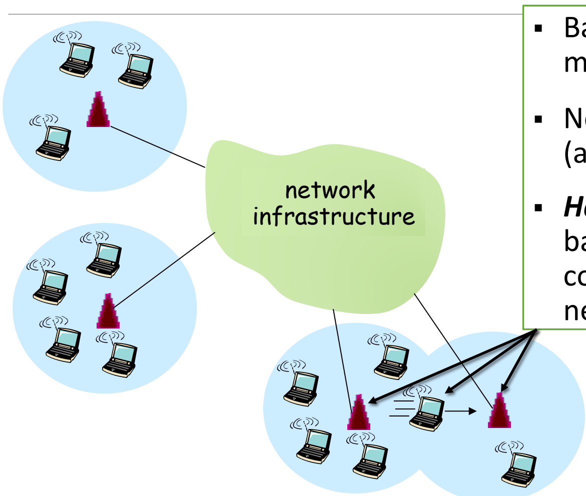
Wireless link

- Typically used to connect terminal(s) to base station (star topology)
- Multiple access protocols coordinate link access

SMCU 2021/2022 64

64

Wireless Network: Infrastructure Mode



- Base station connects mobiles into wired network
- Network provides services (addressing, routing, DNS)
- ***Handoff***: mobile changes base stations providing connection to wired network

SMCU 2021/2022 65

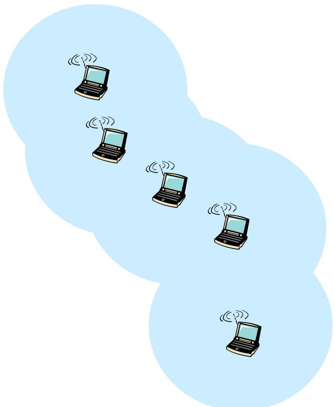
65

Handoff Categories

Sr No.	Hard Hand-off	Soft Hand-off
1	The definition of a hard-hand off is one where an existing connection must be broken when the new one is established	Soft hand-off is defined as a hand-off where a new connection is established before old one is released
2	It allocates Different frequency	It allocates same frequency
3	Hard hand-off typically used in TDMA and FDMA	Soft hand-off used in CDMA and some TDMA systems
4	Hard hand-off is not very complicated	More complex than hard hand-off
5	In hard hand-off handset always communicated with one BS at a time	Communicate up to three or four radio link at the same time

66

Wireless Network: Ad Hoc Networks



- No base stations
- Nodes can only transmit to other nodes within link coverage
- Nodes self-organize and route among themselves

67

Wireless Networks: Infrastructure vs. Ad Hoc

Infrastructure mode
- wireless hosts are associated with a base station
- traditional services provided by the connected network
  - e.g., address assignment, routing, and DNS resolution

Ad-hoc networks
- wireless hosts interact in a P2P fashion
- hosts themselves must provide network services
- and perform multi-hop routing (more later)

Types of Wireless Networks

	Infrastructure-based	Infrastructure-less
Single hop	Base station connected to larger wired network (e.g., WiFi wireless LAN, and cellular telephony networks)	No wired network; one node coordinates the transmissions of the others (e.g., Bluetooth, and ad hoc 802.11 – WiFi direct)
Multi-hop	Base station exists, but some nodes must relay through other nodes (e.g., wireless sensor networks, and wireless mesh networks	No base station exists, and some nodes must relay through others (e.g., mobile ad hoc networks, like vehicular ad hoc networks)

Wireless Communication

- Shared medium, limited spectrum
- Unlike wired links, which can be shielded and can use multiple wires to segregate sending and receiving

Wireless Links

Ability to decode a signal is governed by the **signal to noise ratio** (SNR)

In wireless links SNR degrades with:

- Decreased signal strength
- Interference from other sources
- Multipath propagation

The result is higher and variable bit error rates (BER), when compared to wired channels

Wireless Links

Signal strength

Decreases with distance
- same power/energy spread over larger area

Is attenuated by obstacles
- signal energy is absorbed by matter

Wireless Links

Interference from other sources

Is received as noise

Spectrum (frequency) may be shared by different standards/technologies
- eg. WiFi, Bluetooth, ZigBee

Many devices generate electromagnetic noise
- eg. motors, lamps, transformers, CPUs, microwave ovens

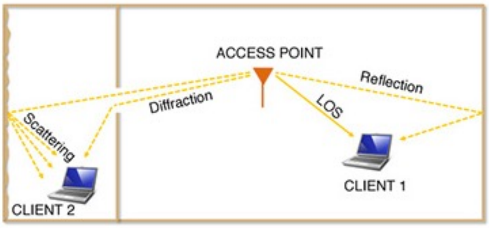
Wireless Links

Multipath propagation

The mechanisms of propagation in the context of an indoor wireless local area network.

Client 1: The LOS path is unobstructed, but it also receives weaker signals as a result of a reflection off of a wall.

Client 2: The LOS path is obstructed, it receives signals through diffraction in the doorway and also scattering off of a rough wall.

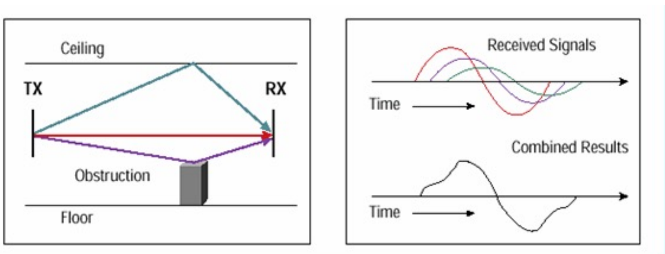


74

Wireless Links

Multipath propagation

Radio signals reflects off objects and ground, arriving at the receptor at different times/phases leading to self-interference



http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html

75

Wireless Links: Multipath effects

- Rapid changes in signal amplitude over a small distance or time interval.
- Rapid changes in signal phase over a small distance or time interval.
- Time dispersion (echoes) caused by multipath propagation delay.

Wireless Links

The higher the SNR, the lower the BER.

Strategies for improving Signal to Noise Ratio (SNR) to reduce Bit Error Rates (BER):

- increase radio power/radio sensitivity
- use different antenna(s)
- coordinate senders to avoid concurrent access

Wireless Links

Investing more power/energy in transmissions
- can improve reception, but creates stronger interference with other senders
- drains batteries faster

78

Wireless Links

Dynamic selection of the physical-layer modulation technique can be used to adapt the modulation technique to channel conditions.

The SNR (and hence the BER) may change as a result of mobility or due to changes in the environment. Adaptive modulation and coding are used in cellular data systems and in the 802.11 WiFi and cellular data networks.

This allows, for example, the selection of a modulation technique that provides the highest transmission rate possible subject to a constraint on the BER, for given channel characteristics.

79

Wireless Links: Access Coordination

Coordinate access to broadcast medium

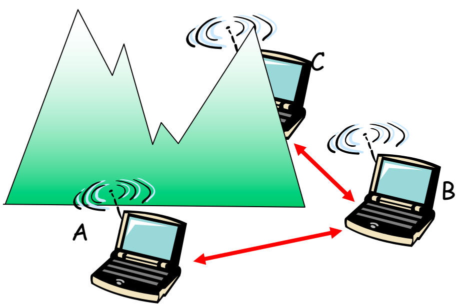
- **goal**: avoid concurrent access to transmission medium to minimize collisions and corrupted frames due to interference

Broadcasting simplifies coordination but, in wireless links it is not guaranteed everybody can hear everybody

- hidden terminal problem
- fading over distance

Wireless: Problems

Hidden terminal problem

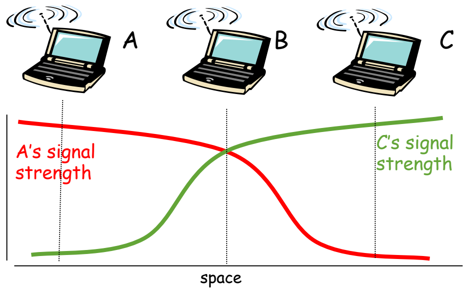


A and B hear each other
B and C hear each other
A and C **do not**

A and C are unaware of their interference at B.

Wireless : Problems

Fading over distance



A and B hear each other
B and C hear each other
A and C **do not**

A and C are unaware of their interference at B.

Access Protocols

- Medium Access Control Protocol
  - Contention–Free Protocols
    - Fixed Assignment
      - FDMA
      - TDMA
      - CDMA
    - Dynamic Assignment
      - Polling
      - Token Passing
      - Reservation–Based
  - Contention–Based Protocols
    - ALOHA
    - CSMA
    - MACA
    - MACAW

Wireless Communication

Hosts communicating over a shared medium => protocol is needed so that the signals sent by multiple senders do not interfere at the receivers.

Multiplexing channel access, for allowing multiple devices to communicate at the same time, anytime

- FDMA (Frequency division multiple access) – partitions the frequency domain
- TDMA (Time-division multiple access) – partitions the time domain
- CDMA (Code-division multiple access) – uses different data "encodings"

- http://www.electronicdesign.com/communications/fundamentals-communications-access-technologies-fdma-tdma-cdma-ofdma-and-sdma

Wireless Communication

FDMA (Frequency Division Multiple Access)

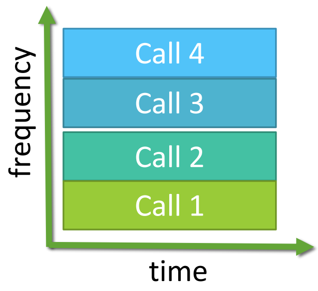
- The frequency band is divided into several smaller frequency bands.
- The data transfer between a pair of nodes uses one frequency band.
- All other nodes use a different frequency band.

Wireless Communication

FDMA – frequency division multiple access

Divides available spectrum into several carrier frequency channels

Each device is assigned its own carrier frequency



86

Wireless Communication

TDMA (Time Division Multiple Access)

- Multiple devices to use the same frequency band.
- Relies on periodic time windows (frames)
  - frames consist of a fixed number of transmission slots to separate the medium accesses of different devices
  - a time schedule indicates which node may transmit data during a certain slot

87

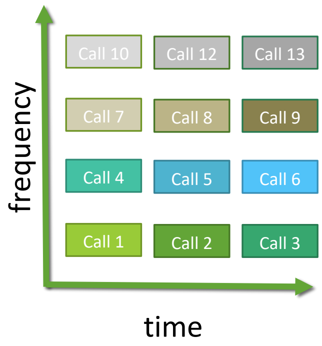
Wireless Communication

TDMA – time division multiple access

Enhances FDMA, dividing spectrum further into a series of time slots

each device is assigned a periodic time slot

- e.g.: GSM is FDMA + TDMA



88

Wireless Communication

CDMA (Code Division Multiple Access)

- Simultaneous accesses of the wireless medium are supported using different codes.
- If these codes are orthogonal, it is possible for multiple communications to share the same frequency band.
- Forward Error Correction (FEC) at the receiver is used to recover from interferences among these simultaneous communication.

89

Wireless communication

CDMA – Code Division Multiple Access

Employs spread-spectrum technology and a special coding scheme

- the data to be transmitted is combined with a code assigned to each call/connection.

analogy: it is as if different devices talked different languages

SMCU 2021/2022 90

90

Wireless communication

CDMA – Code Division Multiple Access

All stations share same frequency

Each station is assigned a “chipping” sequence (code) to encode data

Stations “coexist” and transmit simultaneously with minimal interference, provided codes are unique and “orthogonal”

CDMA is used in several wireless standards (cellular, satellite, etc.)

SMCU 2021/2022 91

91

Carrier Sense, Multiple Access – (CSMA)

Contention-based protocol

Avoid collisions when 2 or more nodes transmit at same time. Base idea:

- sense before transmitting
- don't collide with ongoing transmission by another node (wait for idle)

CSMA with Collision Detection (ex. Cabled ethernet)

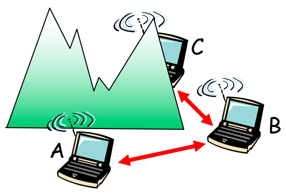
- sense collisions when transmitting
- Backoff and retry later

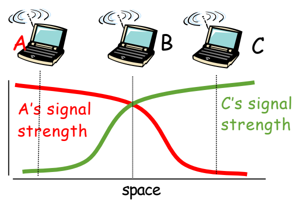
CSMA in Wireless networks

More problems in wireless networks to detect collisions:

- difficult to receive (sense collisions) when transmitting
- can't sense all collisions in any case: hidden terminal, fading
- Only receiver detect collisions

Approach: avoid collisions!





CSMA with Collision Avoidance

CSMA/CA (CSMA with Collision Avoidance)

- Nodes sense the medium, but do not immediately access the channel when it is found idle.
- A node waits for a time period called DCF[1] inter frame space (DIFS) plus a multiple of a slot size.
- In case there are multiple nodes attempting to access the medium, the one with the shorter back-off period will win.

[1] Distributed Coordination Function (DCF) is a protocol which uses carrier sensing along with a four way handshake to maximize the throughput while preventing packet collisions.

CSMA/CA

802.11 sender

1 **if** sense channel idle for **DIFS** (Distributes Inter-frame Spacing) **then**
- transmit entire frame (no CD)

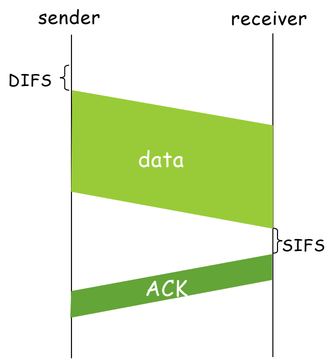
2 **if** sense channel busy **then**
- start random backoff time
- timer counts down while channel idle
- transmit when timer expires
- if no **ACK**, increase random backoff interval, repeat 2

802.11 receiver

- **if** frame received OK

return ACK after **SIFS** (Short Inter-frame Spacing)

(ACK needed due to hidden terminal problem)



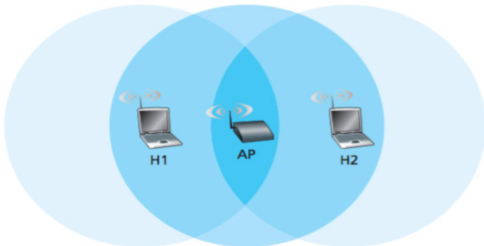
Avoiding collisions (more)

Problem:

Station H1 is transmitting a frame and halfway through H1's transmission, Station H2 wants to send a frame to the AP.

H2, not hearing the transmission from H1, will first wait a DIFS interval and then transmit the frame, resulting in a collision.

The channel will therefore be wasted during the entire period of H1's transmission as well as during H2's transmission.



Hidden terminal example: H1 is hidden from H2, and vice versa

SMCU 2021/2022 96

96

Avoiding collisions (more)

Idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

Sender first transmits small request-to-send (RTS) packets to AP using CSMA
- RTSs may still collide with each other (but they're short)

AP broadcasts clear-to-send CTS in response to RTS

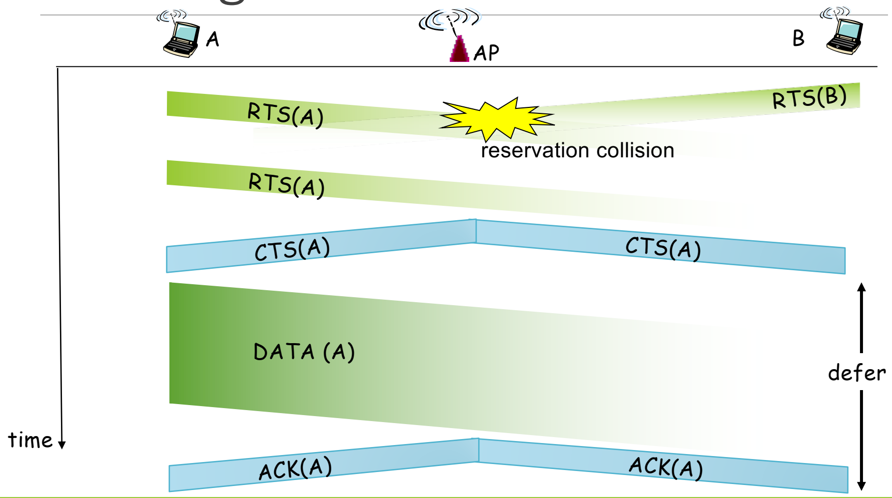
CTS heard by all nodes
- sender transmits data frame
- other stations defer transmissions

avoid data frame collisions completely using small reservation packets!

SMCU 2021/2022 97

97

Collision Avoidance: RTS-CTS exchange



98

802.11 Rate Adaptation

Different modulation techniques -> Different transmission rates

- High SNR, means user can communicate with the base station using a physical-layer modulation technique that provides high transmission rates while maintaining a low BER (Bit Error Rate).
- If BER becomes too high, some 802.11 implementations have a rate adaptation capability that adaptively selects the underlying physical-layer modulation technique to use based on current channel characteristics.
  - the transmission rate is increased until something "bad" happens

99

802.11 Power management

Power-management capabilities, to minimize the amount of time that their sense, transmit, and receive functions and other circuitry need to be "on."

- Alternate between sleep and wake states,
  - A node indicates to the access point that it will be going to sleep by setting the power-management bit (header frame).
  - Node set a timer to wake up before AP send its beacon frame (~ 100 ms)
  - Beacon frames sent out by the AP contain a list of nodes whose frames have been buffered at the AP (wakeup time ~ 250 microseconds).
  - If there are no buffered frames for the node, it can go back to sleep.
  - Otherwise the node can explicitly request that the buffered frames be sent by sending a polling message to the AP.

(A node that has no frames to send or receive can be asleep 99% of the time, resulting in a significant energy savings.)

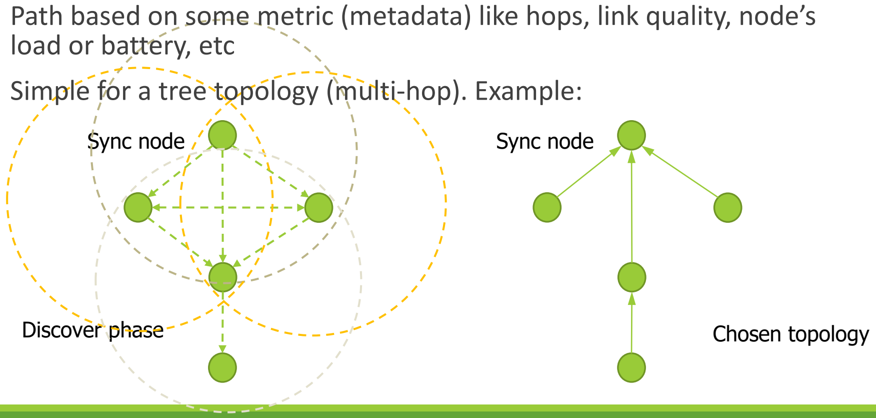
100

WSN: routing

Build routing tables based on food (broadcast to neighbors) and Bellman-Ford algorithm

Path based on some metric (metadata) like hops, link quality, node's load or battery, etc

Simple for a tree topology (multi-hop). Example:

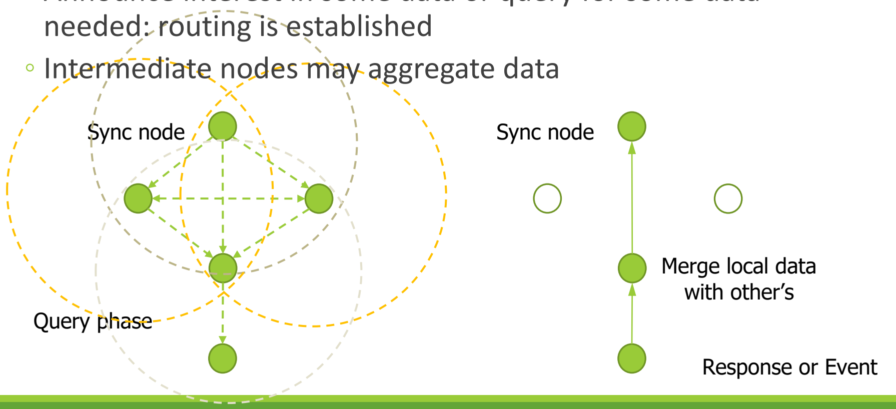


101

WSN: data center routing

Query/Event driven Example

- Announce interest in some data or query for some data needed: routing is established
- Intermediate nodes may aggregate data



SMCU 2021/2022 102

102

Bibliography

Book: Frank Adelstein, et. al. Fundamentals of Mobile and Pervasive Computing. McGraw-Hill. 2005. Chap 8 + Chap 10.

- https://www.slideshare.net/pantechsolutions/basics-of-rf
- https://en.wikipedia.org/wiki/Zigbee
- https://www.design-reuse.com/articles/5715/adaptive-frequency-hopping-for-reduced-interference-between-bluetooth-and-wireless-lan.html
- https://en.wikipedia.org/wiki/Bluetooth_Low_Energy

SMCU 2021/2022 103

103