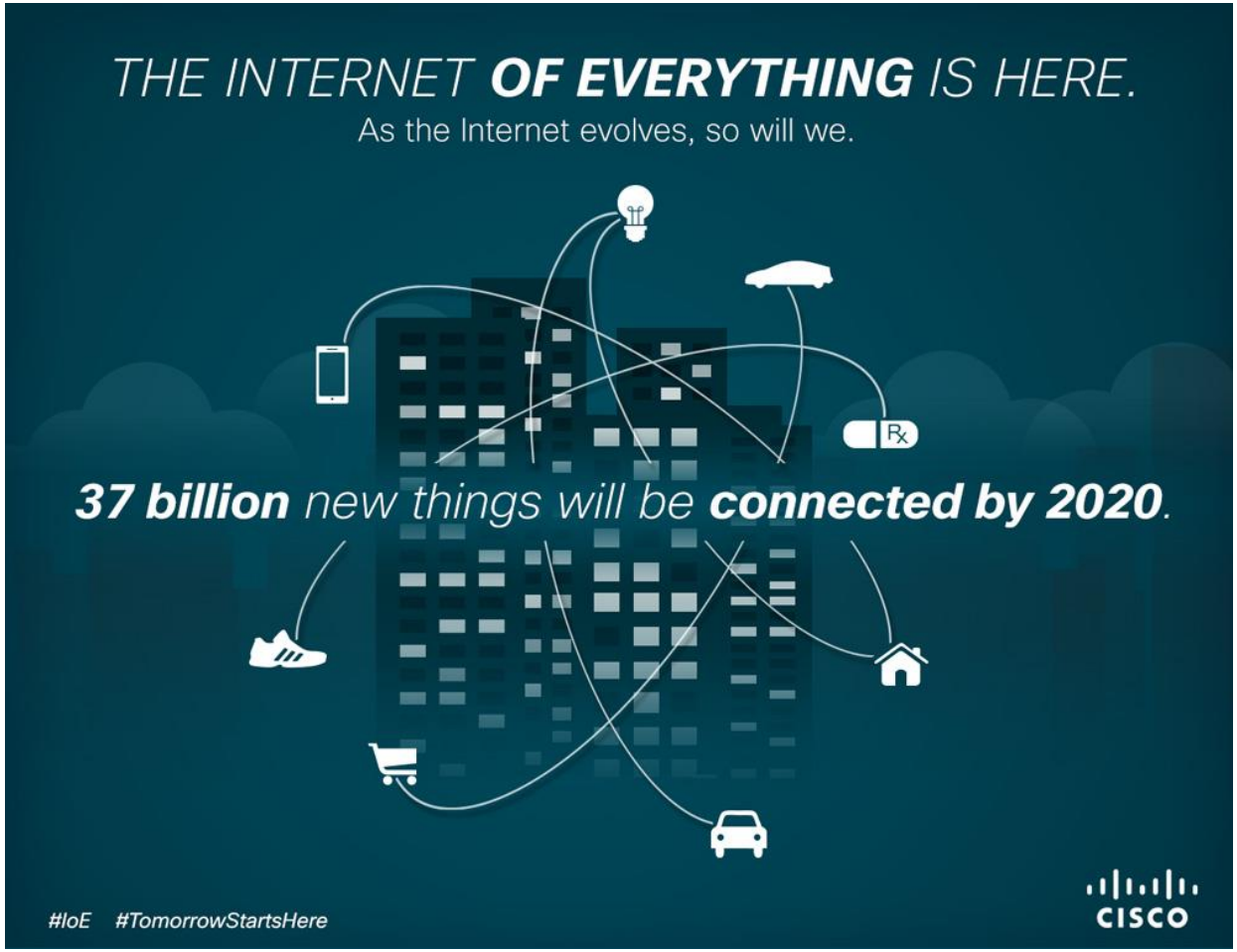
Wireless Sensor Networks

Gérard Chalhoub
Associate Professor at University of Clermont Auvergne

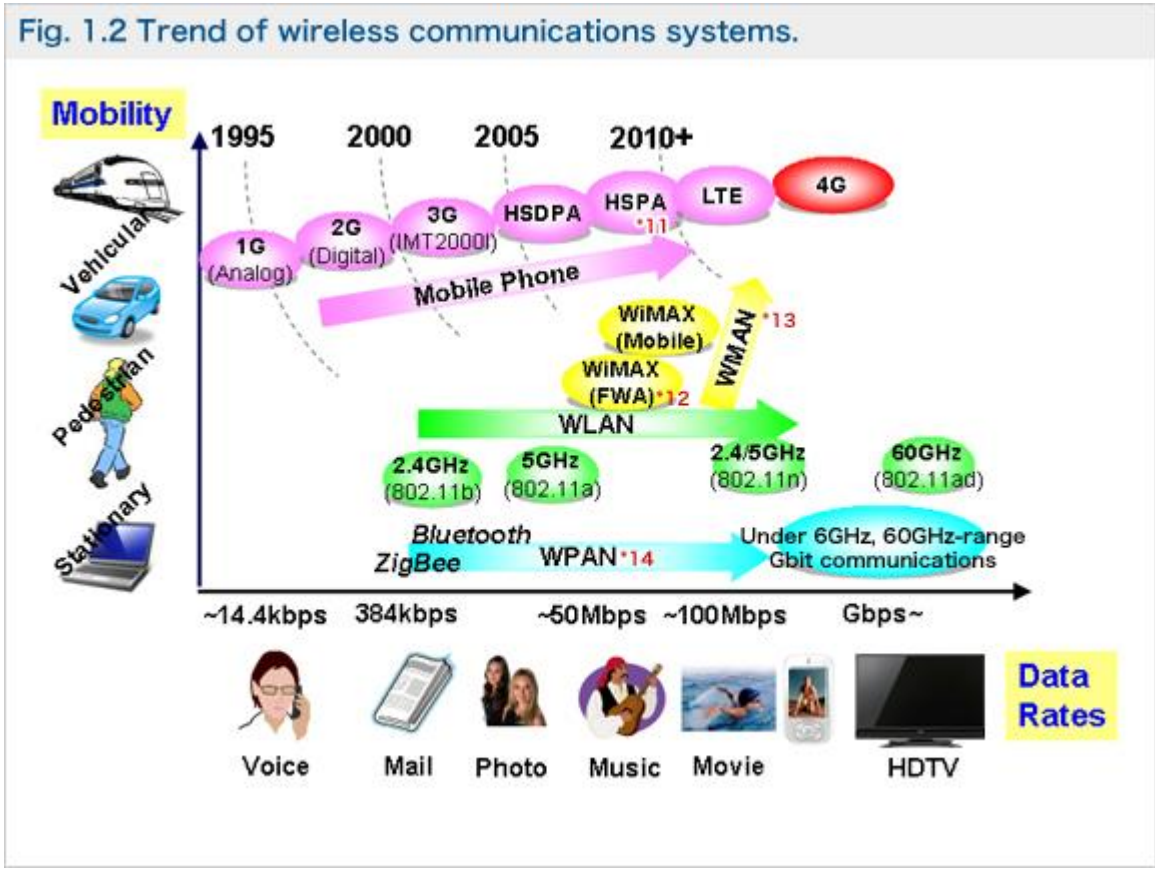
gerard.chalhoub@uca.fr
http://sancy.univ-bpclermont.fr/~chalhoub/

Everything is connected



Source: https://blogs.cisco.com/digital/the-internet-of-everything-has-begun

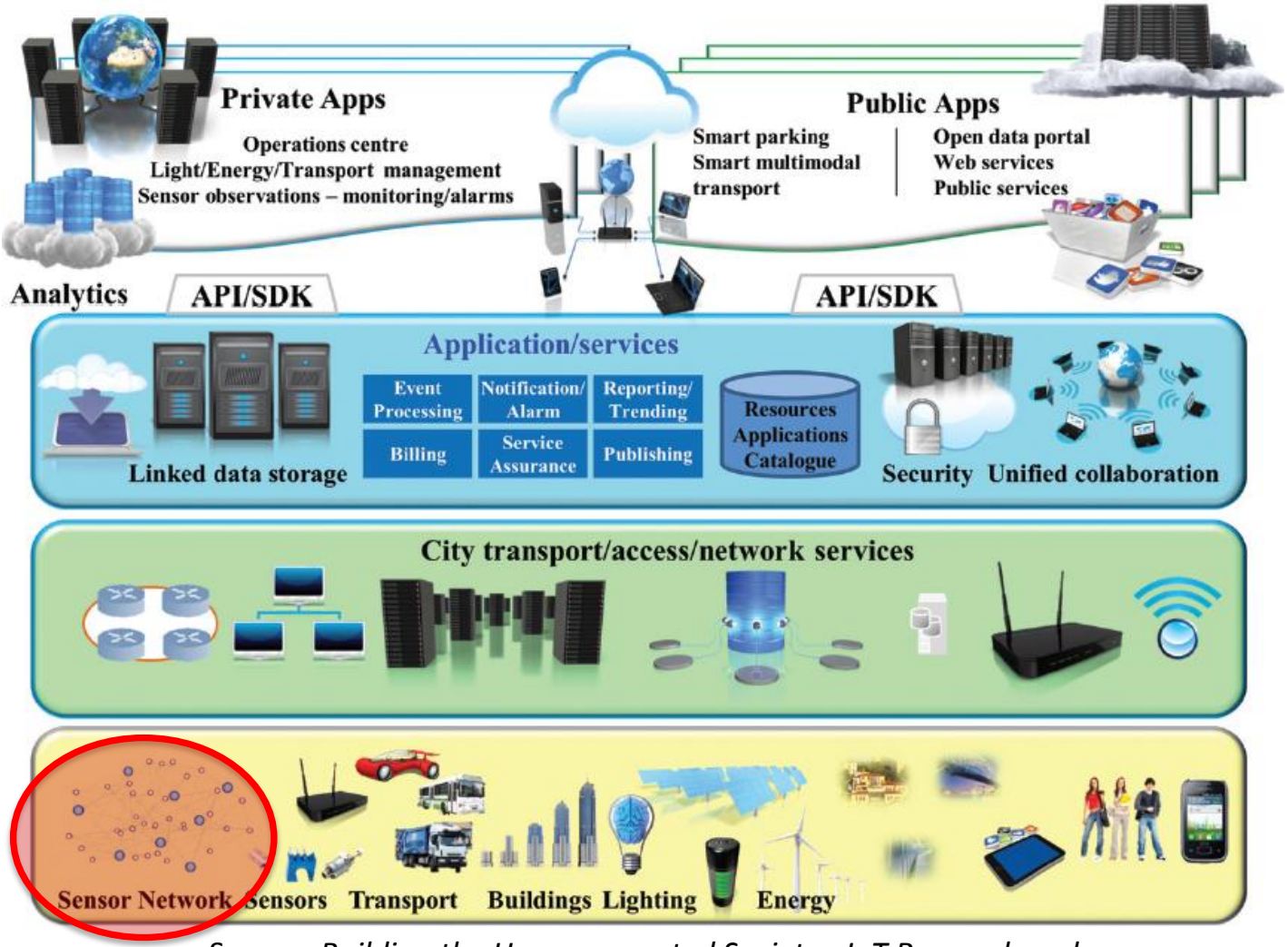
Trend of wireless communications systems



*11 HSPA : High Speed Packet Access
*12 FWA : Fixed Wireless Access
*13 WMAN : Wireless Metropolitan Area Network
*14 WPAN : Wireless Personal Area Network

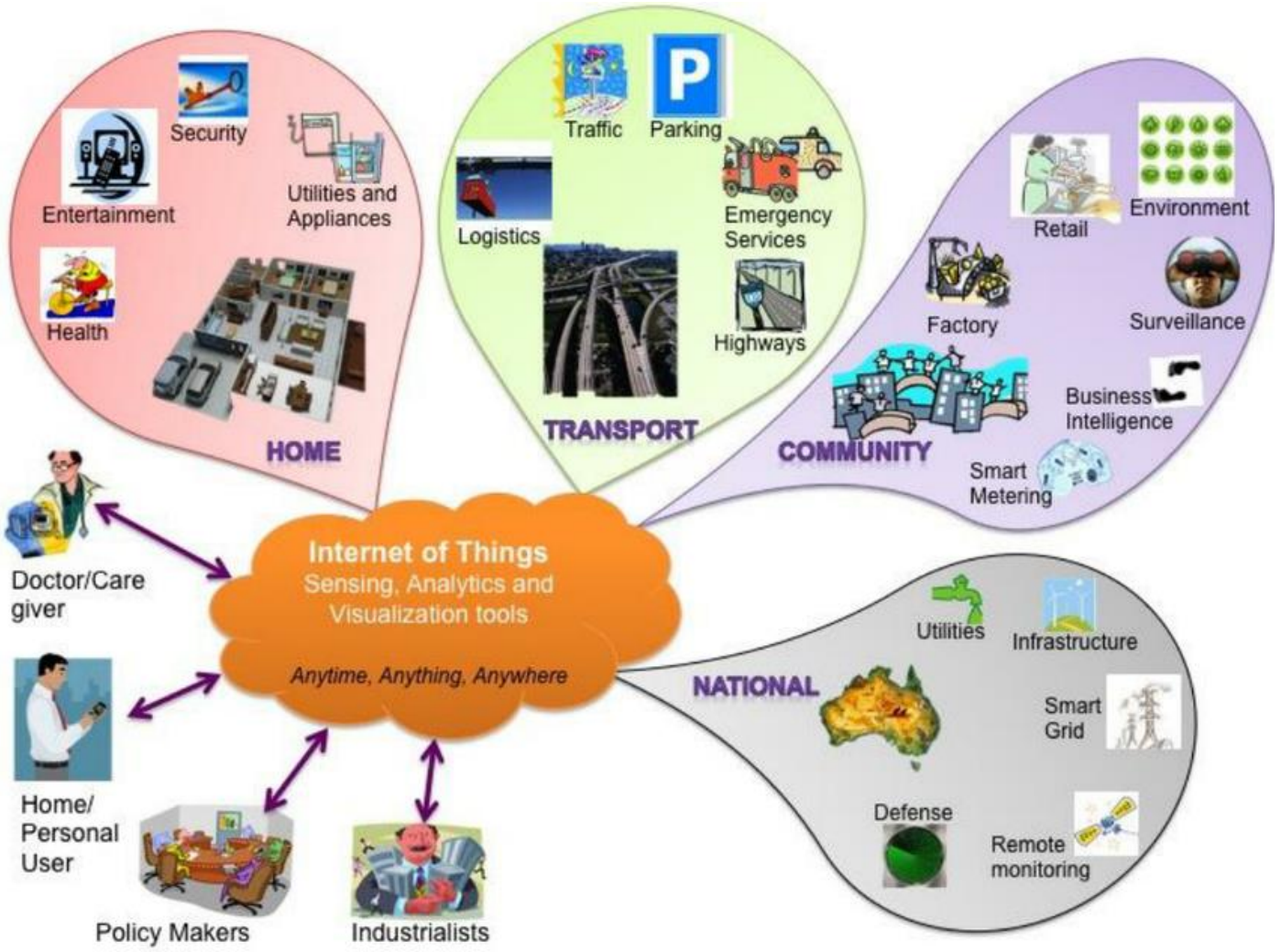
Source: http://www.mitsubishielectric.com/semiconductors/triple_a_plus/technology/02/index2.html

Internet of things and WSNs



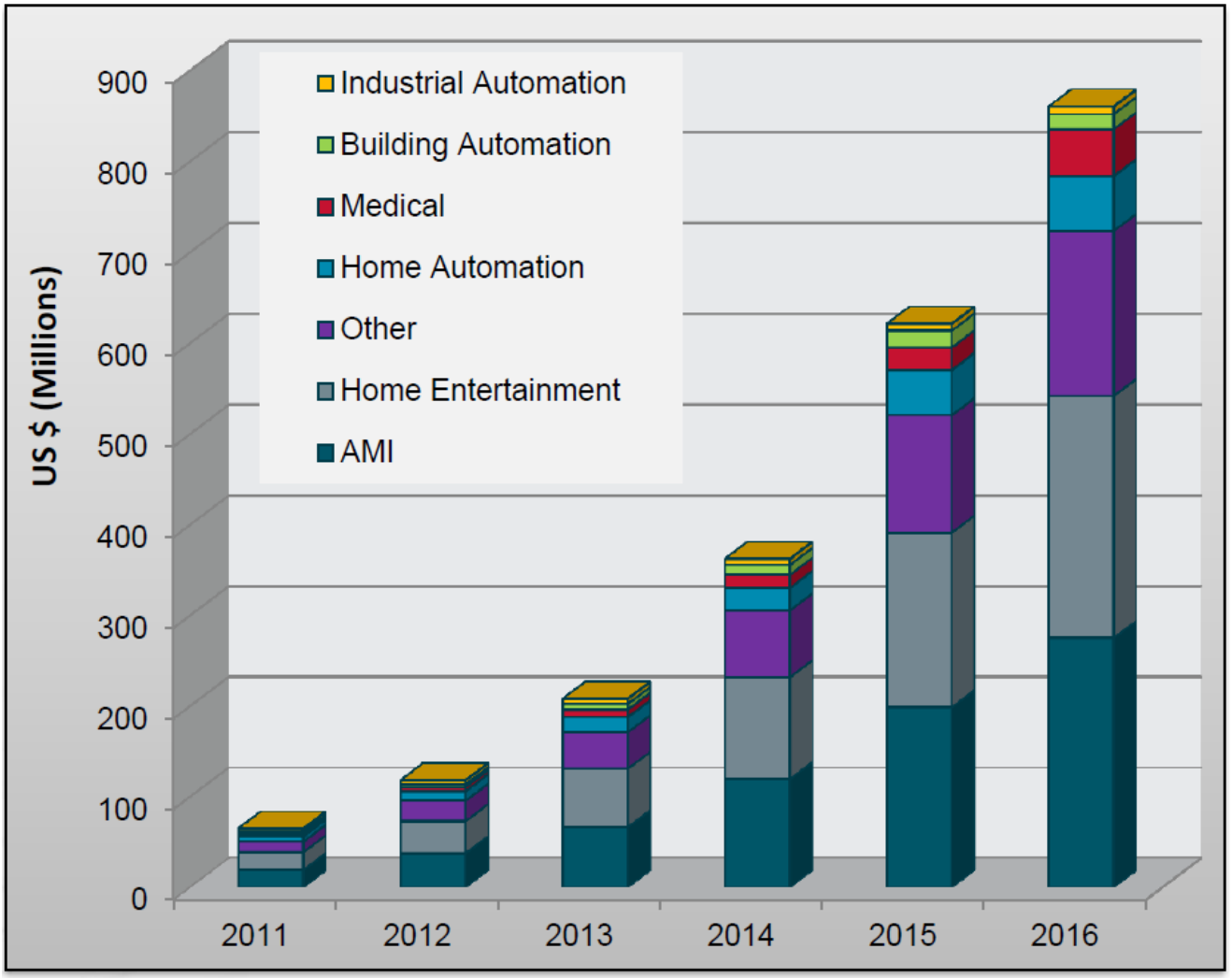
Source: *Building the Hyperconnected Society - IoT Research and Innovation Value Chains, Ecosystems and Markets*

Everything is controlled and monitored



Source: Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions

Application domains using WSNs



Source: ABI research

The goal of this course

- Understand the specificity of wireless links
- Understand the basic physical phenomena in wireless communications
- Analyze wireless MAC protocols
- Study examples of MAC layers of IEEE standards
- Study routing in ZigBee networks

Chapters

- Part 1: Wireless Medium
- Part 2: MAC Protocols
- Part 3: WiFi IEEE 802.11
- Part 4: IEEE 802.15.4
- Part 5: ZigBee

Introduction

- What makes wireless networks different?
- Can we just replace the cable with the air and keep using the same protocols to access the medium?
- What adaptations should be made?
- How reliable wireless is?

Needs in a WLAN

- Mobility or nomadism of users
- Speed, cost and efficiency of deployment
- Absence of cabling
- Robustness: links reliability and auto-reconfiguration
- Emergent needs:
  - Localization: home automation
  - Industrial applications
  - Comfort and multimedia
  - Security and surveillance

The challenge

- To ensure:
  - High data rate
  - Low latency
  - Low jitter
  - Respect a certain QoS (voice and video)
  - Non harmful transmission power

Medium capacities

- In a wired network, stations share the bandwidth capacity of the cable used in the network
- In a wireless network, the bandwidth of the medium is shared with « everyone »
- Bandwidth and channel allocation are managed by international and governmental rules (European Telecommunications Standards Institute ETSI in France, Federal Communications Commission FCC in the US)

Allocation

- Part of the bandwidth is licensed and reserved for certain types of usage:
  - Strategic services (surveillance, satellites, etc.)
  - Mobile operators
  - Airspace activities
  - For more details *http://transition.fcc.gov/oet/spectrum/table/fcctable.pdf*

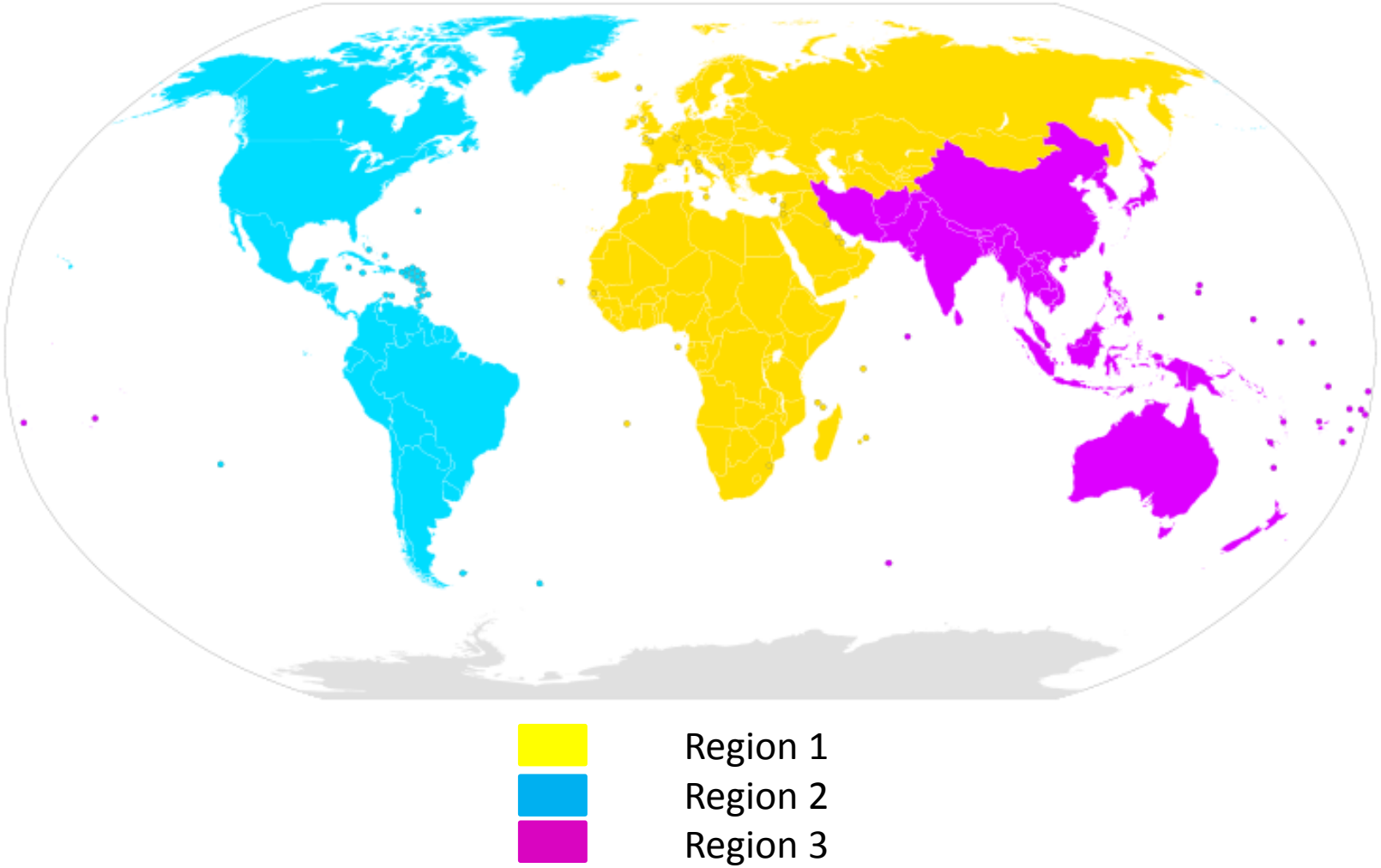
Industrial, Scientific and Medical

- For example, the US authorized public use of the following bands:
  - 902-928 MHz
  - 2.4000-2.4835 GHz
  - 5.725-5.850 GHz
- In Europe, the GSM uses the 890-915 MHz band → Only 2.4 et 5 GHz bands are available in Europe

Other ISM bands

Frequency range		Bandwidth	Center frequency	Availability
6.765 MHz	6.795 MHz	30 kHz	6.780 MHz	Subject to local acceptance
13.553 MHz	13.567 MHz	14 kHz	13.560 MHz	Worldwide
26.957 MHz	27.283 MHz	326 kHz	27.120 MHz	Worldwide
40.660 MHz	40.700 MHz	40 kHz	40.680 MHz	Worldwide
433.050 MHz	434.790 MHz	1.74 MHz	433.920 MHz	Region 1 only and subject to local acceptance
902.000 MHz	928.000 MHz	26 MHz	915.000 MHz	Region 2 only (with some exceptions)
2.400 GHz	2.500 GHz	100 MHz	2.450 GHz	Worldwide
5.725 GHz	5.875 GHz	150 MHz	5.800 GHz	Worldwide
24.000 GHz	24.250 GHz	250 MHz	24.125 GHz	Worldwide
61.000 GHz	61.500 GHz	500 MHz	61.250 GHz	Subject to local acceptance
122.000 GHz	123.000 GHz	1 GHz	122.500 GHz	Subject to local acceptance
244.000 GHz	246.000 GHz	2 GHz	245.000 GHz	Subject to local acceptance

ISM Region map (wikipedia)



Wireless technologies that use the 2.4GHz band

- WiFi: IEEE 802.11 (mobile phones, computers, etc.)
- Bluetooth: IEEE 802.15.1 (mobile phones, computers, headphones, etc.)
- ZigBee, WirelessHART, ISA100.11a: IEEE 802.15.4 (home automation equipment, industrial machines, etc.)
- Microwave ovens

Wireless LAN standards and certifications (1)

- The standardization bodies make sure that equipment from different vendors can interoperate
  - Internet Engineering Task Force (IETF): protocols and standards for the Internet, such as TCP/IP, EAP (Extensible Authentication Protocol), many more…
  - Institute of Electrical and Electronics Engineers (IEEE): the most influential standards body

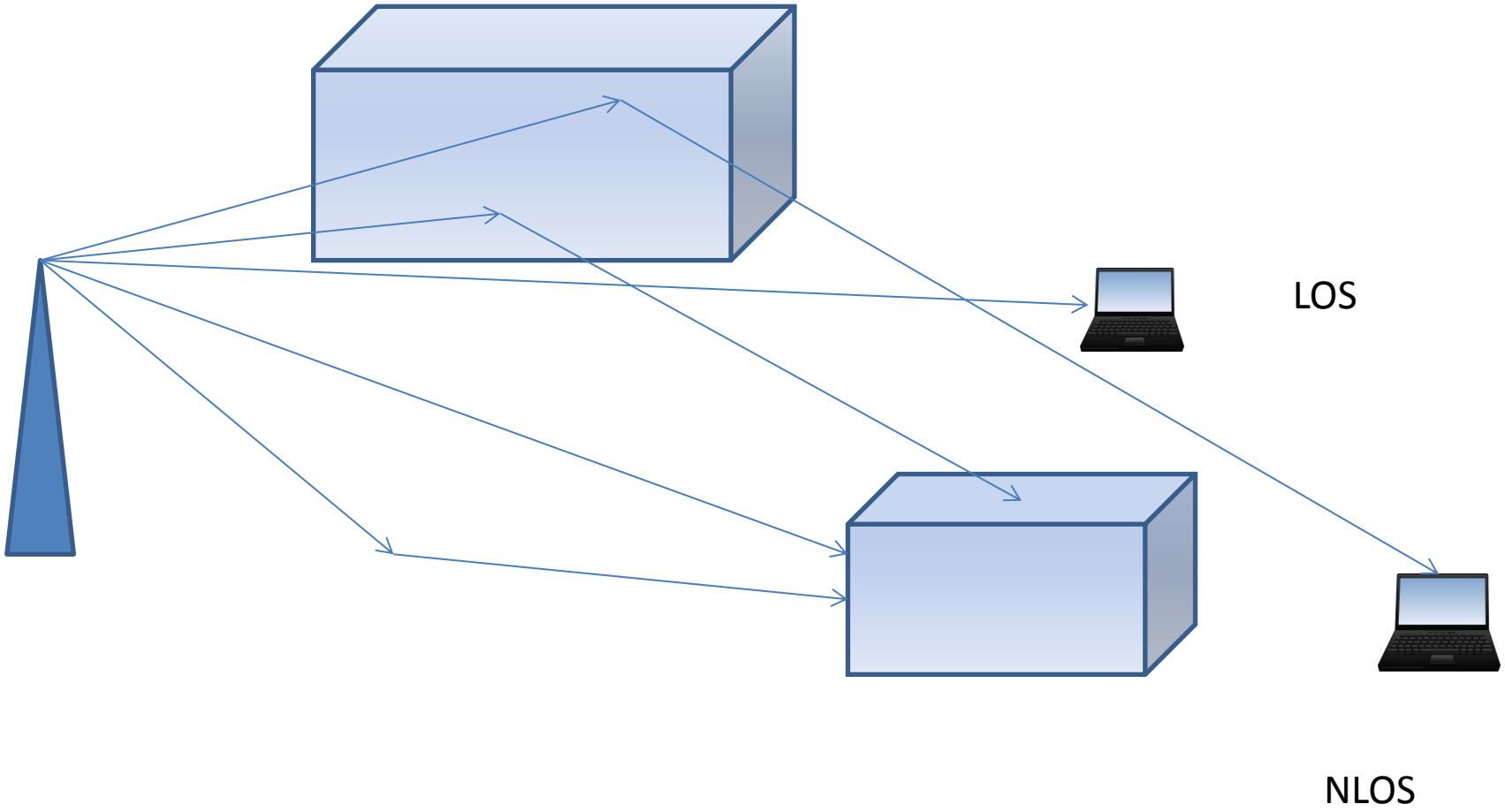
Wireless LAN standards and certifications (2)

- WiFi Alliance: nonprofit organization formed in 1999, main goal is to make sure that IEEE 802.11 standards are widely and correctly adopted
- ZigBee Alliance: nonprofit organization formed in 2002, main goal is to ensure the ZigBee standard widely and correctly adopted for sensing and control applications

Important issues

- LOS and NLOS
- Inter Symbol Interference
- Doppler Shift
- Attenuation and Path Loss
- Capture Effect

Obstacles and signal propagation
Multipath effect

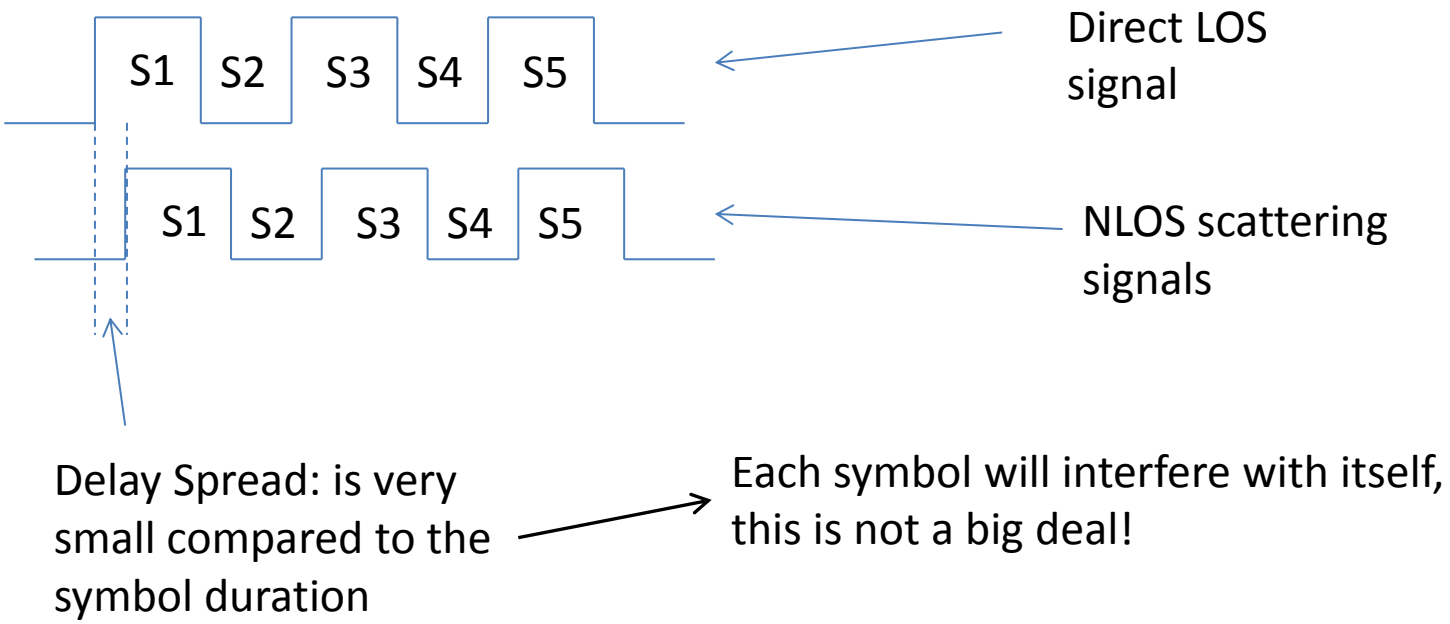


Positive Impact

- No need to be in Line Of Sight to be able to communicate → Reflections and multipath help establish links
- Note that lower frequencies have better ability to penetrate obstacles and travel longer distances than higher frequencies

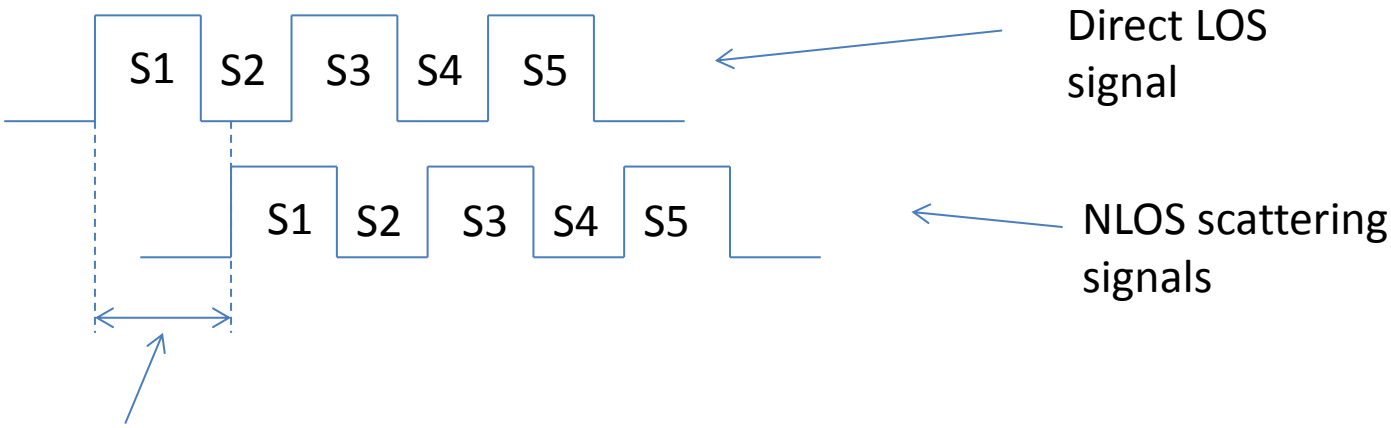
On the other hand

- A receiver will have to deal with multiple replicas of the same signal: because of the multipath effect



Inter Symbol Interference

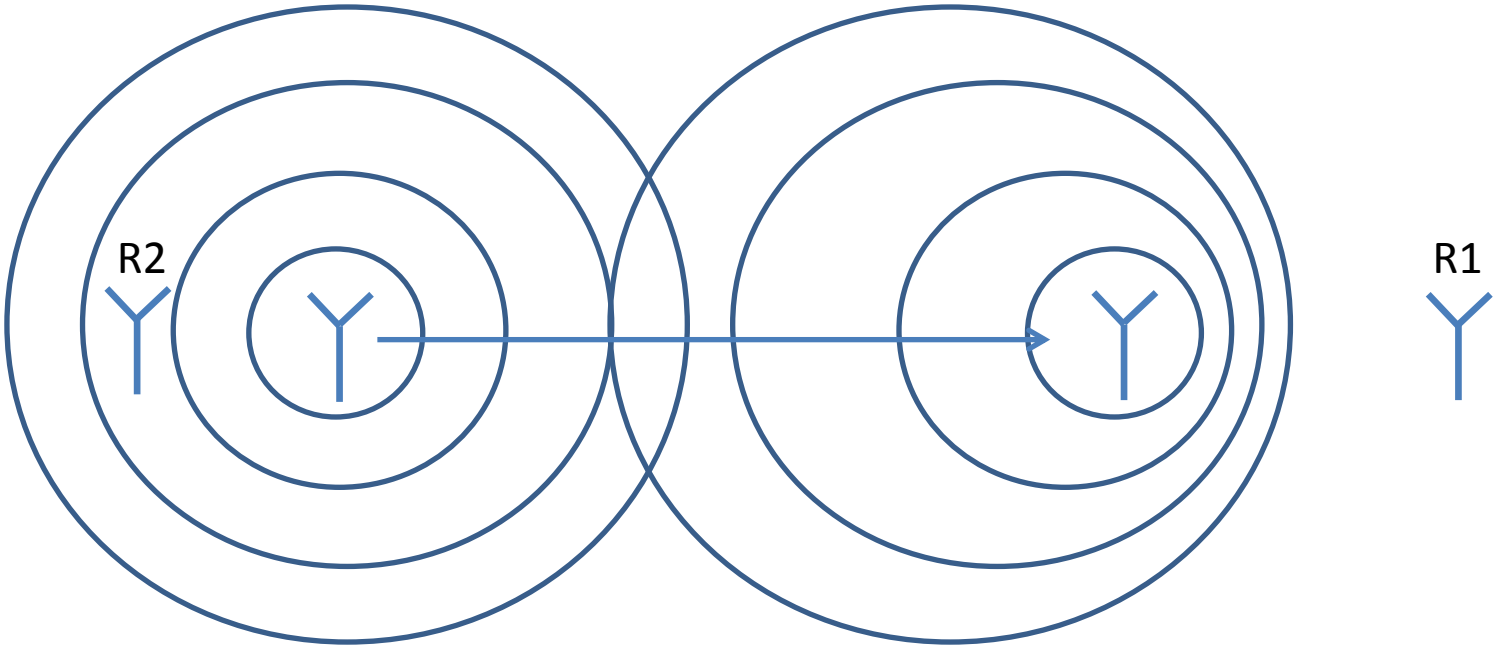
- The previous symbol interferes with the current symbol, this is a bigger deal!
- With more NLOS signals, symbols will interfere with S - 1, S - 2, S - 3 and so forth… A counter measure to avoid ISI is ECC (Error Correction Code) which consists in multiplying the number of bits that represents one bit (Hamming code)



Doppler Shift

- Change in the frequency that arises due to relative motion between the transmitter and the receiver
- If the receiver is moving towards the transmitter: the frequency gets higher
- If the receiver is moving away from the transmitter: the frequency gets lower
- If the receiver is moving in a perpendicular way in regards to the receiving signal: the frequency does not change

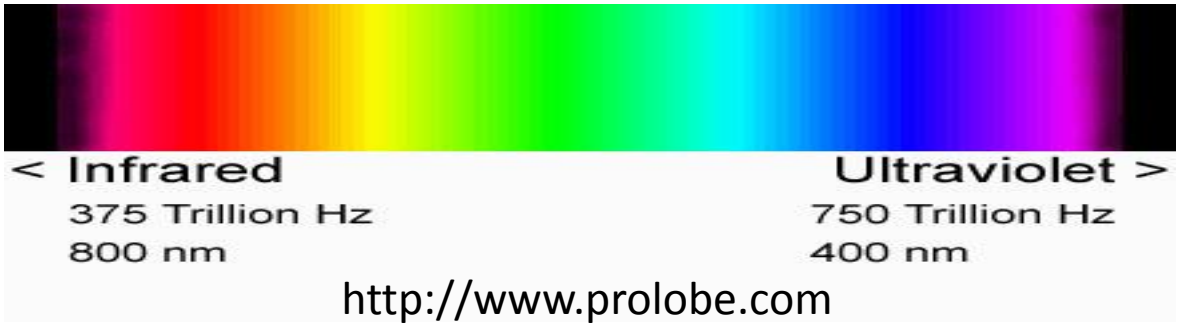
Moving transmitter



R1 will detect higher frequencies compared to what S is sending
R2 will detect lower frequencies compared to what S is sending

Examples of Doppler Shift

- When an ambulance is moving towards you its siren sounds differently from when it will be moving away from you
- When a star is moving towards the earth it will look bluer than it actually is, and when it is moving away from the earth it will look more reddish



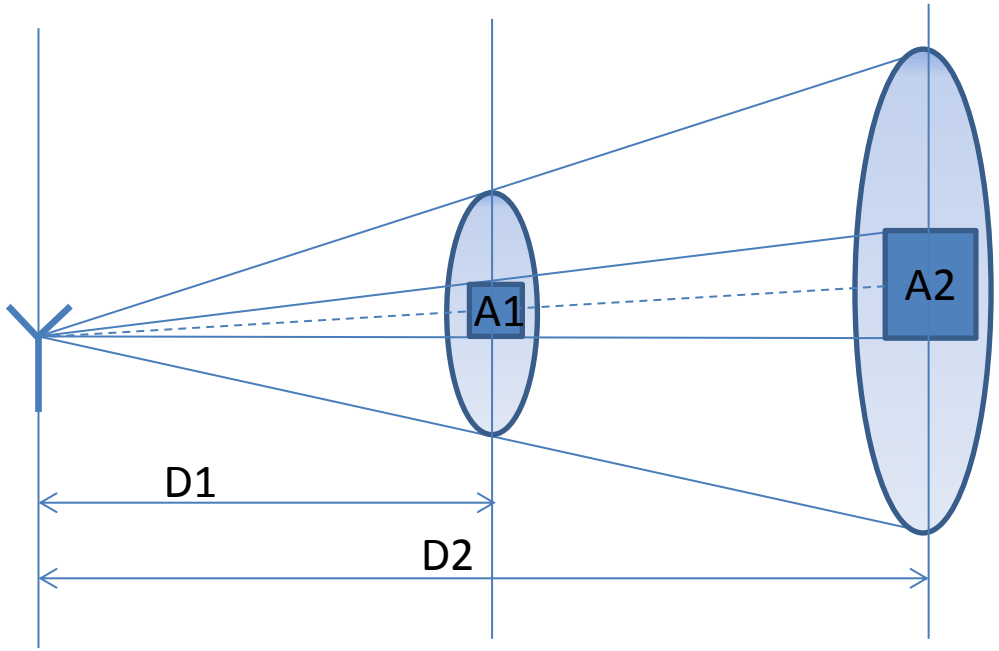
Effect of Doppler Shift

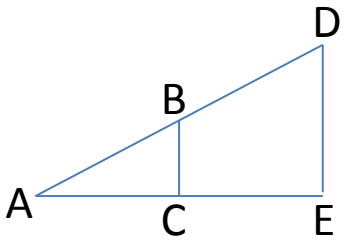
- Depending on the PHY encoding, some bits might flip
- The relative velocity is an important factor, higher velocities have more impact
- Walking speed in indoor environment has insignificant effect
- Might become more important for industrial rotating machines

Attenuation

- All signals loose power over distance, this is called Path Loss
- The Path Loss exponent is an indicator of the propagation environment
- It varies from 1 to 6, where 2 represents Path Loss exponent in Free Space
- Values between 3 and 6 represent urban environments
- Values less than 2 represent tunnel like places
- Free space formula: $\frac{Pr}{Pt} = Gt * Gr * \left(\frac{\lambda}{4\pi D}\right)^{\mathbf{2}}$

Power over distance





$AB/AD = AC/AE = CB/ED$

$A1 = 4CB^2$ $A2 = 4ED^2$

$A1/A2 = (D1/D2)^2$

(Same reasoning can be applied for the area of the disks πCB^2)

Conclusion: given a reference power Pref at 1 m from the source, the received signal power Pr at a point D is:
Pr = Pref/(Distance to D) ^{2}

But…

- Distance is not the only factor in communication establishment
- Location is an important factor that might cause starvation for certain receivers
- The choice of frequency has an effect as well
- This aspect is almost impossible to predict: very small movements in the room cause a change in the multipaths

dBm

- dBm is used to express signal power
- It is the ratio in dB of the measured power referenced to 1 milliWatt
- $P_{dBm} = 10*log_{10}(P_{mW}/1mW)$
- 0dBm = 1mW
- Every time the power in mW is doubled, the power in bBm is incremented by 3
- 2mW = 3dBm, 4mW = 6dBm, 8mW = 9dBm
- -3dBm = 0.5mW, -6dBm = 0.25mW, -9dBm = 0.125mW
- Also, when you increment by 10 in dBm, you multiply by 10 in mW

Path Loss formula

- $L = 10 * n * log_{10}(d) + C$
  - *L* is the Path Loss in decibels
  - *n* is the Path Loss exponent
  - *d* is the distance
  - *C* is a constant that accounts for system loss
- Path Loss is very difficult to predict, it can be roughly estimated according to measurements and observations

Received signal power

- Friis equation (for Free Space propagation):

$$\frac{Pr}{Pt} = Gt * Gr * \left(\frac{\lambda}{4\pi D}\right)^2$$

Where Pr is received signal power, Pt is the transmitted signal power, Gt is the antenna gain at the transmitter, Gr is the antenna gain at the receiver, λ (lambda) is the wavelength, D is the distance between the antennas

When Gt and Gr are in dB and Pt in dBm, it becomes:

$$Pr = Pt + Gt + Gr + 20log_{10}(\frac{\lambda}{4\pi D})$$

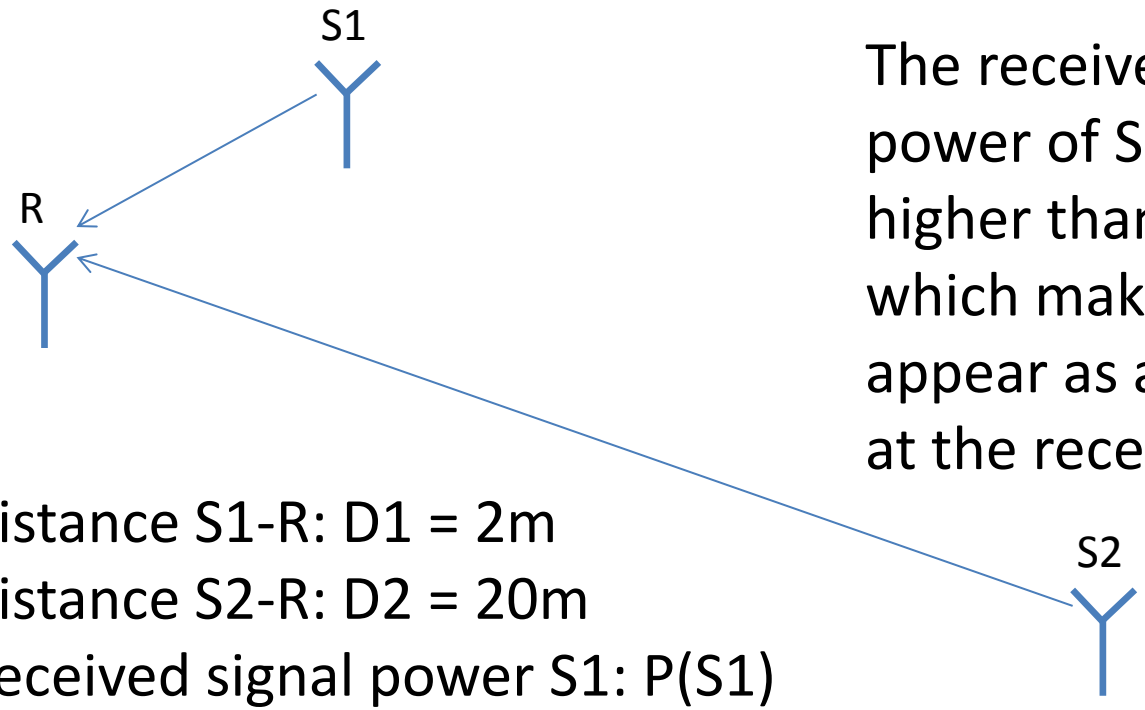
Unrealistic modeling

- Friis equation can only be applied for satellite communications and tests in anechoic chambers
- Friis considers that there is no multipath!
- Other more complex models exist… The Path Loss exponent is the most important factor to calibrate

Collisions and capture effect

- The received power at one point is very difficult to predict when dealing with a moving environment
- The higher the receiving power the better the signal resists against interferences and background noise
- Consequences of simultaneous receptions (collision): Signal loss or Capture Effect

Near Far Effect: Capture effect

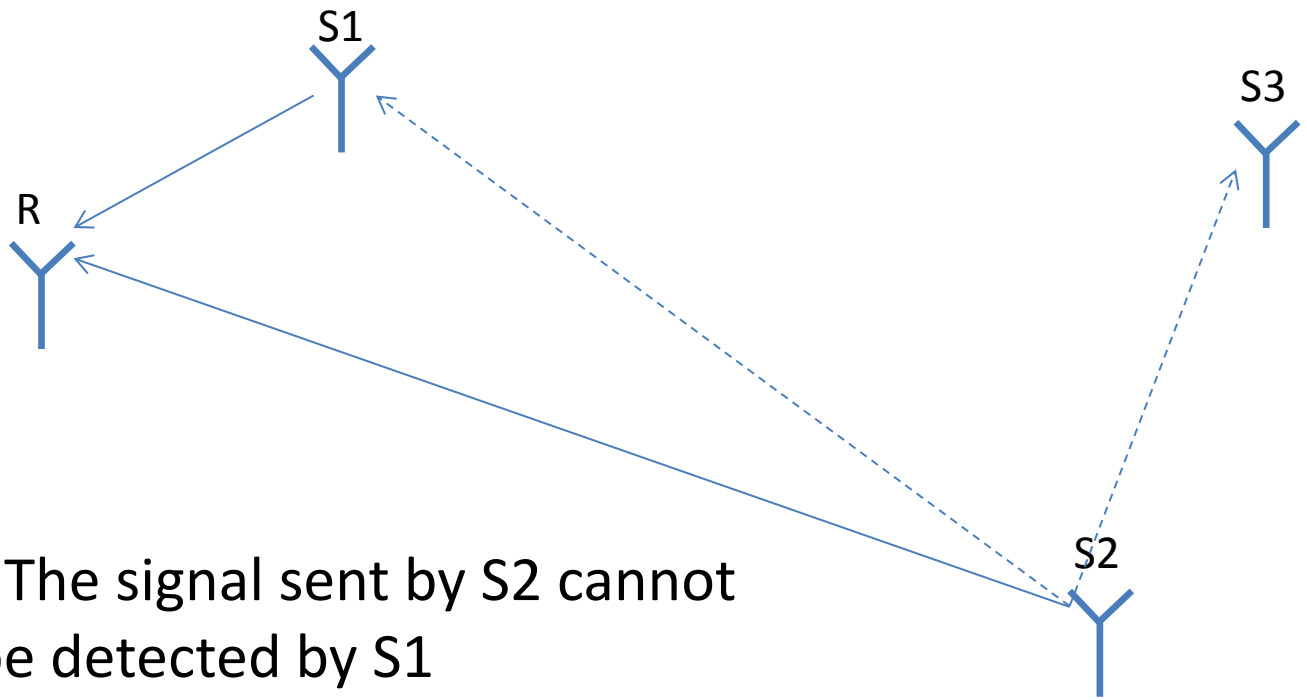


The received signal power of S1 is much higher than that of S2, which makes the latter appear as ambient noise at the receiver

Distance S1-R: D1 = 2m
Distance S2-R: D2 = 20m
Received signal power S1: P(S1)
Received signal power S2: P(S2)
$P(S1)/P(S2) = (D2/D1)^2$

P(S1) = 100 * P(S2)

Near Far Effect: Activity detection



- The signal sent by S2 cannot be detected by S1
- S1 is blinded by its own signal
- S3 can detect the activity of S2 if it is not in transmit mode and is listening to the medium

Effect on the MAC protocols

- CSMA/CD is based on the fact that a sender is able to detect collisions while in transmission mode
- This is not possible in wireless communications
- New MAC protocols should be proposed for WLANs

Transmission range and receiver sensitivity

- The transmission range depends essentially on the transmission power, the throughput, and the receiver sensitivity
- The receiver sensitivity might slightly vary between constructors and NICs
- Higher throughputs decrease communication range
- Transmission power is regulated (20dBm is the maximum transmission power for 2.4GHz)

Example for Cisco Aironet CardBus

Receiver Sensitivity 802.11g (typical)

- -94 dBm @ 1 Mbps → 124 m
- -93 dBm @ 2 Mbps
- -92 dBm @ 5.5 Mbps
- -86 dBm @ 6 Mbps → 91 m
- -86 dBm @ 9 Mbps
- -86 dBm @ 12 Mbps
- -86 dBm @ 18 Mbps → 54 m
- -84 dBm @ 24 Mbps
- -80 dBm @ 36 Mbps
- -75 dBm @ 48 Mbps
- -71 dBm @ 54 Mbps → 27 m

Higher throughput → Lower range and Less sensitivity

Received signal power

- A signal can still be decoded if received at -94 dBm, which is the equivalent of $4*e^{-10}$ mW
- We are dealing with very small energy levels!

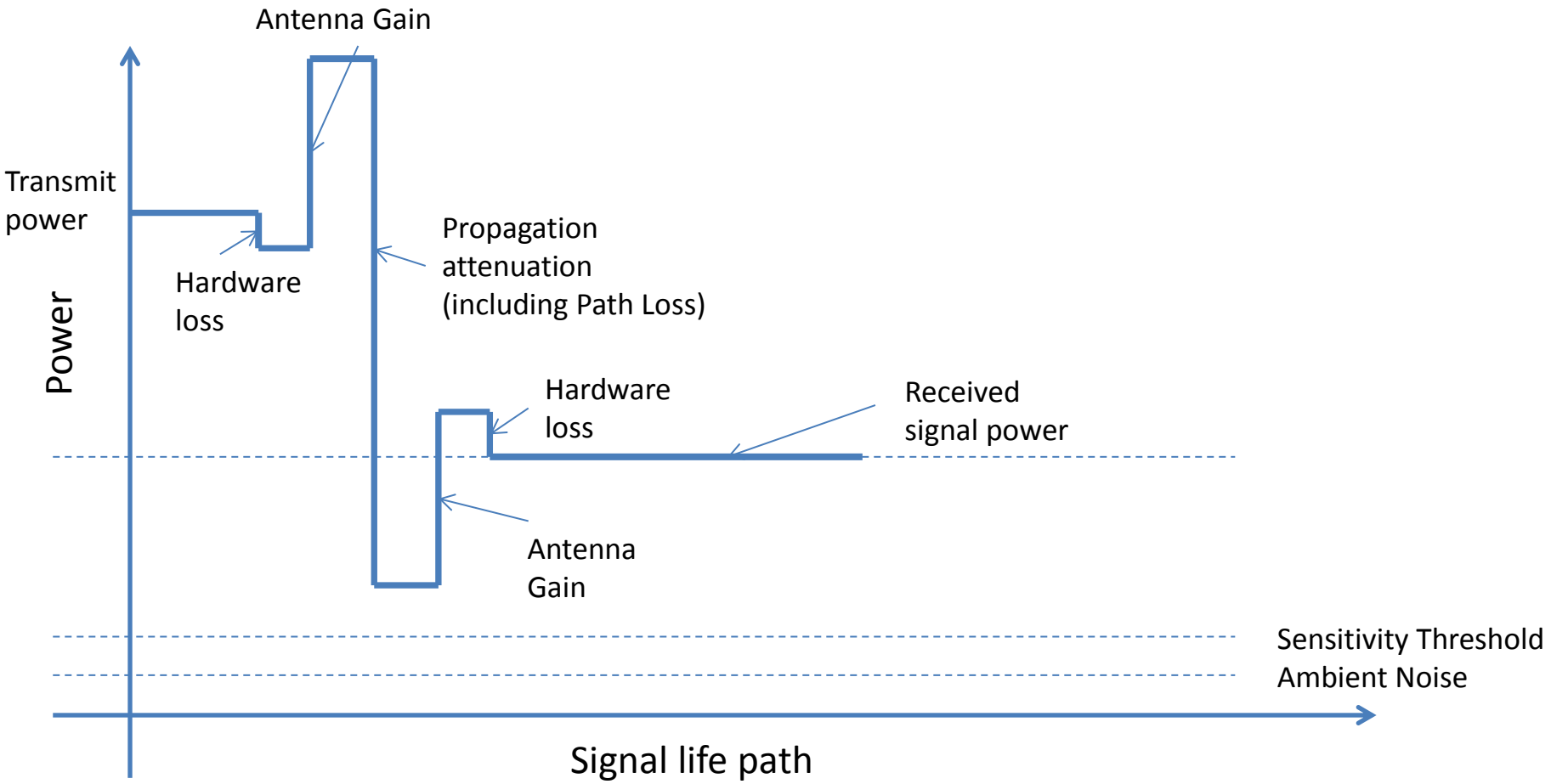
Reception without errors

- Two conditions have to be met:
  - Transmit power + antenna gains – Path Loss > receiver sensitivity
  - Received signal power/Ambient Noise power > a given threshold (16 dB for WiFi at 11 Mbps)
- If this threshold is exceeded, we start observing a significant increase in packet loss

Ambient Noise and Carrier Sensing

- In general, ambient noise is estimated at -100 dBm
- This means that receivers sensitivity should be higher than -100 dBm
- To make a carrier sense, any energy detected above -95 dBm means that the medium is occupied by at least one active transmission

Link behavior



In theory

- In a nutshell:
  - Transmit signal power = transmitter power(dBm) – hardware loss (dB) + antenna gain (dBi)
  - Signal Propagation = signal attenuation (dB)
  - Received signal power = antenna gain (dBi) – hardware loss (dB) – receiver sensitivity (dB)
- The positive result leaves us with a margin to choose the adequate throughput, modulation, transmission power, etc.

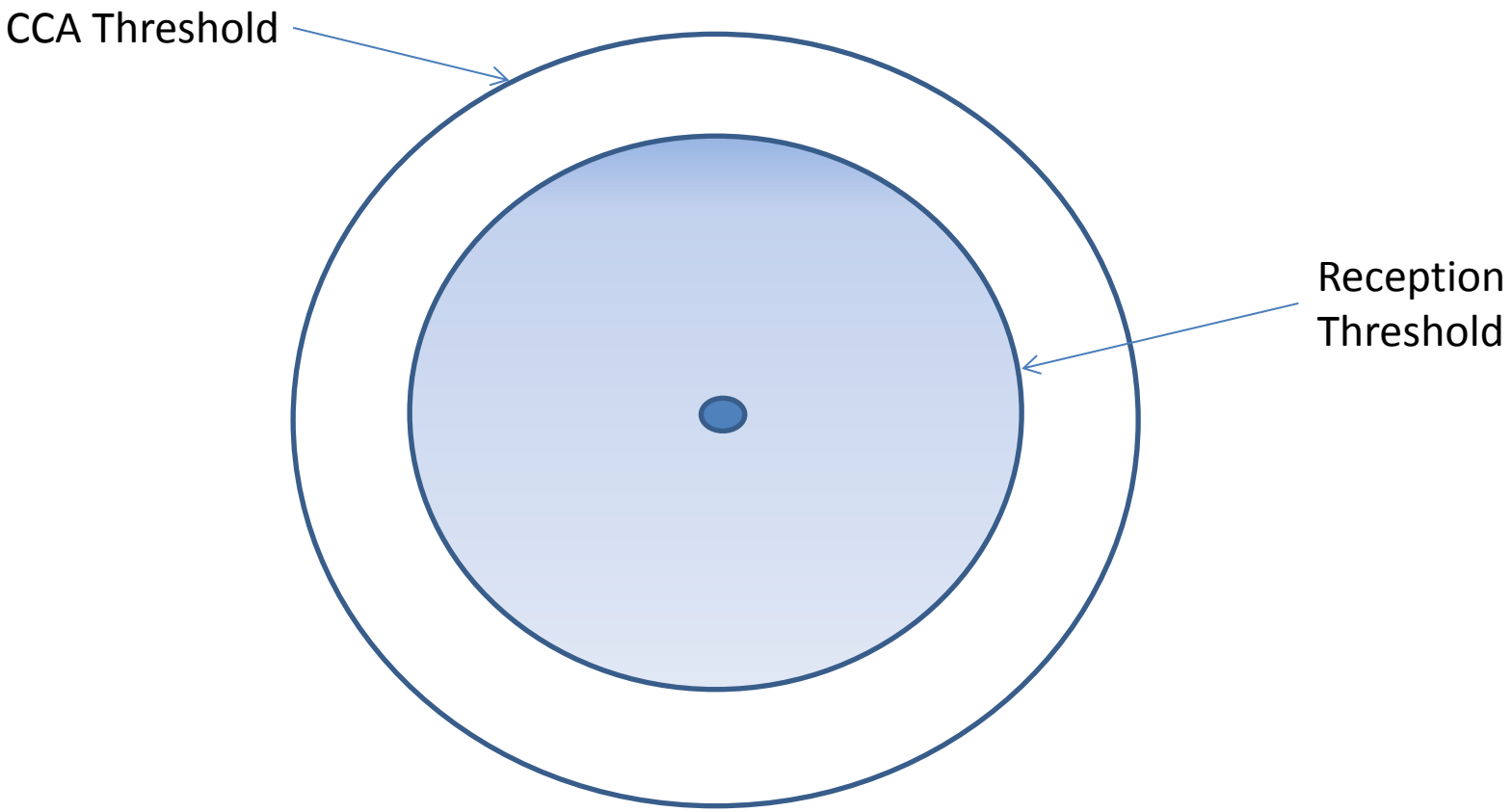
Communication range

- The efficiency of a link depends on the relative positions of the transmitter and the receiver
- This efficiency is estimated based on either the number of frames (FER, Frame Error Rate) or the number of bits (BER, Bit Error Rate) or the number of symbols that the transmitter had to retransmit because of detected errors

Good reception

- All points where the receiver is able to receive from the transmitter with a certain BER or FER above a certain threshold form the communication range of a transmitter
- This range is often represented as a circle around the transmitter
- The radius of the circle represents the communication range

Summary



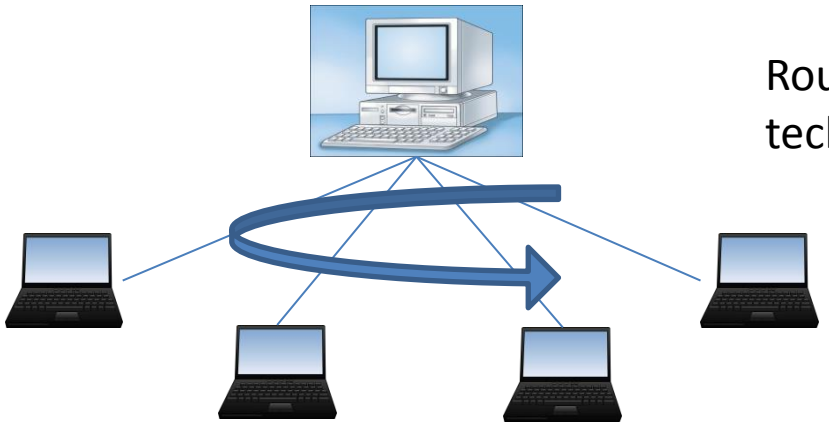
Part 2:
Wireless MAC protocols

Definition

- A MAC protocol is the method used to access a shared medium with the available resources
- These resources are essentially the channel bands and time slots for radio transmissions
- For Infrared transmissions for example, it is the color (wave length)

Origins

- In LANs, one of the first sharing techniques to access one computer via several terminals was Polling Selecting
- A Master controls when and for how long each terminal slave is allowed to transmit or receive



Round Robin technique

Main goal

- When different independent users want to access a shared transmission medium, they need to follow a set of rules to avoid or solve conflicts when they access simultaneously
- This set of rules constitute the MAC protocol
- The main goal is to optimize the use of the available resources

Functionalities

- Optimal resource usage: avoid time and energy consumption, for example by preventing continuous access when collisions occur
- Guaranteed Quality of Service: access delay should not exceed a certain threshold
- Equity between stations belonging to the same class of service

The challenge

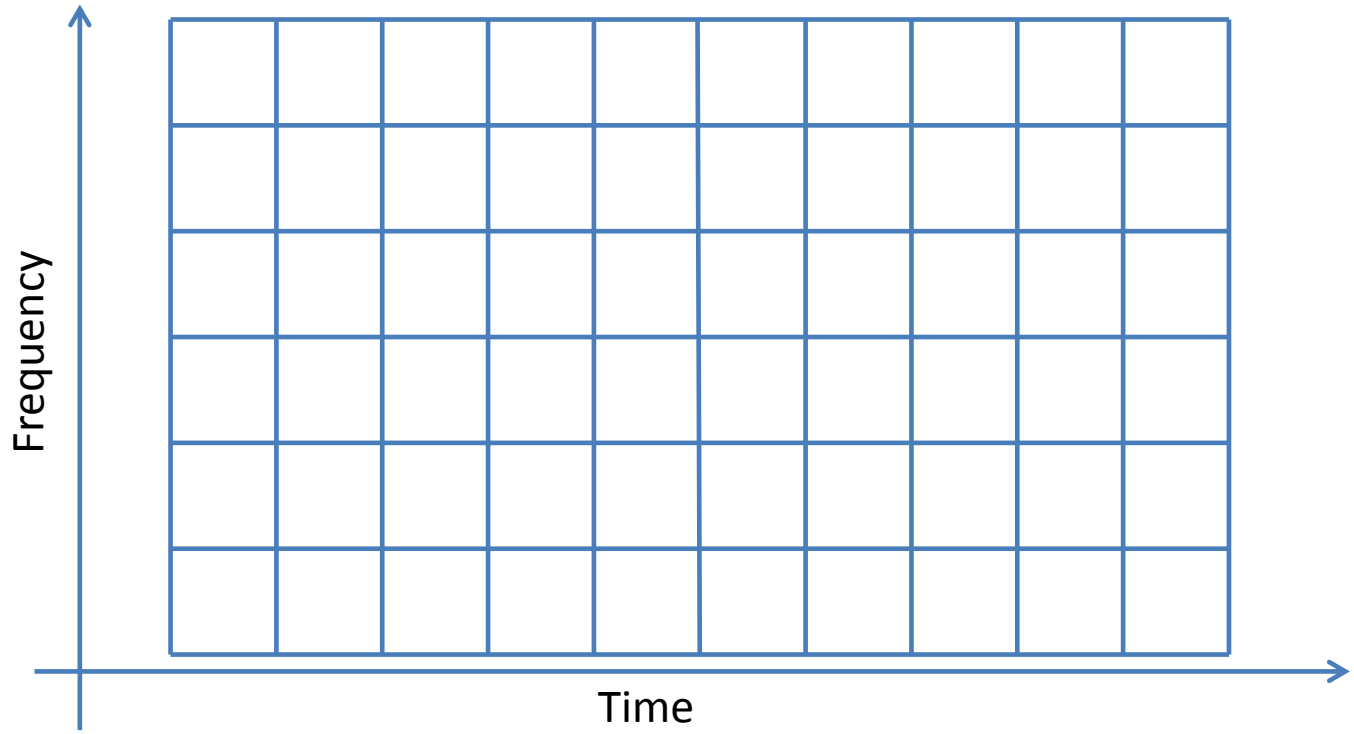
- With a given limited bandwidth, the MAC protocol should allow users to access the medium at a certain point in time, space and frequency:
  - Distributing timeslots
  - Allocating channels inside the bandwidth
  - Managing antenna orientation and transmission power

Classifications

- Centralized/Distributed: depending on the existence of a central network entity that manages access to the medium (allocating timeslots for nodes)
- Deterministic/Probabilistic: access to the medium is either guaranteed (a node is sure to be able to transmit) or not guaranteed with a certain probability of success (prone to collisions)

Bandwidth sharing

- At a certain point in space, the channel is represented as a matrix of frequencies and timeslots

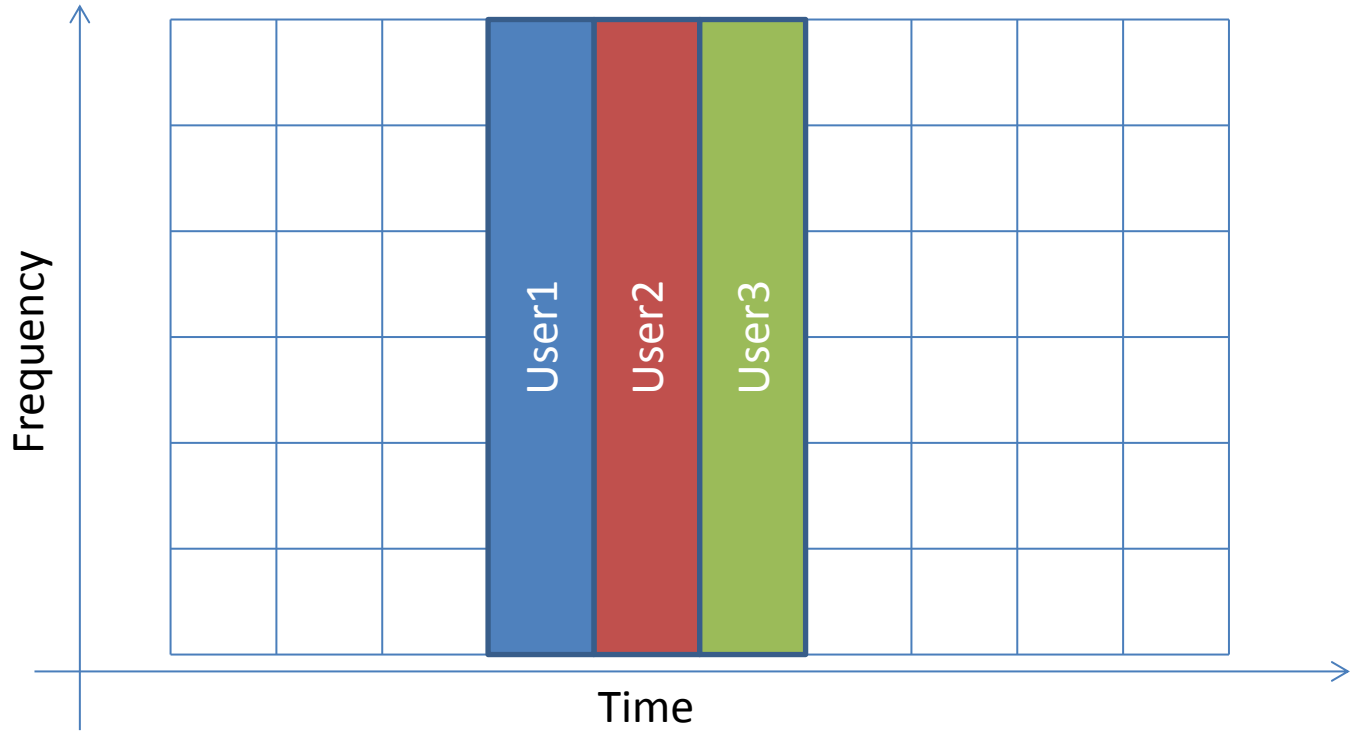


TDMA

- Time Division Multiple Access (TDMA) mode allows a user to send a signal during a given timeslot
- Users send signals one after the other for very small durations
- TDMA is used by GSM 2G (Global System for Mobile Communications second Generation) and DECT (Digital Enhanced Cordless Telecommunications)

TDMA example

- Example of 3 users accessing the bandwidth in a consecutive manner



Pros and Cons of TDMA

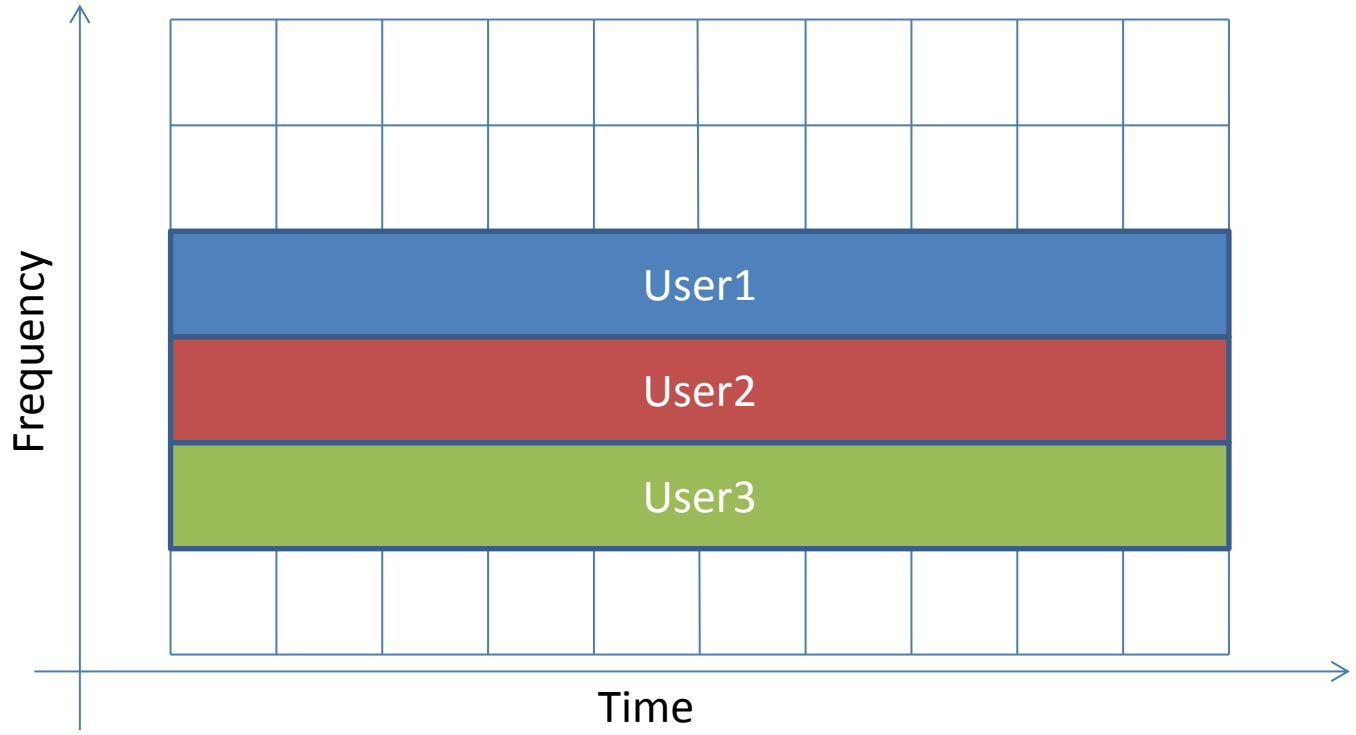
- Advantages:
  - Simple transceivers
  - Each user has the whole bandwidth for a period of time which helps fight against Rayleigh fading
- Disadvantages:
  - Synchronization is needed at every timeslot
  - Time and energy wasting due to margin considerations for synchronization imprecision

FDMA

- Frequency Division Multiple Access mode allows a user to send on a certain channel permanently
- Users can access the channel simultaneously
- Each user has its own portion of the channel
- FDMA is used in satellite communications

FDMA example

- Example of 3 users accessing the bandwidth simultaneously on different channels

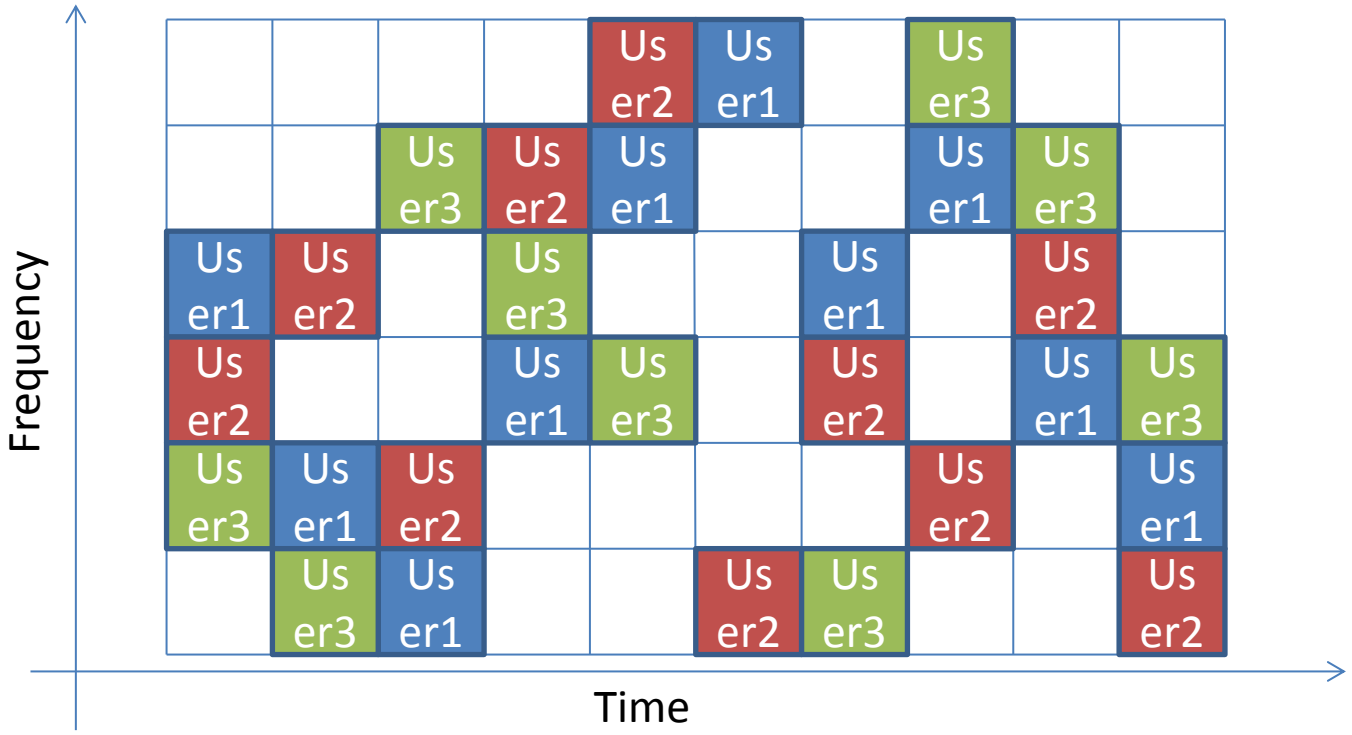


Pros and Cons of FDMA

- Advantages:
  - Protection against interferences
  - Loose synchronization
  - Little energy and time wastage
- Disadvantages:
  - More complex transceivers (more accurate filters)
  - Rayleigh fading more difficult to avoid
  - Channel wastage due to channel spacing to avoid interferences (imperfection of filters)

Hybrid method: Bluetooth example

- Bluetooth uses a frequency hopping scheme to change channels every timeslot



Base Station

- TDMA and FDMA schemes are generally implemented for infrastructure deployments
- A base station is responsible for calculating and allocating timeslots and communications schemes for the stations
- This is often done in a static way and without taking into account the communication needs of the stations

Sharing the same channel during the same time interval

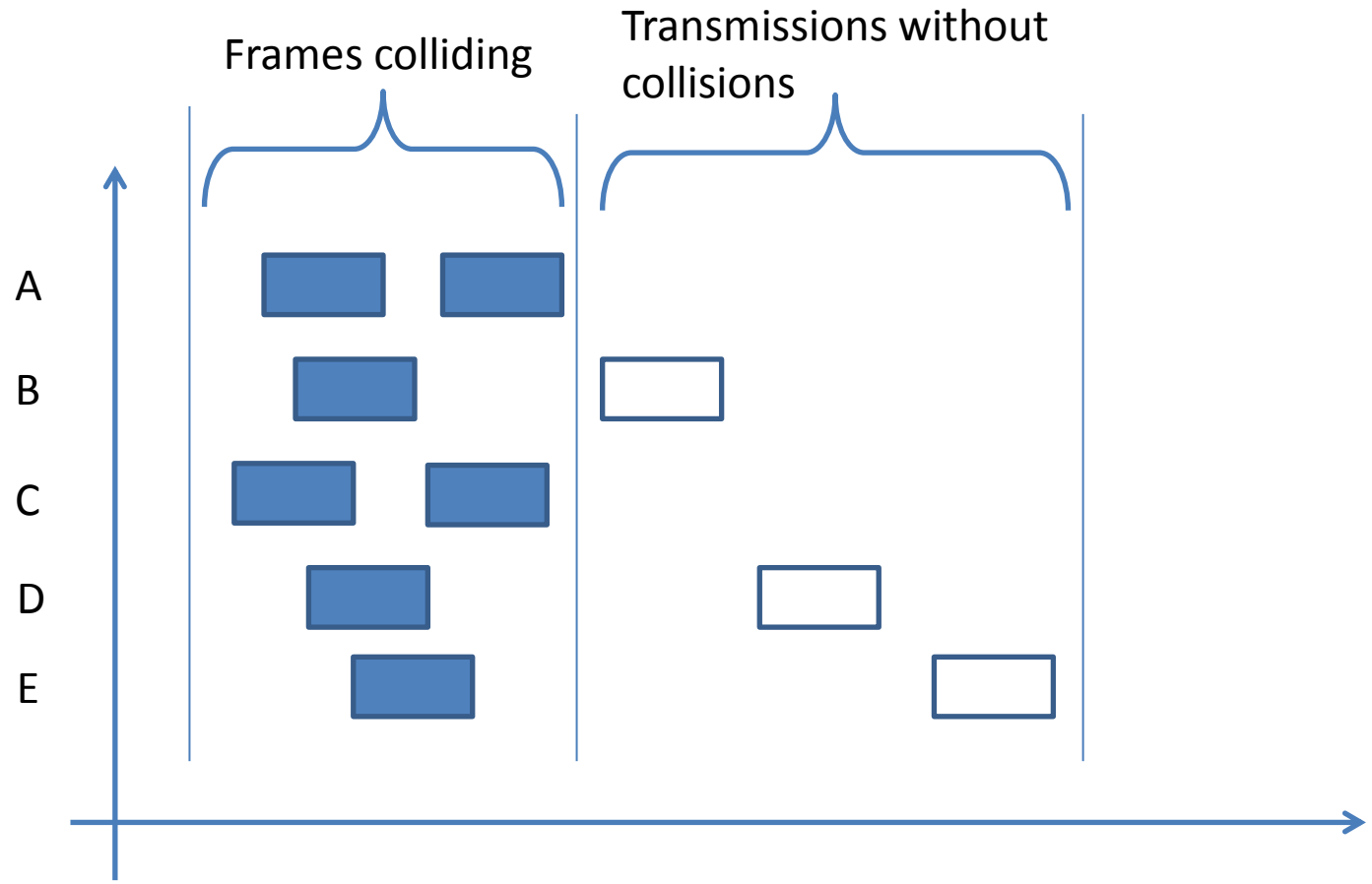
- In this section, we assume that stations need to share the same channel
- For example, sharing the same channel in the 2.4 GHz band
- Important facts:
  - Only one signal can be received
  - Simultaneous access might lead to collisions
  - Cannot use FDMA nor TDMA

Aloha protocol (ALOHAnet)
Pure Aloha

- Project started in 1968 to interconnect islands of Hawaii using low cost radio equipment
- When a sender has something to send, it sends it
- When a collision occurs, the sender waits for a random period (called backoff) and then resends the packet again
- N.B. the random backoff scheme is the deciding factor in the performance

Multiple access example with Aloha

- 5 competing nodes with traffic to send

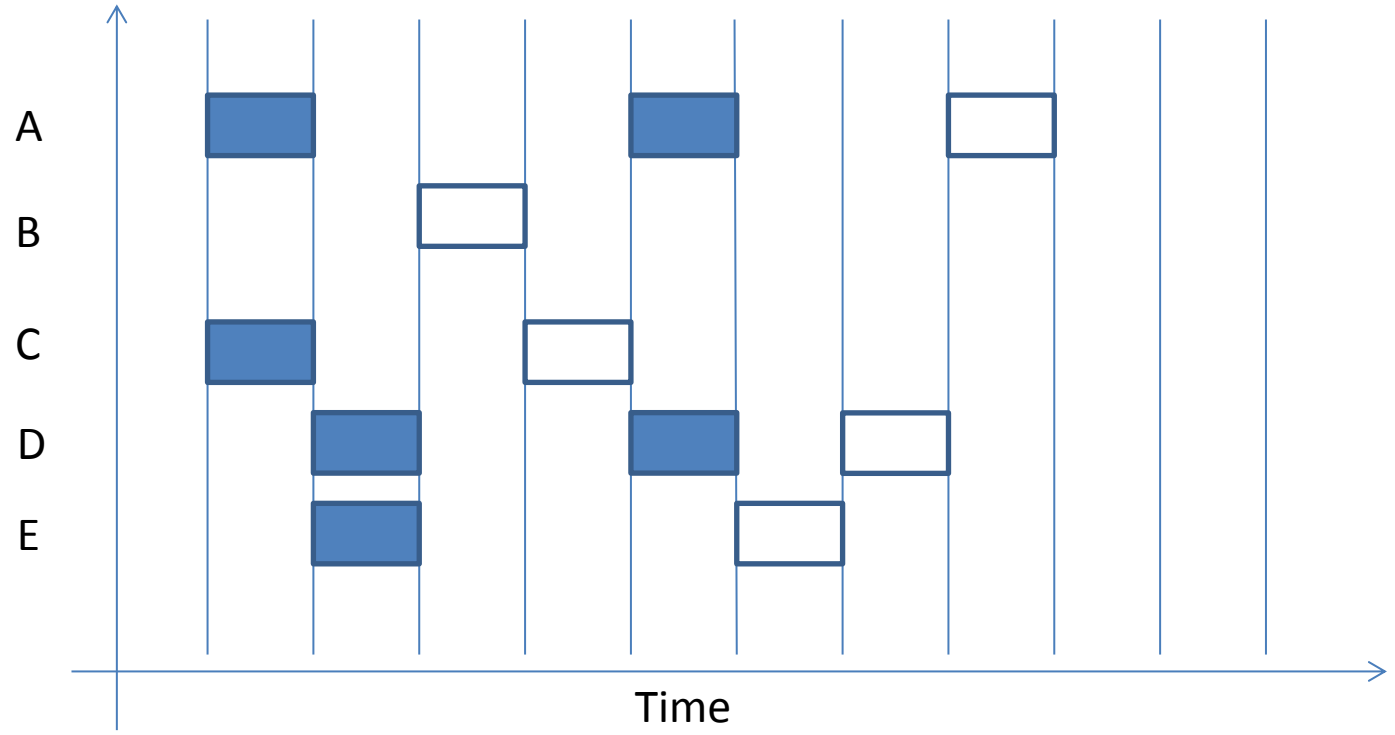


Slotted Aloha

- Slotted Aloha is an improvement to Aloha
- Nodes send traffic at the start of predefined timeslots
- This helps reduce collisions and thus enhance performances

Slotted Aloha example

- 5 competing nodes transmitting at the start of timeslots

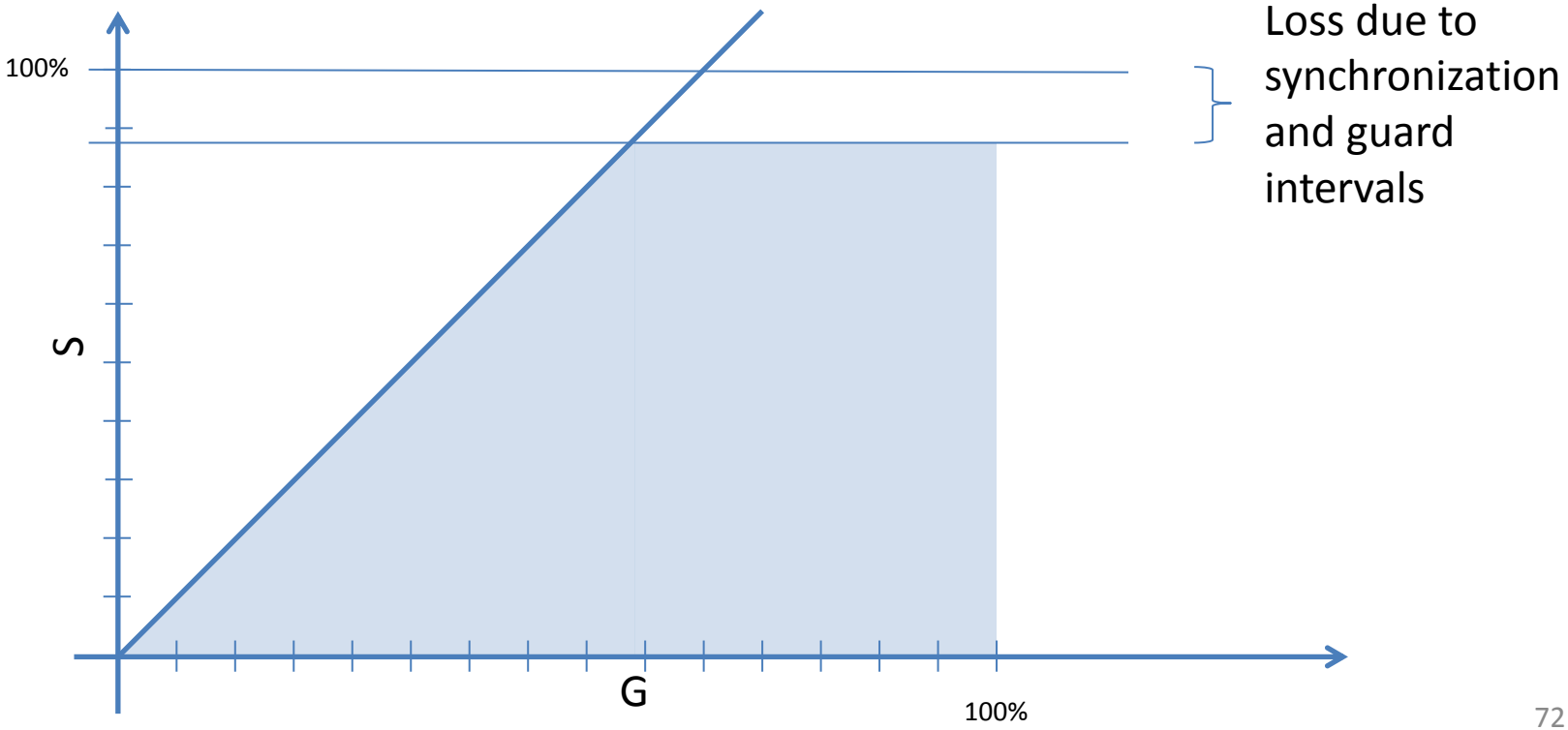


How to evaluate a MAC protocol?

- Important factors:
  - G: represents the offered load, the quantity of traffic that needs to be sent
  - S: represents the throughput, the quantity of traffic that the network was able to send
  - D: represents the delay, the time that separates the instant that a frame is given to the MAC layer and the instant that it is sent
  - Jitter: represents the variation in the delivery delay

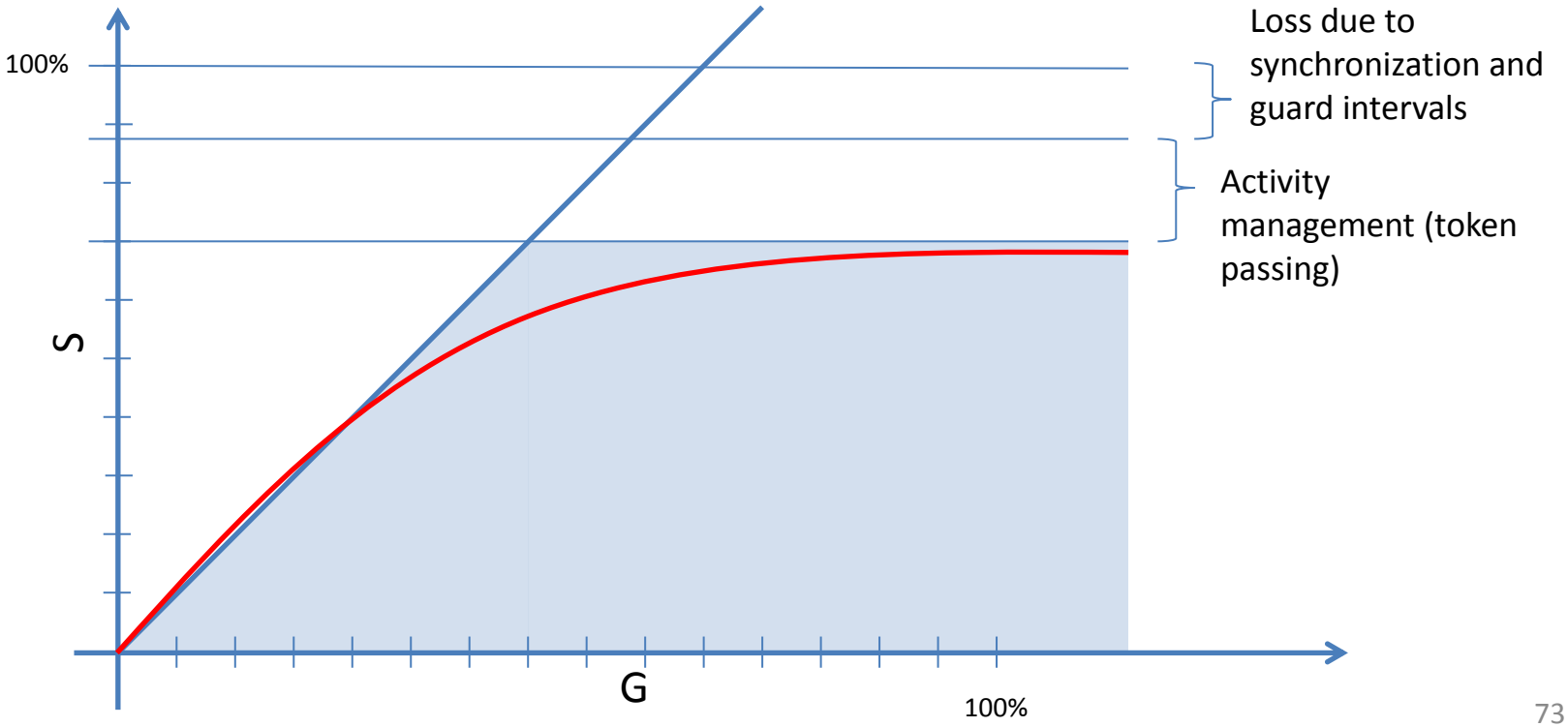
Ideal performance

- An ideal non existent MAC protocol should be able to send all the offered load correctly



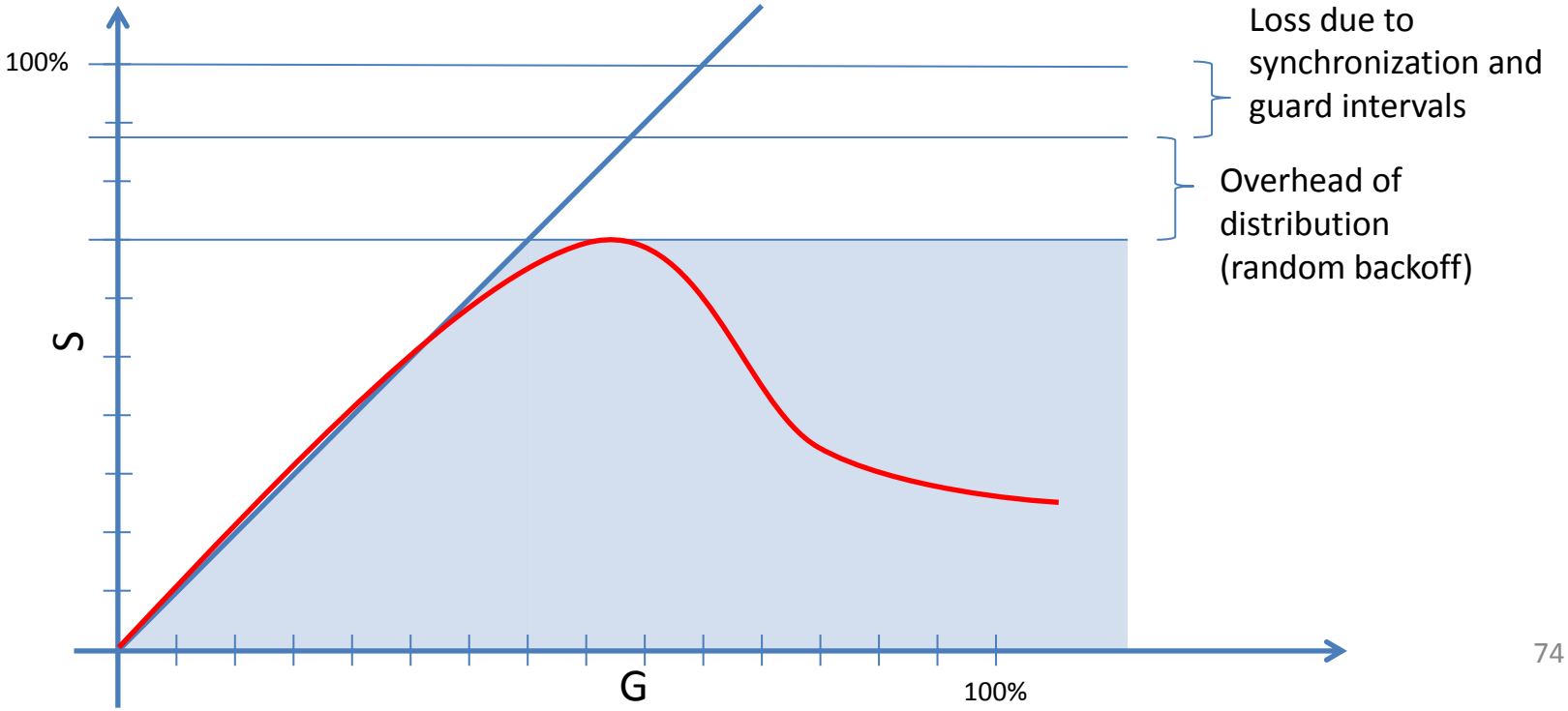
Performance of a deterministic MAC protocol

- The network reaches a saturation point where it cannot absorb the offered load anymore



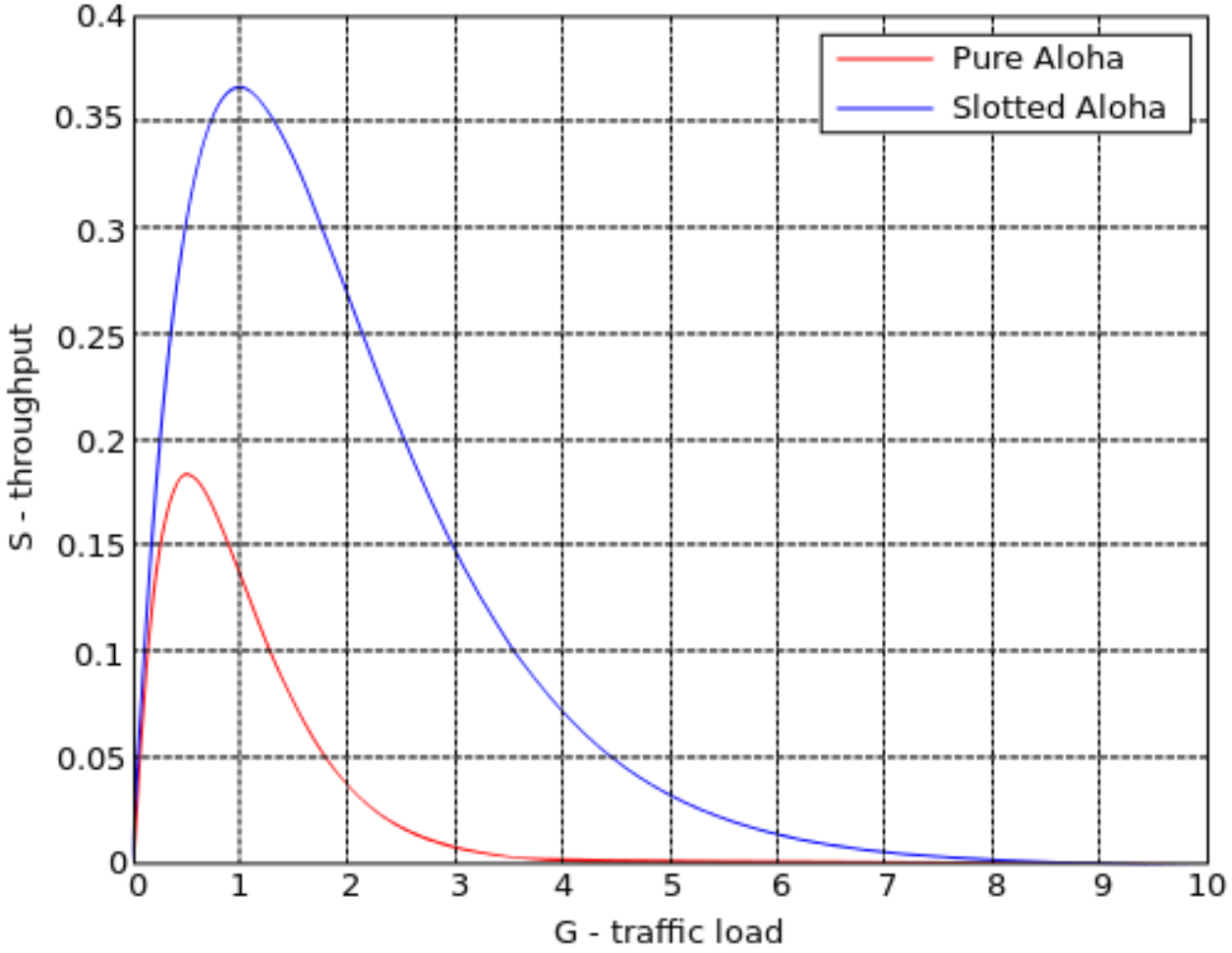
Performance of a probabilistic MAC protocol

- The network reaches a saturation point where it cannot absorb the offered load anymore, and then it starts to decrease if the offered load continues to increase



Aloha performance

(source wikipedia)



Modeling of Aloha

- Assumptions:
  - All frames have the same length
  - Packet loss is only due to collisions, no packet loss due to the medium behavior
  - All FIFOs are empty, nodes have only one frame to send at a time
  - The offered load respects a Poisson distribution (average behavior is known, but events are independent from one another. Knowing when the last event happened does not help us know when the next event will occur)

Probability of frame arrival (to be sent)

- According to Poisson distribution, the probability of *n* frames arriving during a period Δt:

  $P_n(\Delta t) = (\lambda)^n * e^{-\lambda(\Delta t)}/n!$

  - $\lambda(\Delta t)$: *average arrival rate of frames during* Δ
  - *n!: factorial of n*
  - *e* = 2.71828
- Since every node has only one frame to transmit at a time, we can consider *n* to be the number of competing nodes and λ to be the average number of nodes having a frame to send during Δt

Probability of frame arrival (to be sent)

- Examples:
  - The probability for 1 node to send during a period Δt is: $P_1 = (\lambda)^1 * e^{-\lambda} / 1! = \lambda * e^{-\lambda}$
  - The probability for 0 node to send during a period Δt is: $P_0 = (\lambda)^0 * e^{-\lambda} / 0! = e^{-\lambda}$

But in reality…

- Real measurements show that Aloha and Slotted Aloha are more efficient than what the theoretical results show
- This is essentially due to the fact that not all simultaneous transmissions lead to collisions
- Near far effect and capture effect

Channel Assessment

- Aloha protocol accesses the medium without testing its “availability”
- In order to check if other nodes are currently transmitting on the channel, a node should do a Channel Assessment
- This can help avoid accessing the medium when it is already occupied by other nodes

Listen Before Talk

- MAC protocols that make sure that the medium is clear before accessing use the technique known as Listen Before Talk
- This does not guarantee avoiding collision:
  - It is not the case for wired network
  - Even less, for wireless networks
- Propagation delay, limited communication range, unidirectional links, frequent simultaneous access, etc. make avoiding collisions very difficult

Carrier Sense

- Check if the channel is busy or not is the action of detecting the energy level on that particular channel
- If the energy level is above a certain threshold it is considered to be busy and a node should refrain from transmitting
- This operation is called Carrier Sensing, or Clear Channel Assessment (CCA)

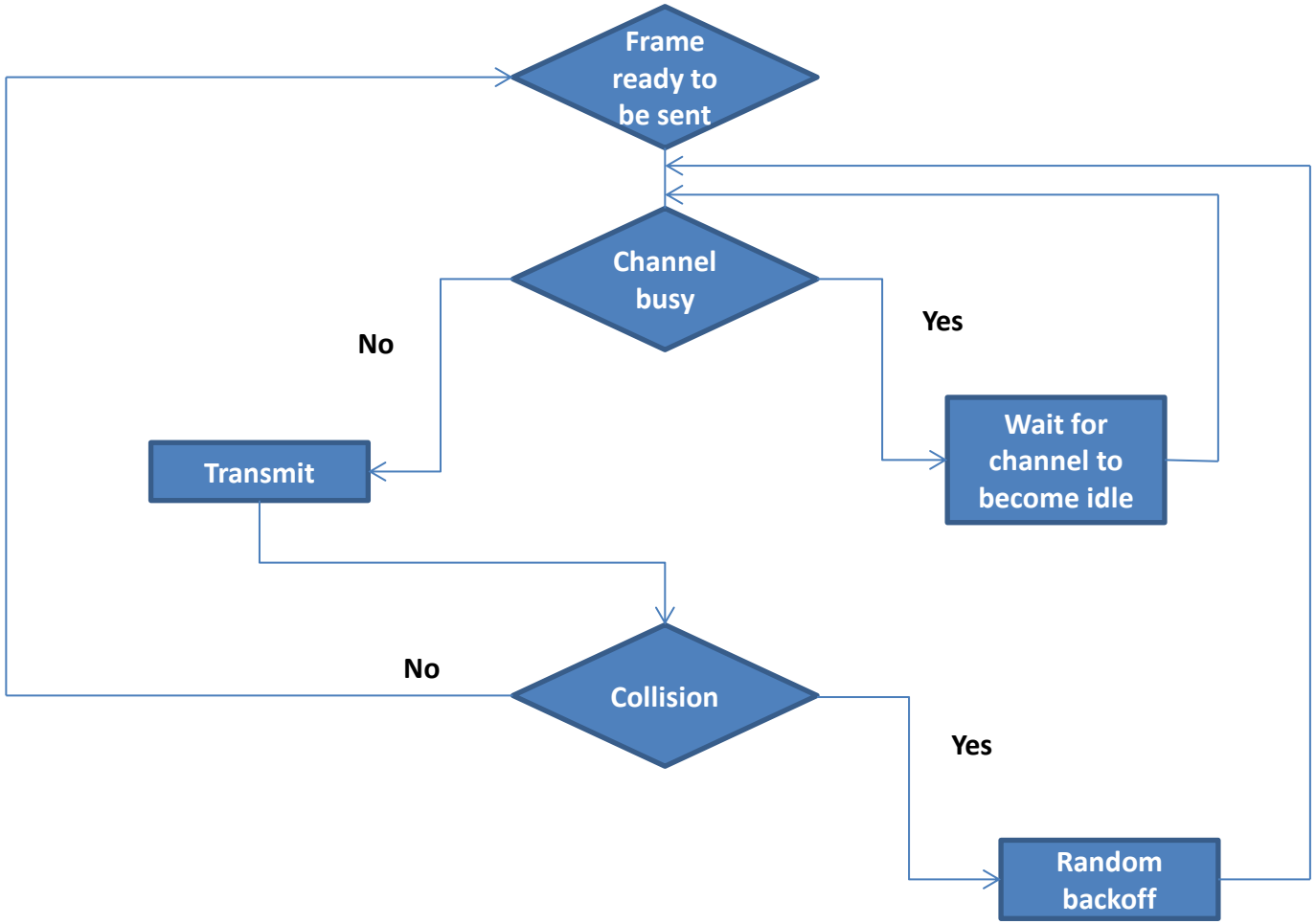
CSMA

- MAC protocols that are based on Carrier Sensing are called Carrier Sense Multiple Access MAC protocols
- Ethernet uses a type of CSMA protocol called CSMA/CD (for Collision Detection)
- Ethernet suffers from collisions whenever multiple stations share the same “collision domain” because of simultaneous transmissions

Persistence in CSMA

- A CSMA MAC protocol is said to be 1-persistent in the following case (this is the case for CSMA/CD):
  - When a node is ready to transmit, it checks if the channel is busy
  - If so, the node then senses the channel continuously until it becomes idle
  - Once idle, the node transmits a frame
  - In case of a collision, the node waits for a random period of time before it reattempts to transmit again

1-persistent CSMA



P-persistent CSMA

- In P-persistent CSMA, a node will not transmit once the medium is no longer busy
- Instead, the node decides to transmit with a certain probability *p*, and not to transmit with a probability *(1 – p)*
- WiFi uses a variant of P-persistent CSMA

Non-persistent CSMA

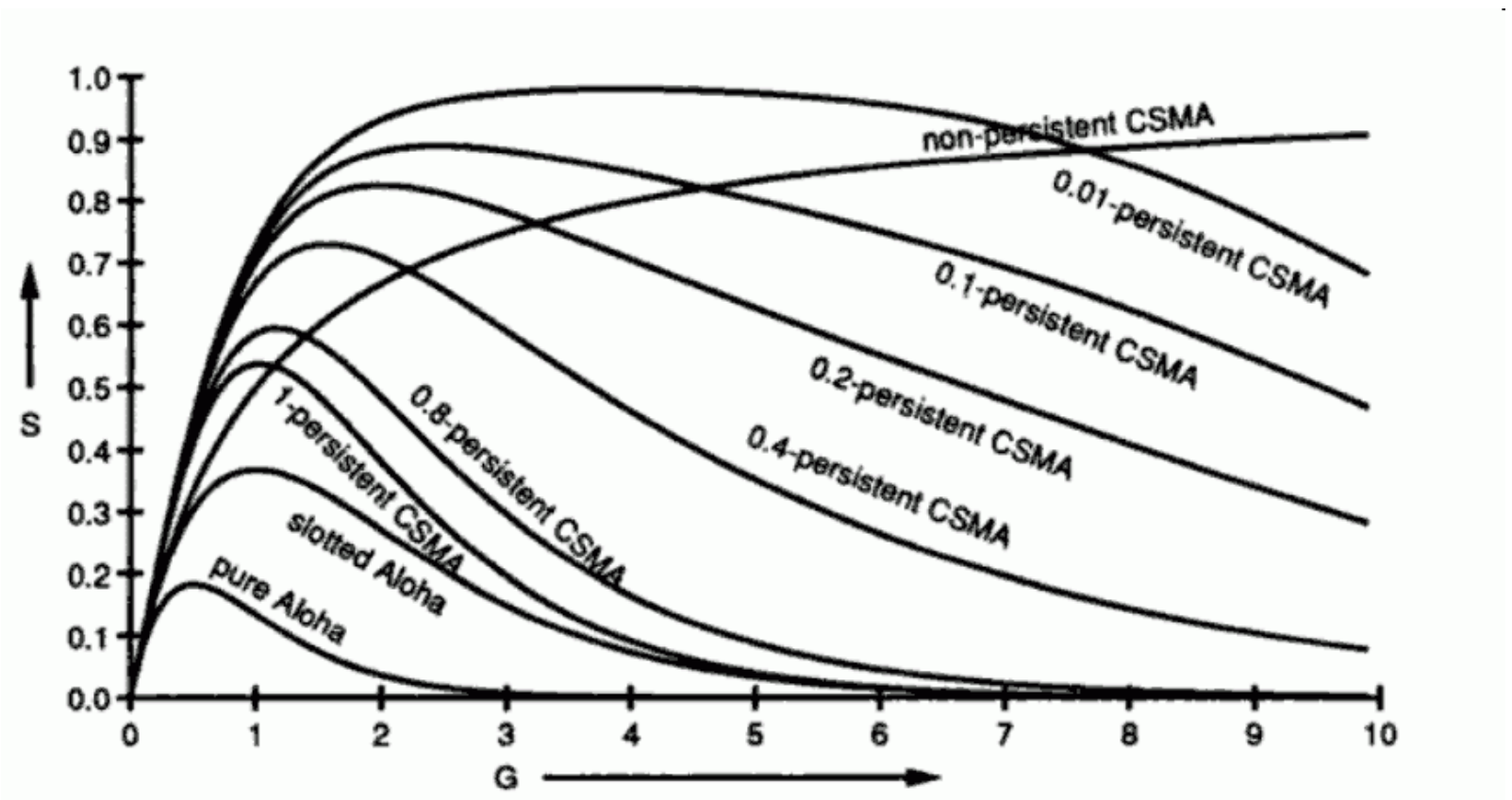
- In Non-persistent CSMA, a node does not continuously sense the channel until it becomes idle
- When the node finds the channel busy, it waits for a random backoff and then resenses the channel
- If it finds the channel idle, it starts transmitting

Summary on persistence

- 1-persistent CSMA leads to a collision when 1 node is transmitting and 2 or more nodes want to access the medium: good for lightly loaded network
- Non-persistent reduces collision risk thanks to the random backoff but uses less often the channel: good for heavily loaded network
- P-persistent is a trade-off and depends on the probability used for transmission
- Sensing the channel is only useful when the propagation delay is very small compared to the transmission duration

Performance of CSMA

(source http://www.mathcs.emory.edu/~cheung/Courses/455/Syllabus/3a-MAC/csma.html)



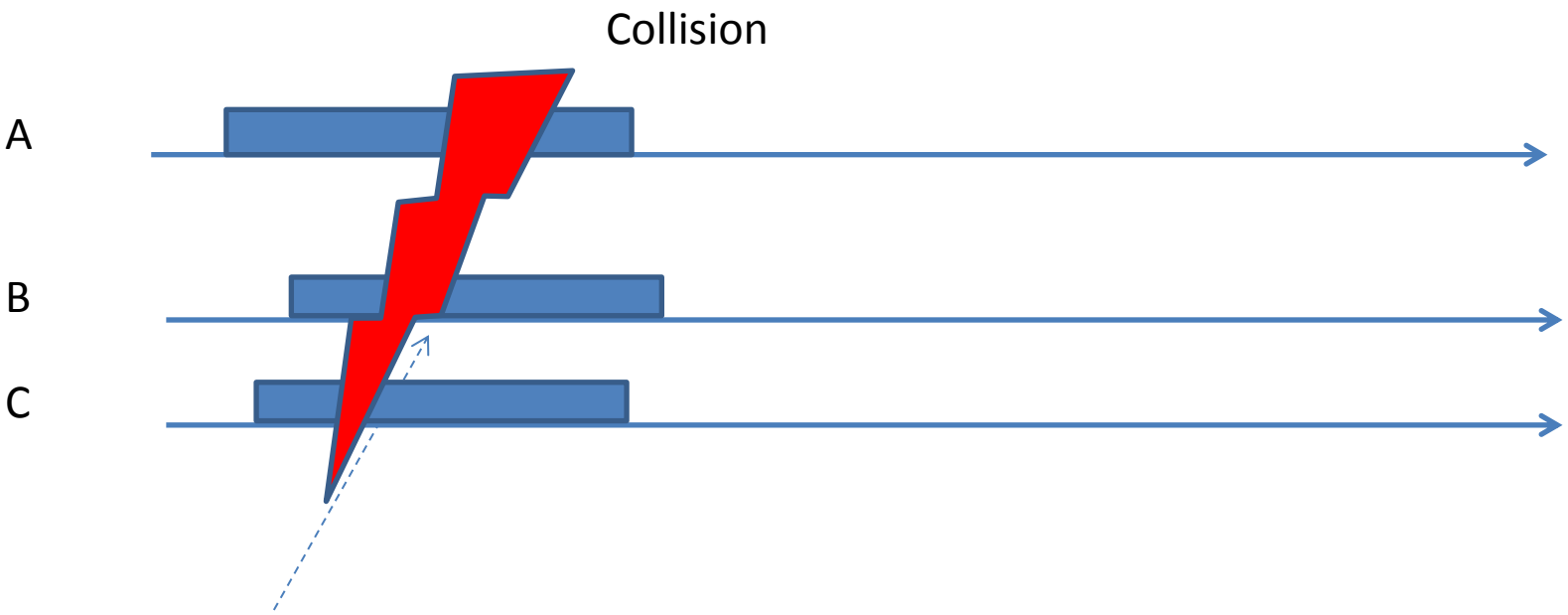
The case of IEEE 802.3 (Ethernet)

- CSMA/CD used by Ethernet is a 1-Persistent CSMA protocol → Collisions are synchronized
- When collisions are detected, a random backoff algorithm is used to dynamically resolve conflicts
- After the n^{th} collision, a node chooses a random value from the interval [0; $2^n - 1$], where n = *Min[n, 10]*
- After the 16^{th} collision the packet is dropped

Exercises on Aloha and CSMA

- Using an activity diagram, explain what happens when a node is currently transmitting and 2 other nodes want to access the channel for the following MAC protocols:
  - Aloha
  - Slotted Aloha
  - CSMA 1-Persistence
  - CSMA non-Persistent
  - CSMA 0.5-Persistence

Solution for Aloha

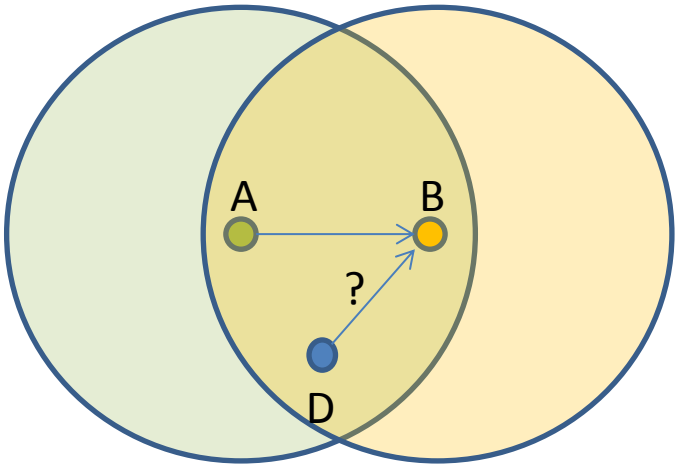


CSMA and communication range

- Testing the availability of the medium does not necessarily give an accurate state of the channel
- This is essentially due to the communication range of nodes and multi-path fading
- The relative positions of senders and receivers are very important factors

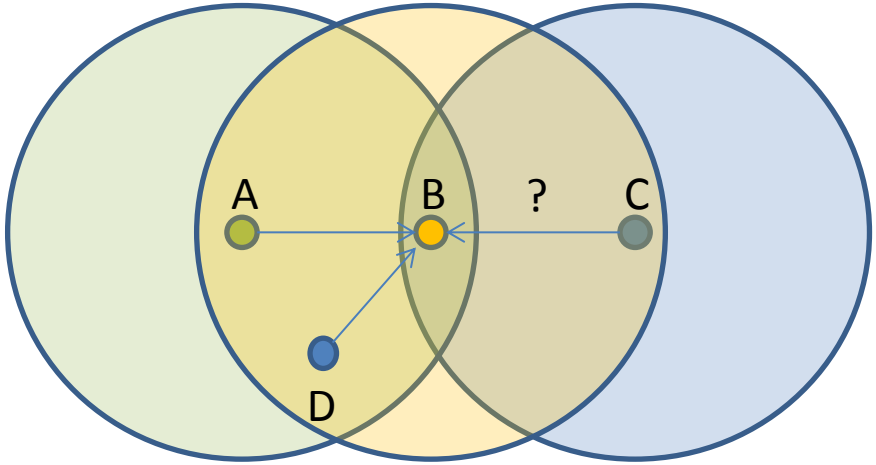
Hidden Terminal (1)

- A is currently sending a message to B, D wants to send a message to B using CSMA/CA
- D is able to receive the signal A is sending because it is in range of A
- Result: D detects a busy channel and refrains from sending the message



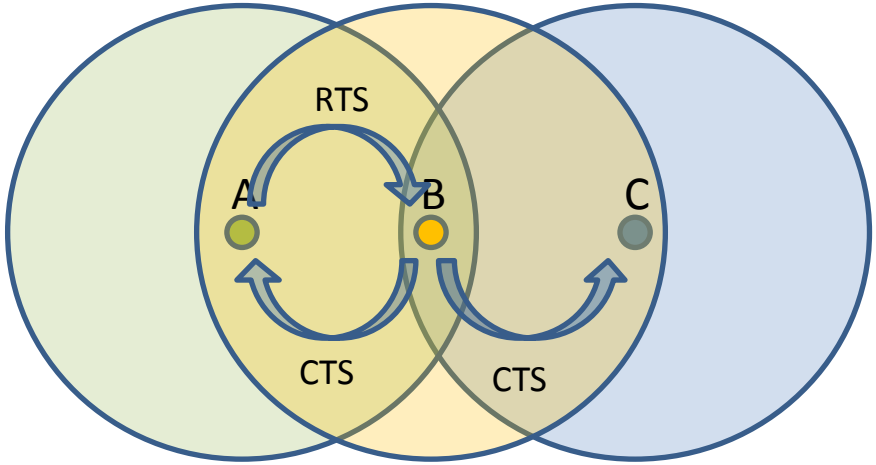
Hidden Terminal (2)

- Now node C wants to send a message to B while A is transmitting
- C is unable to detect A's activity because it is out of range and cannot receive A's signal
- Result: C detects an idle medium and sends its message



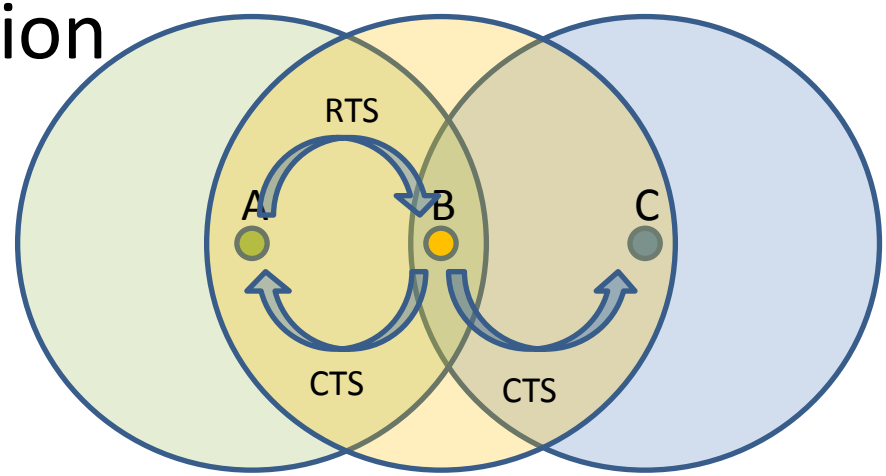
Hidden Terminal solution: RTS/CTS (1)

- Before starting a transmission, the sender (A) sends an RTS (Request To Send) message asking if the receiver (B) is available
- If the receiver is available, it replies with a CTS (Clear To Send) message



Hidden Terminal solution: RTS/CTS (2)

- When C hears the CTS sent by B it knows that the medium will be busy by the transmission between A and B
- C refrains from sending by considering the medium busy for the duration of the transmission

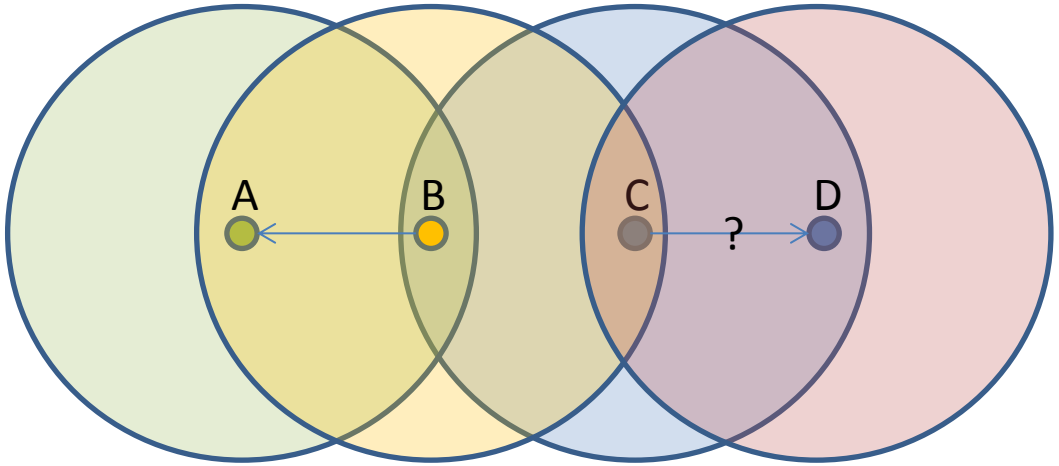


NAV: Network Allocation Vector

- When a node receives a CTS it is able to know for how long the transmission is going to last
- A NAV is used to help a node knows when the medium is busy without doing a CCA
- It is referred to as Virtual CCA

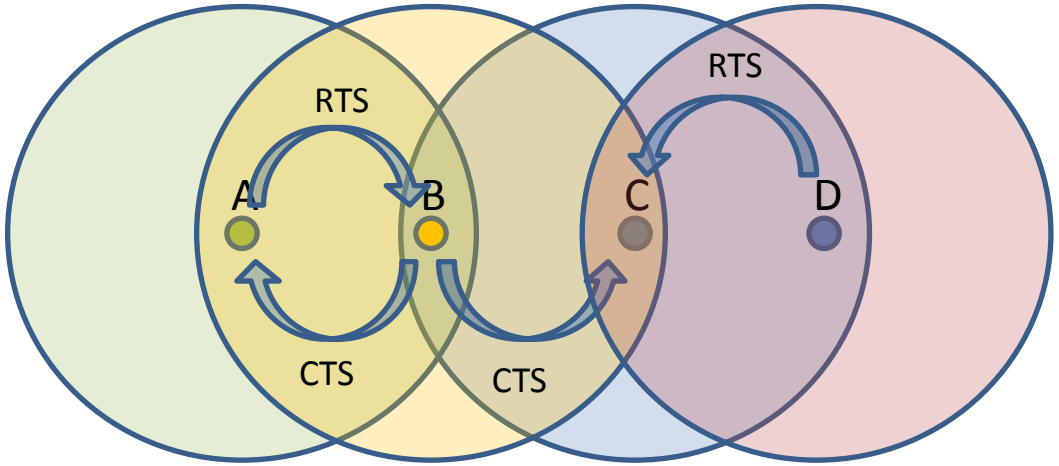
Exposed Terminal example

- If node B is sending a message to node A, C is able to detect its activity and thus CSMA forces C to refrain from sending
- Even though C is able to send data to D without interfering with the reception on node A



Exposed Terminal continues

- The RTS/CTS exchange enhances even more the Exposed Terminal problem
- When C receives the CTS sent by B, it concludes that the medium is busy, thus it will refrain from replying to an RTS sent by D



Exposed Terminal

- The Exposed Terminal problem prevents nodes from exchanging messages even though their transmissions do not interfere with other simultaneous transmissions
- This leads to degradation of node's throughput

Part 3:
WiFi/IEEE 802.11

IEEE 802.11

- The IEEE 802.11 standard was first released in 1997 by the LAN/MAN group (802) of IEEE
- It defines the MAC and Physical layers for WLANs
- It is adopted by WiFi for both layers
- The first widely used version of the standard is IEEE 802.11b 1999 at 2 Mbit/s with Complementary Code Keying for higher rates (up to 11 Mbit/s) but lower range
- Followed by IEEE 802.11g and 802.11a

Main differences

- 802.11b and g work in the 2.4GHz band, whereas 802.11a works in the 5GHz band
- b uses a DSSS technique at the physical layer, whereas a and g use OFDM
- Maximum data rate for b is 11 Mbit/s, g and a can reach 54 Mbit/s

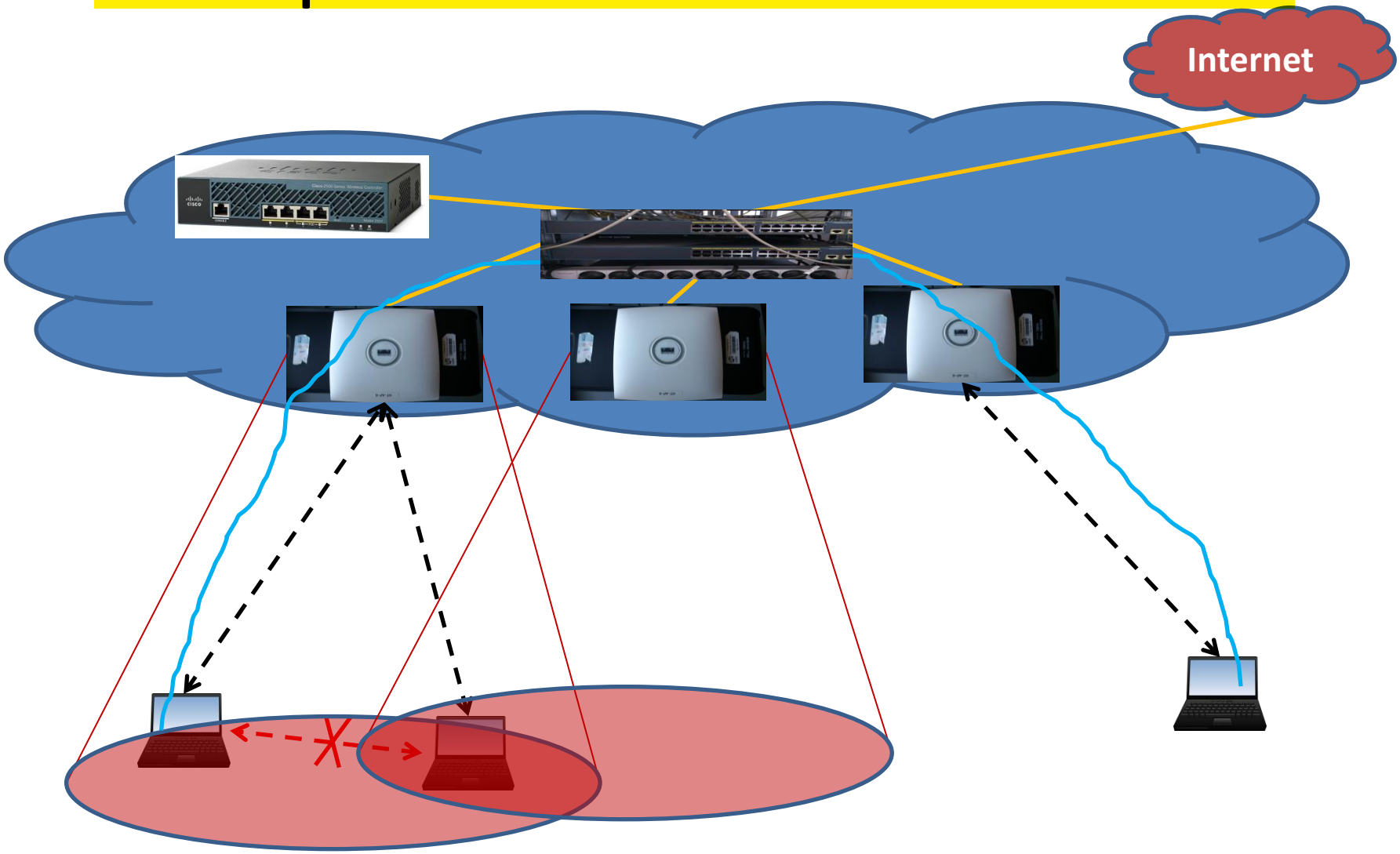
Today

- WiFi is widely used in the 2.4 GHz and 5 GHz bands → New band has opened in 2013 in the 60 GHz
- New versions with better antennas for concentrating transmissions towards the destinations in order to limit the interference coverage (beam forming)

Network architecture

- The network is organized into cells, each Access Point (AP) manages its own cell
- Some APs can be configured to take over when other APs fail
- APs part of the same network are generally interconnected with Ethernet links
- Two types of topologies: Infrastructure (widely used) and Ad Hoc (802.11s)

Example of a WiFi infrastructure



Physical layer of 802.11

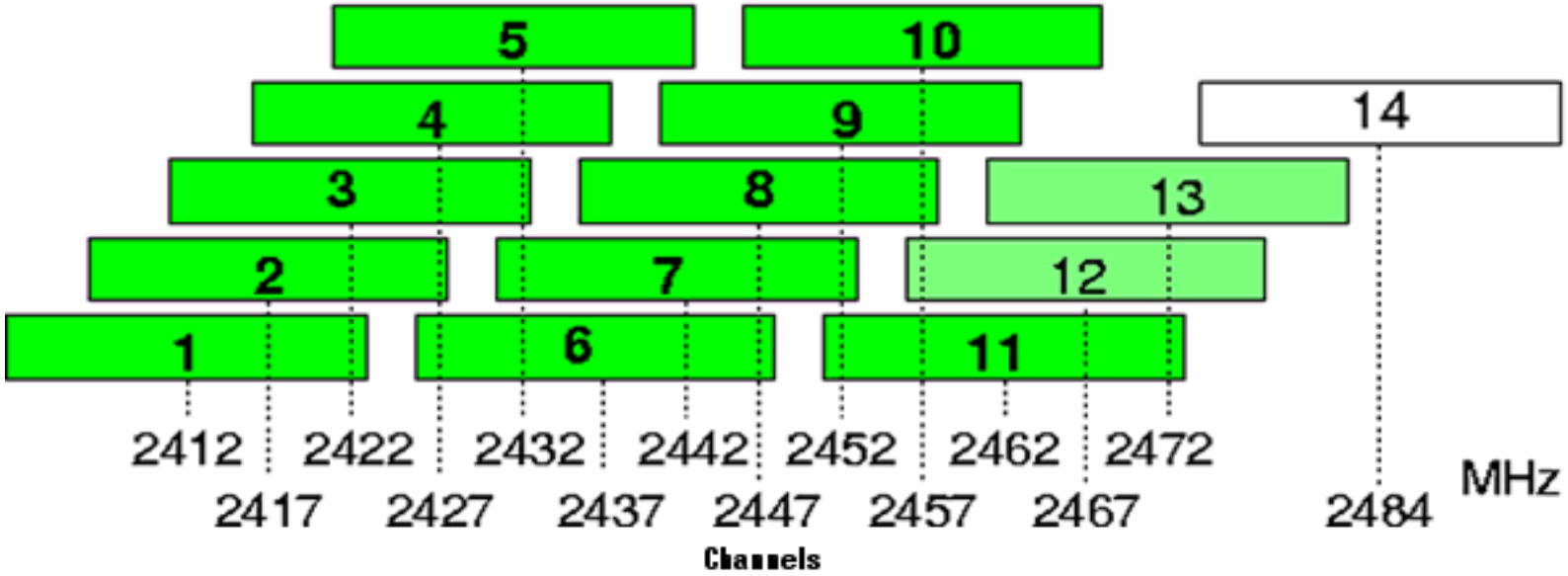
- Originally, the physical layer of 802.11 supported 3 modes:
  - Infrared: has not been successful due to public rejection
  - FHSS: is rarely used today because it requires more bandwidth when data rate is increased
  - DSSS: this is the most successful implementation for WLANs
- It is divided into 2 sublayers:
  - PLCP: Physical Layer Convergence Protocol, its role is to prepare and parse sent and received data units
  - PMD: Physical Medium Dependent, its role is to transmit/modulate and receive/demodulate signals

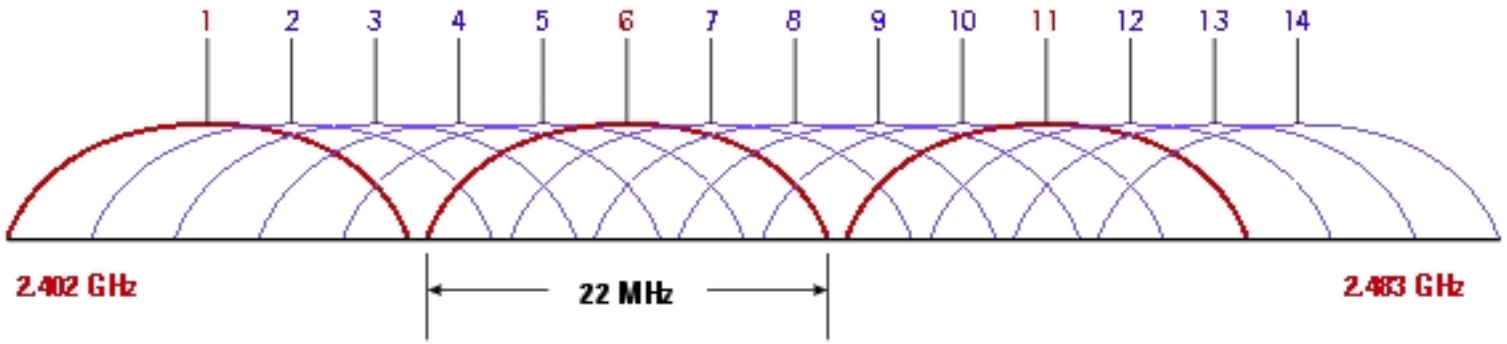
DSSS

- Direct Sequence Spread Spectrum transmission technique helps transform the signal after a multiplication with a pseudo random sequence (PRN) into a noise like signal almost undetectable by receivers that do not know the random sequence
- The use of different PRNs makes it possible to have simultaneous non-interfering signals using the same frequency band (but this is not used in WiFi)

Channels in DSSS

(source http://www.netstumbler.org/hardware/channel-diagram-explanation-t20721.html)





DSSS of 802.11b

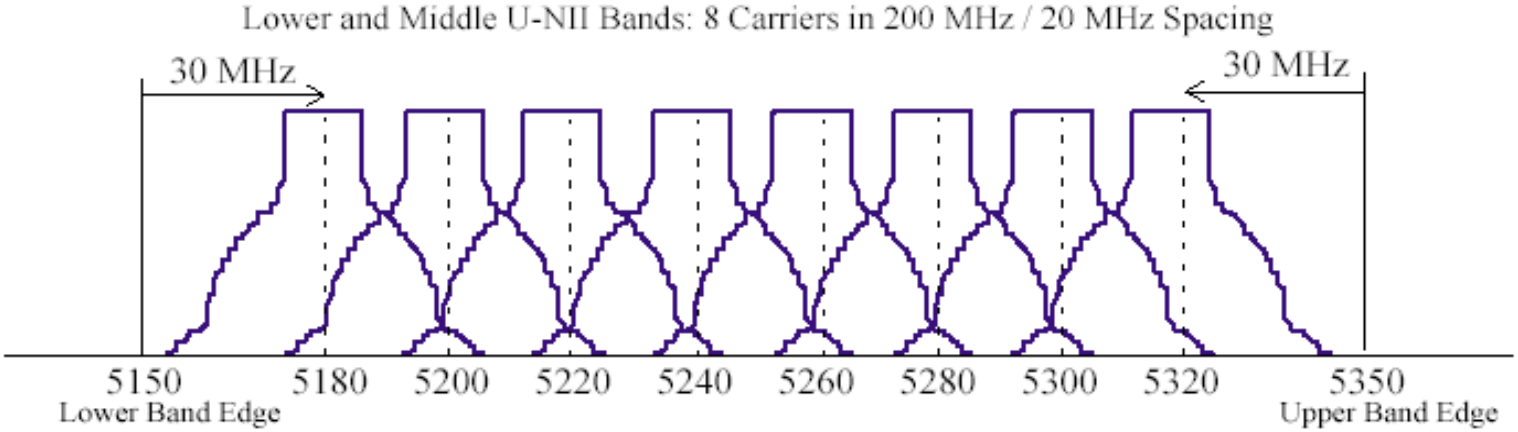
- The use of CCK allowed 802.11b to reach 11Mbps thanks to shorter chipping sequences (from 11 bits in Barker Code to 8 bits in CCK)
- 4-bit symbols at 5.5Mbps, 8-bit symbols at 11Mbps
- It falls back to lower rates depending on the link quality (lower rates help make the link stronger)

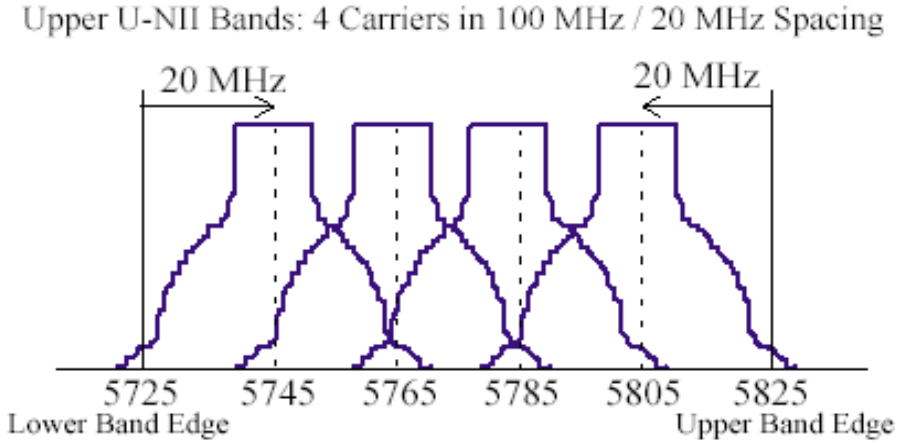
OFDM of 802.11a

- 802.11a can reach 54 Mbit/s and works in the 5GHz frequency band: 5.15GHz - 5.35GHz and 5.725GHz - 5.825Ghz
- 802.11a has 12 overlapping channels but the coding technique makes it possible to use consecutive channels without interfering

OFDM channels

(source Denis Bakin, http://www.okob.net/texts/mydocuments/80211physlayer/)



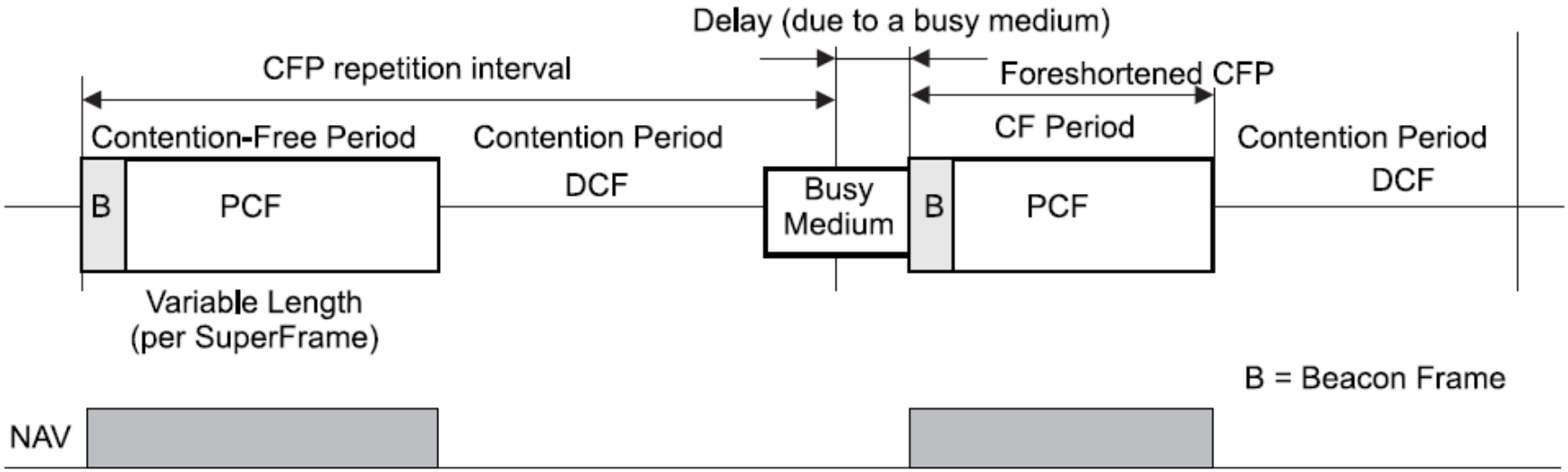


802.11 MAC layer: DCF and PCF

- Distributed Coordination Function (widely used mode):
  - Operates using CSMA/CA
  - RTS/CTS messages for long messages (optional, it can be used for all frames)
  - Stations apply virtual channel sensing by the means of duration fields in RTS, CTS and Data frames (discussed later on)
- Point Coordination Function (rarely implemented):
  - Access point manages when each station is allowed to send
  - Allows collision free transmissions
  - PCF rules shall be applied by all stations (by means of updating their NAVs, discussed later on)
  - RTS/CTS are not used for Contention Free access
  - It is built on CSMA/CA of DCF

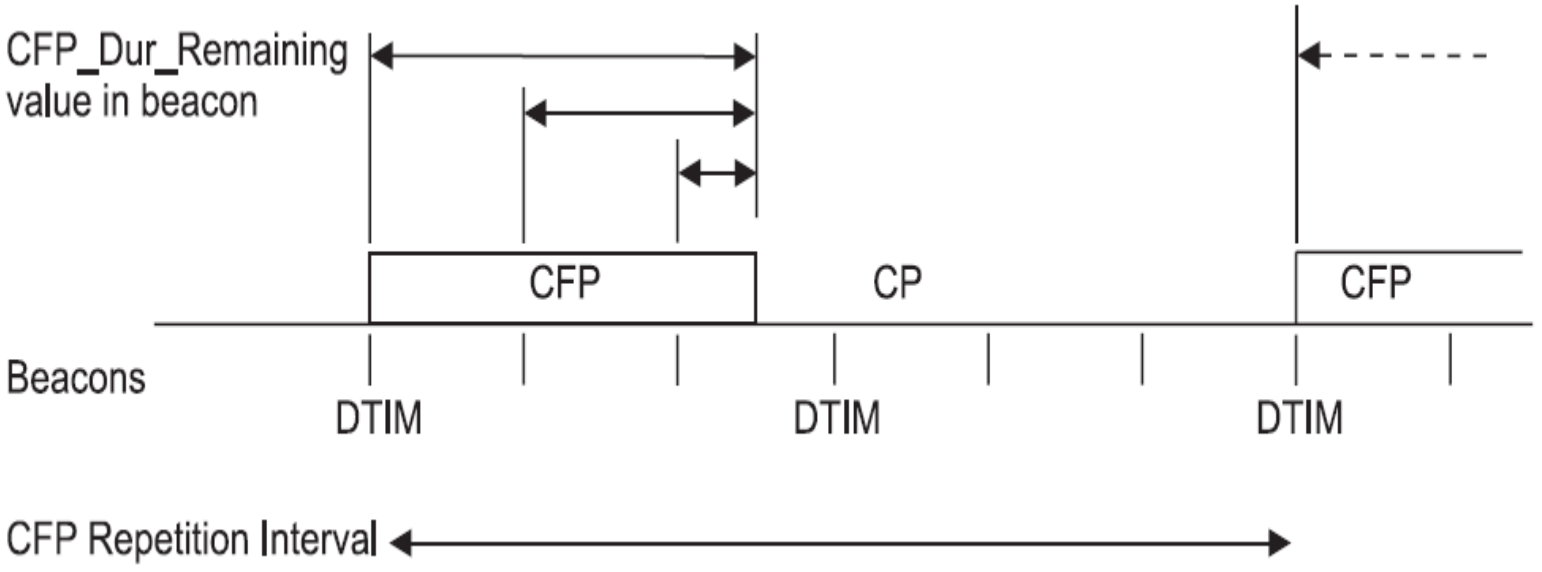
PCF and DCF alternation

- Beacons shall contain DTIM information (Delivery Traffic Indication Message)
- Beacons might be delayed by DCF transmissions



DTIM, beacons and CFP example

- CFP maxDuration = 2,5 beacon intervals
- DTIM interval = 3 beacon intervals
- CFP interval = 2 DTIM intervals



CSMA/CA of 802.11

- CSMA/CA algorithm for accessing the channel in a decentralized manner (used in the DCF mode)
- It is based on:
  - CCA tests before transmitting
  - Desynchronizing transmissions using a random backoff
  - Frame spacing to separate consecutive frames

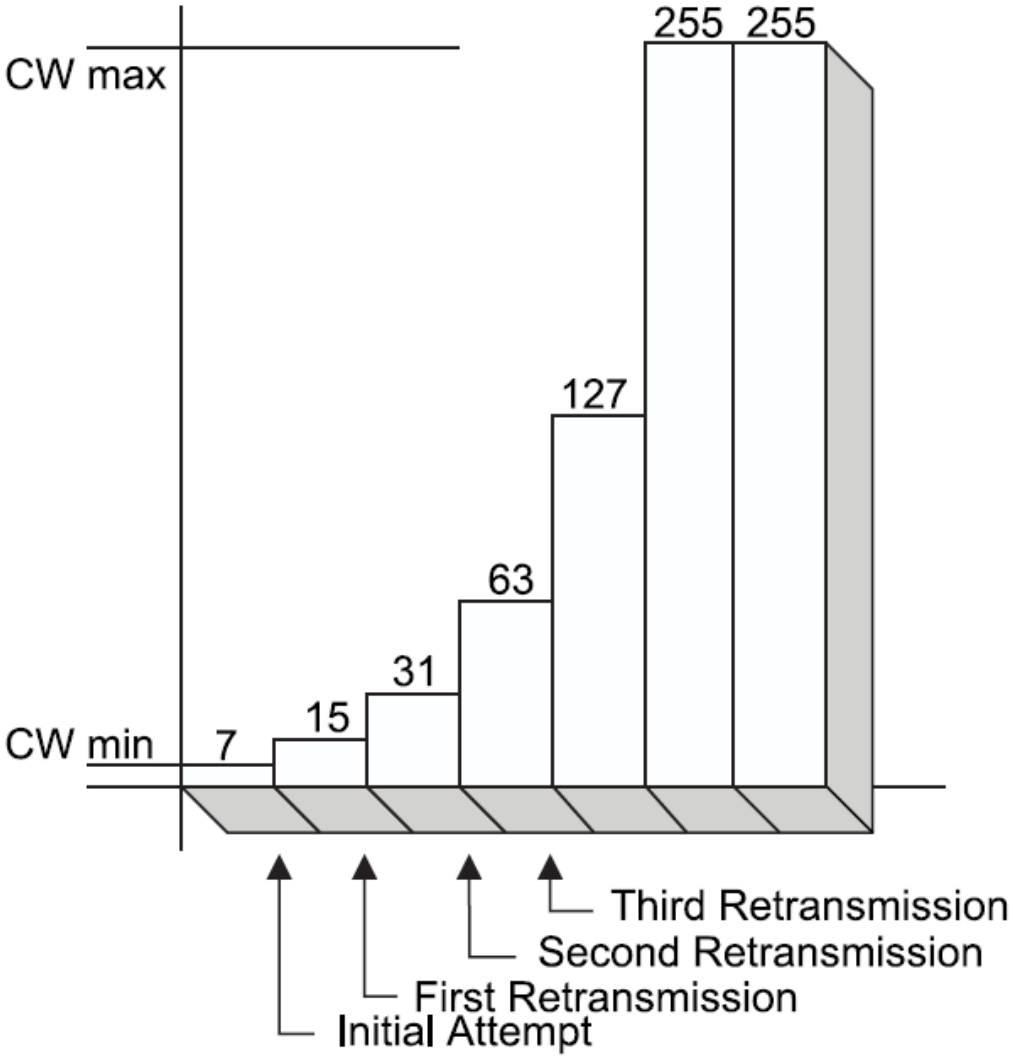
CSMA/CA Algorithm (1)

- When a station wishes to send a frame it has to wait for the medium to be idle for a DIFS (DCF Inter-Frame Spacing) duration
- In case the channel is found busy, the station shall defer its transmission until the medium is idle for a DIFS duration in case the last transmission was successful, or for a EIFS (Extended IFS) if the last transmission was unsuccessful

CSMA/CA Algorithm (2)

- After the DIFS or the EIFS, the station chooses a random backoff
- A backoff is a number of slot times
- This number is drawn from a uniform distribution over the interval [0 ; CW], $CW = 2^{be} - 1$
- Where CW is the Contention Window
- $minCW \leq CW \leq maxCW$
- CW starts at minCW and *be* is incremented after each retry until CW reaches maxCW

maxCW evolution



CSMA/CA Algorithm (3)

- During the backoff, when the medium is idle for a slot time, the drawn value is decremented
- When the medium is detected busy, the backoff is suspended, the station waits for the medium to be idle for a DIFS or EIFS before the backoff procedure is allowed to proceed
- The transmission shall start when the backoff reaches 0

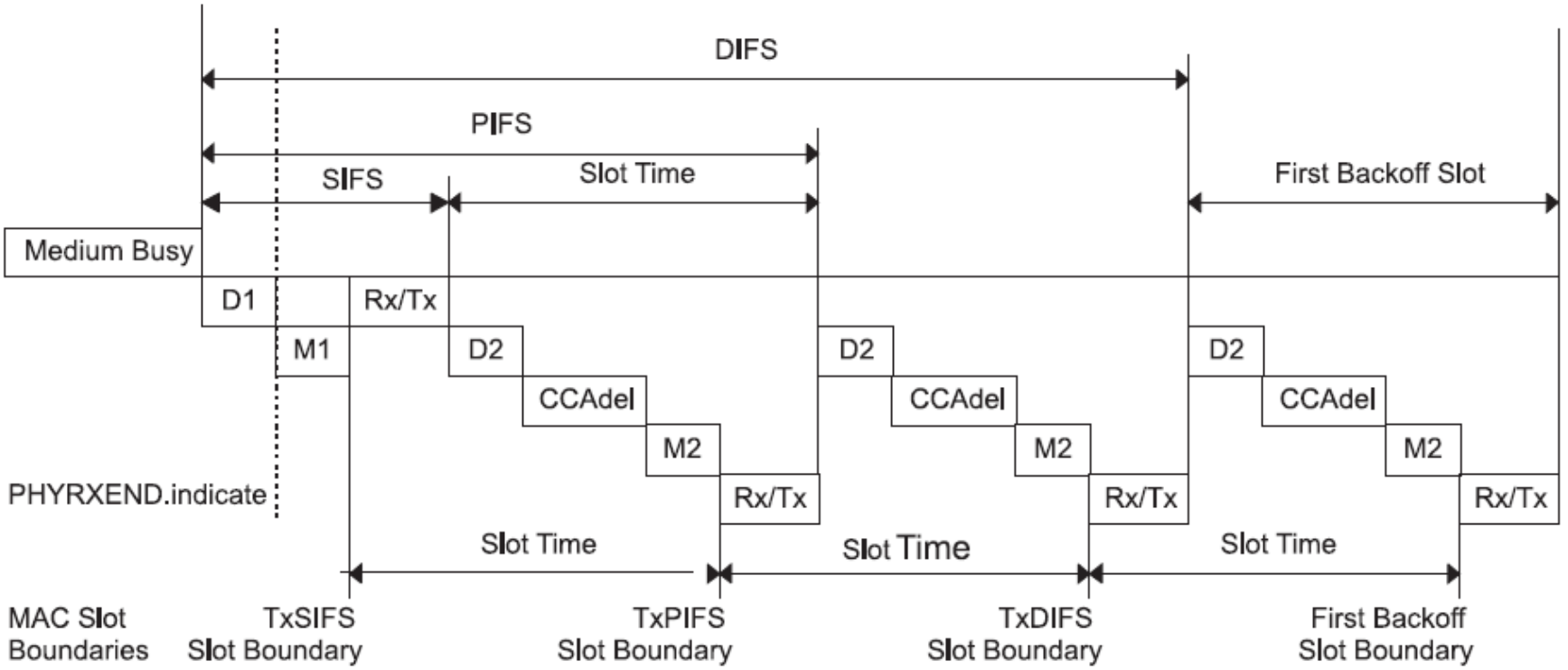
IFS types (1)

- The duration of IFSs are defined based on the PHY characteristics
- SIFS: Short IFS is used for ACK, CTS, fragments of frames, responses to a polling in PCF mode, all frames sent during CFP (Contention Free Period). It helps give priority for finishing a frame exchange that has already contented and won the medium
- PIFS: PCF IFS is used in PCF mode. It gives priority at the start of a PCF period for stations to access medium without contention

IFS types (2)

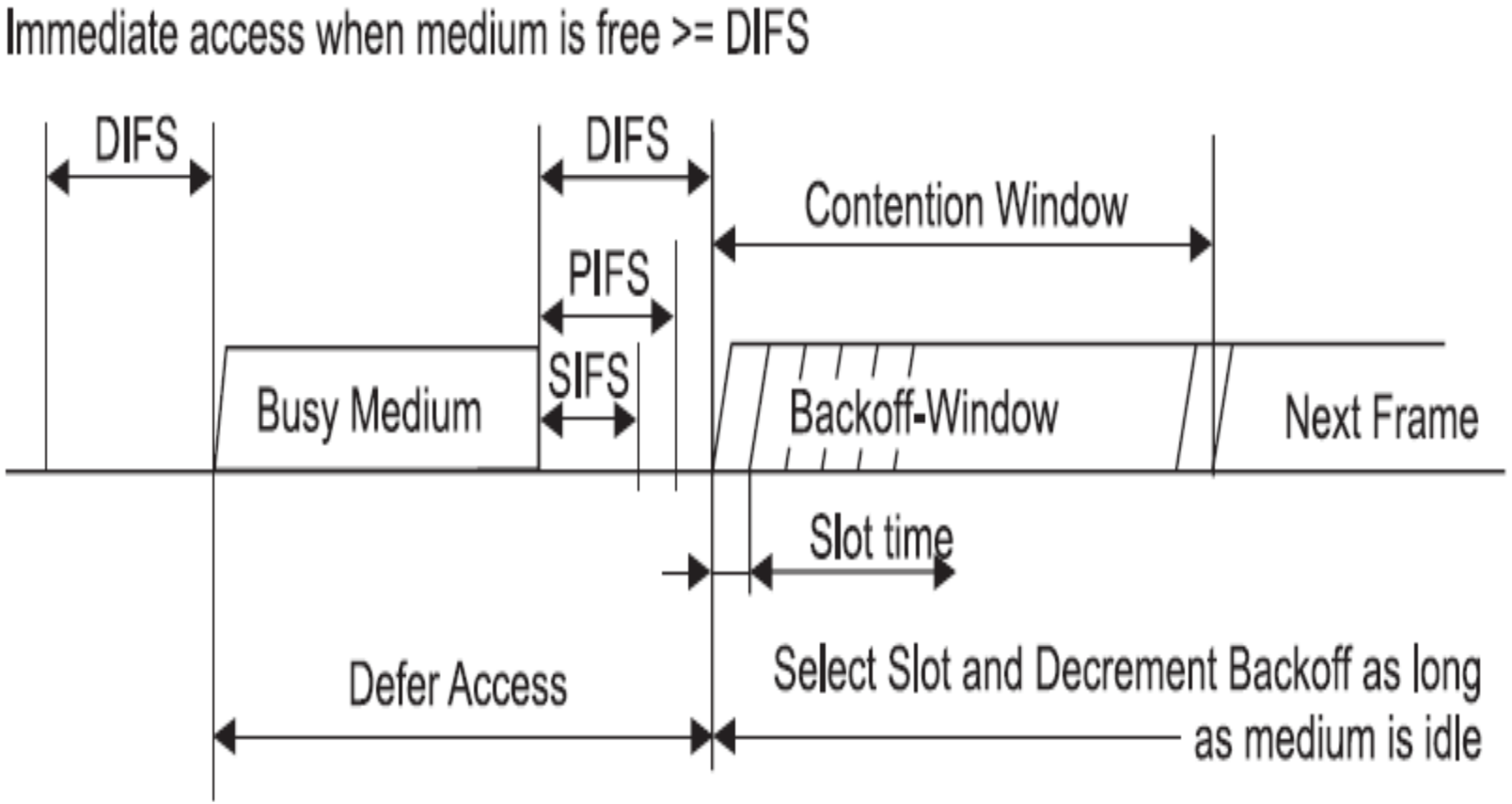
- DIFS: DCF IFS is used for first transmissions of a frame
- EIFS: Extended IFS is used when retransmitting a frame that already accessed the medium and resulted in an transmission error
- PIFS = SIFS + 1 slot time
- DIFS = SIFS + 2 slot times
- EIFS = SIFS + 8*ACKtime + aPreambleLength + aPLCPHeaderLength + DIFS (durations are calculated for 1 Mbit/s)

IFS timings

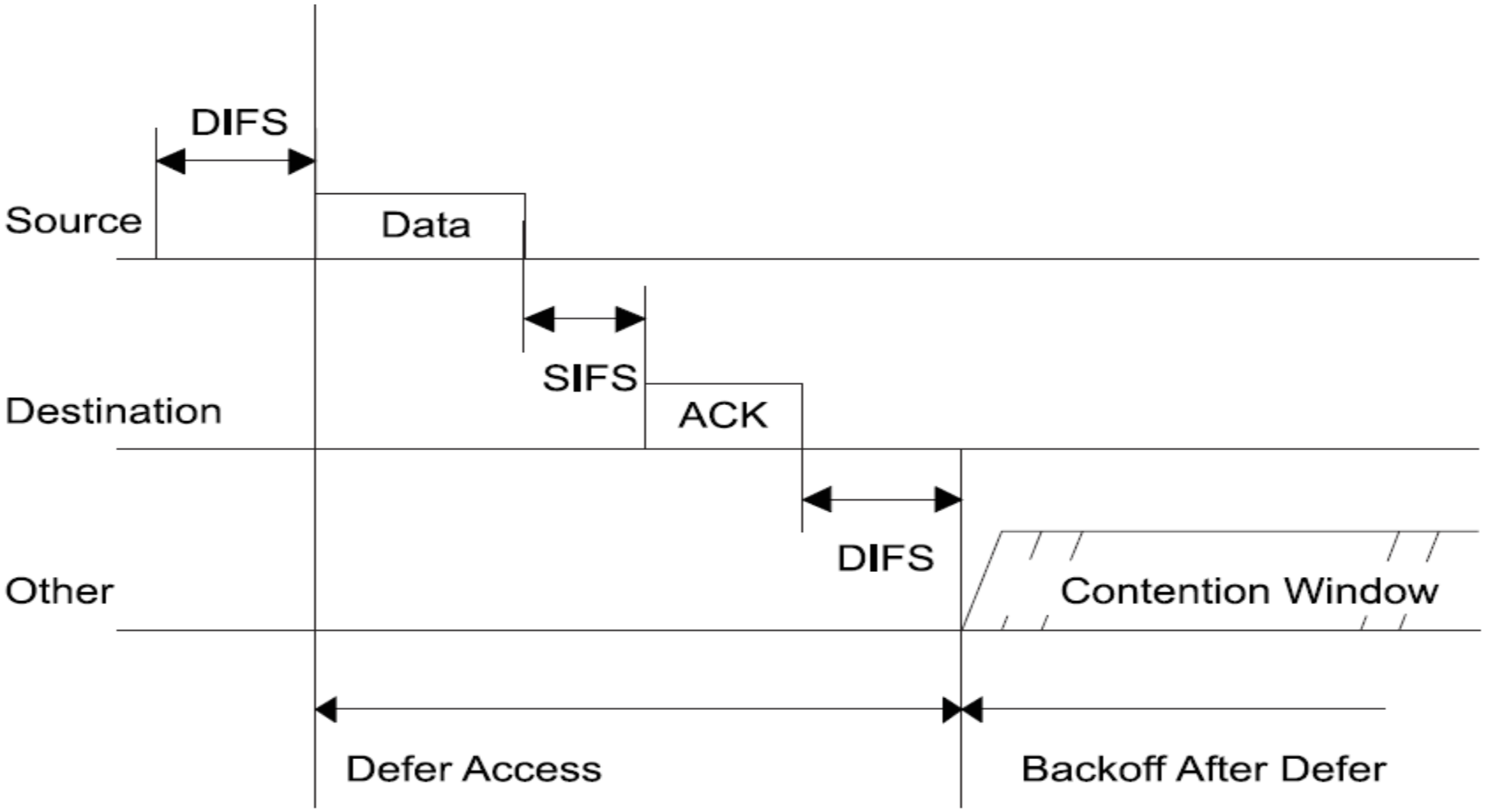


D1 = aRxRFDelay + aRxPLCPDelay (referenced from the end of the last symbol of a frame on the medium)
D2 = D1 + Air Propagation Time
Rx/Tx = aRXTXTurnaroundTime (begins with a PHYTXSTART.request)
M1 = M2 = aMACPrcDelay
CCAdel = aCCA Time - D1

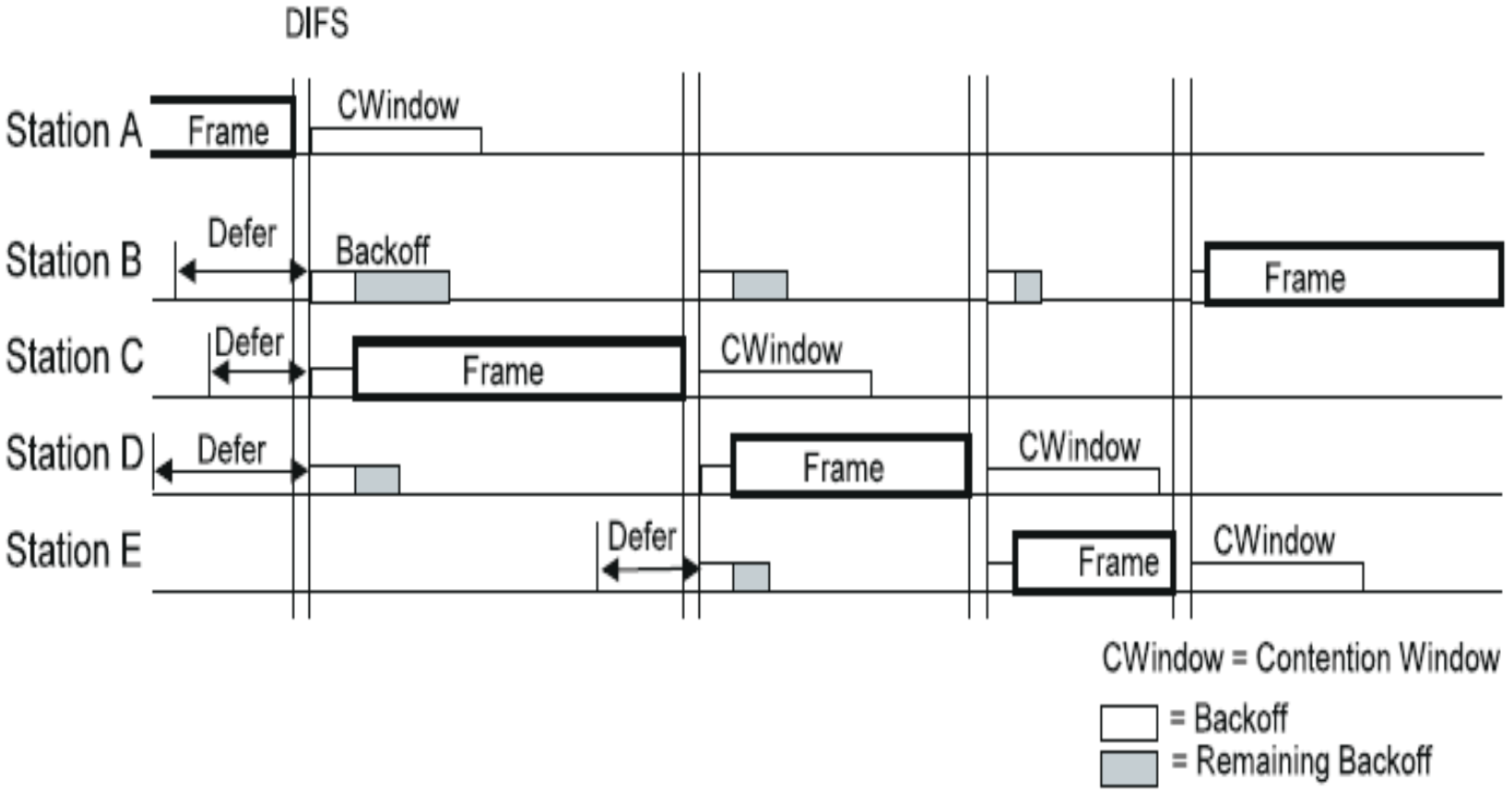
Inter-Frame Spacing



Frame exchange example



Backoff example



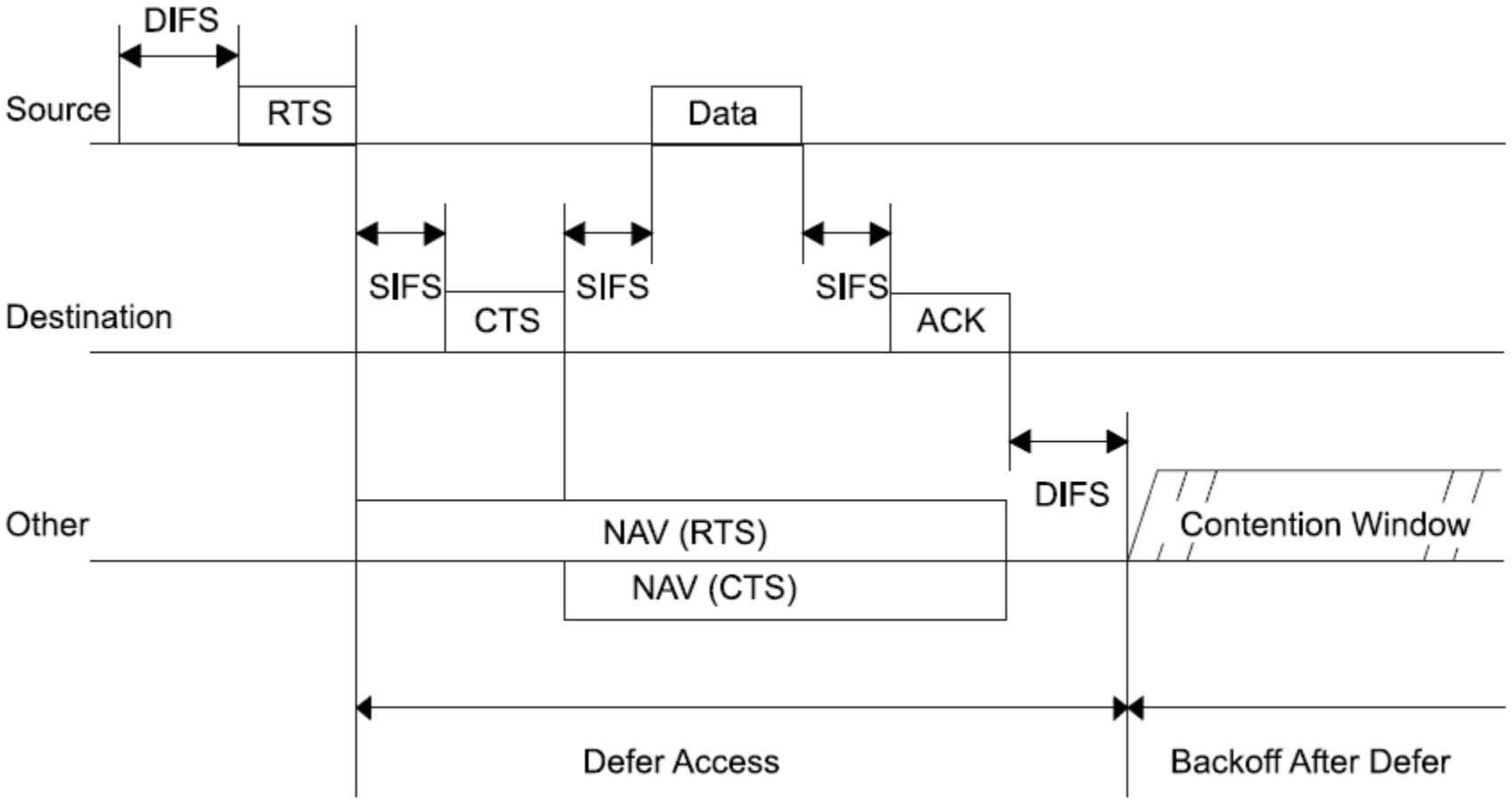
Retransmissions

- The sending station shall retry a transmission when this transmission fails
- It can fail because of collisions, or because the destination is also contending for the channel and unable to answer
- Retransmissions shall occur until the transmission is successful or until the retry limit is reached (there are 2 retry counters SSRC for Station Short Retry Count, and SLRC for long frames)
- Upon non reception of an ACK, the backoff procedure shall restart before retransmission

NAV

- A Network Allocation Vector is used to avoid doing CCAs in order to determine if the channel is busy or not
- When a station receives a valid frame that is not destined to it, it updates its NAV according to the duration field of the frame

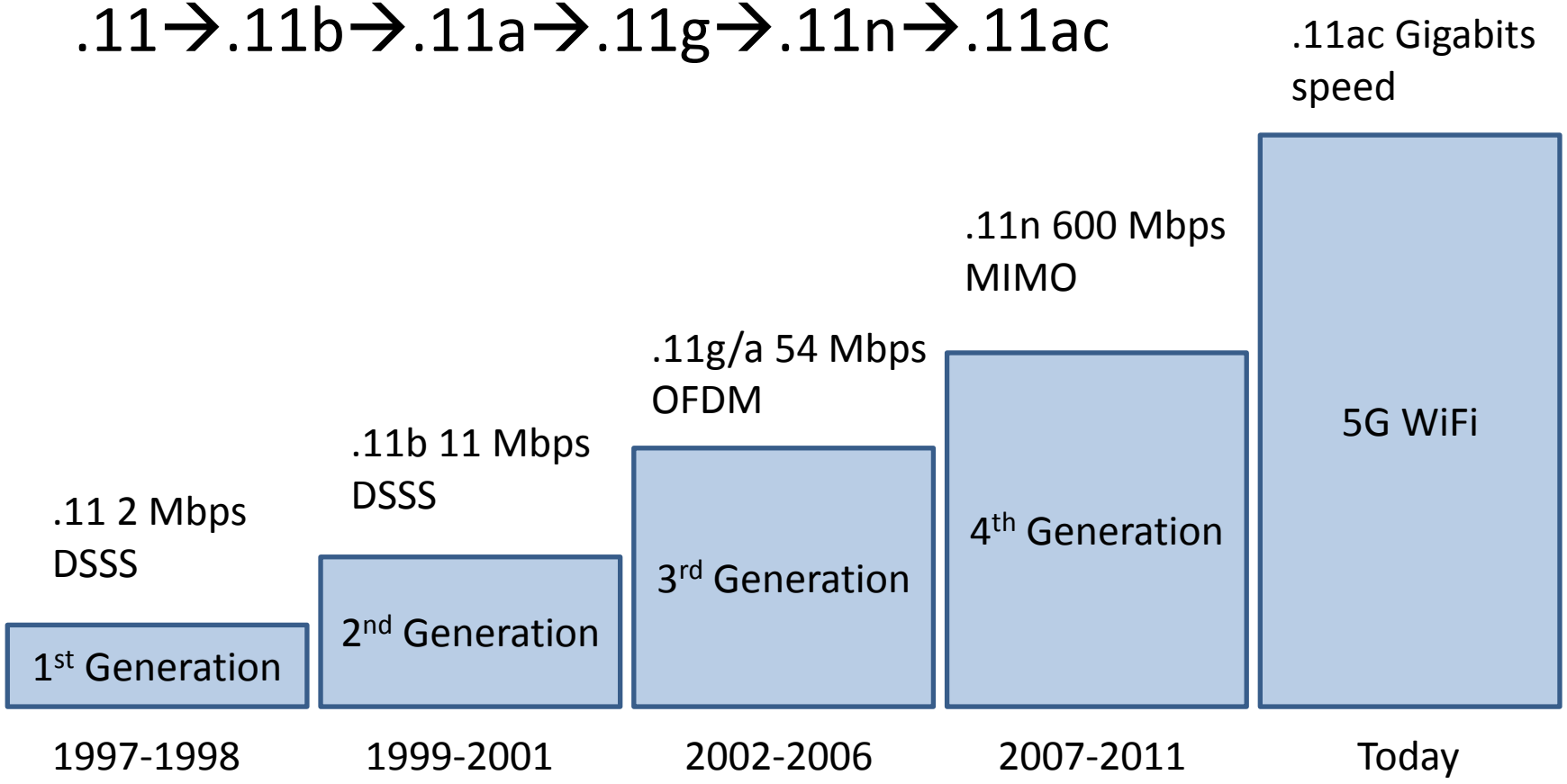
Data exchange example with RTS/CTS and NAV updates



WiFi evolution

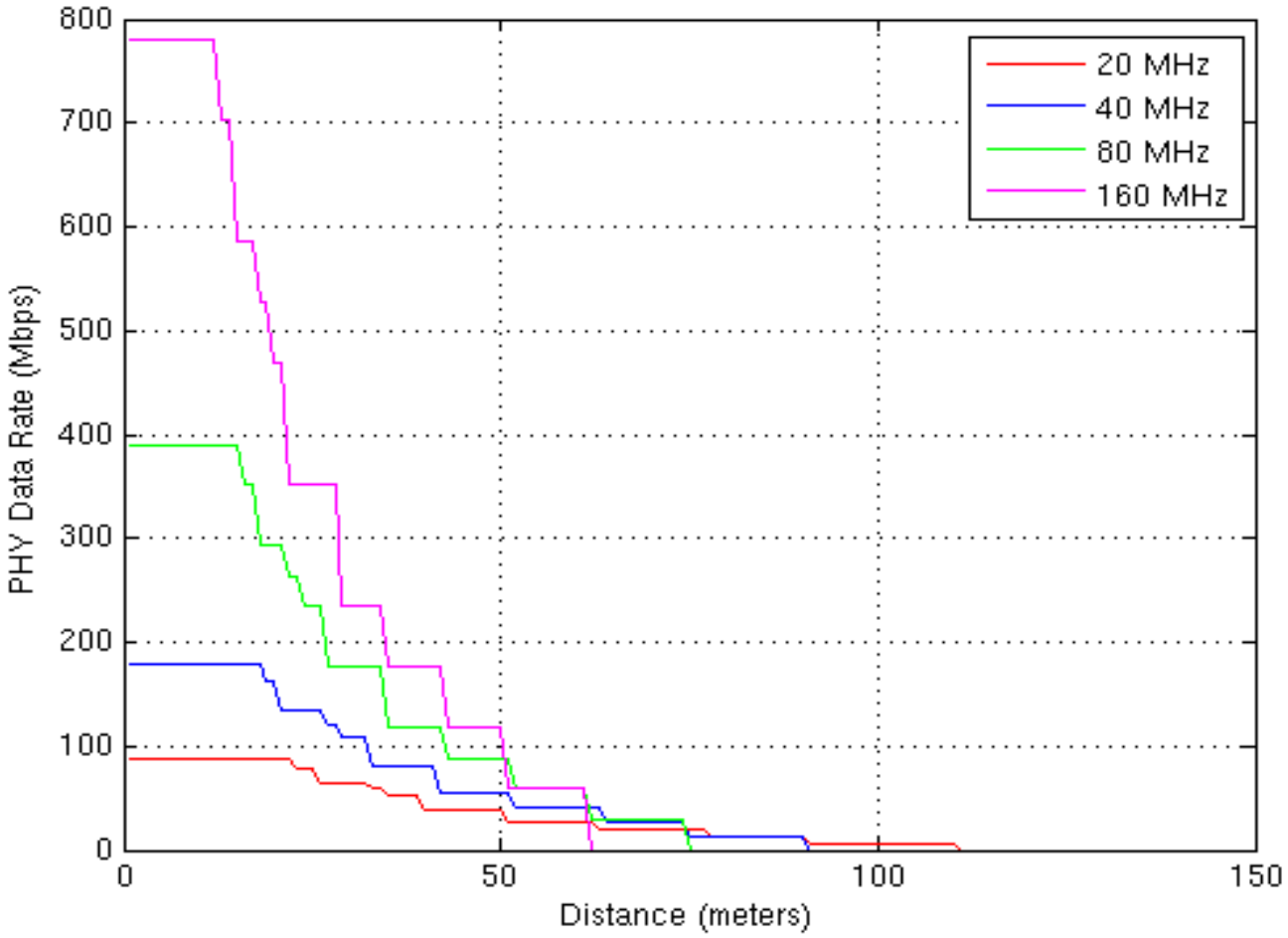
(Source Ron Porat, VTC 2013 Panel)

- Evolution of WiFi:
  .11→.11b→.11a→.11g→.11n→.11ac



802.11ac: Rate vs Range

(Source Ron Porat, VTC 2013 Panel)



Summary features

- 802.11: 2.4 GHz 1-2 Mbps
- 802.11b: 2.4 GHz, 20 MHz channels, DSSS, up to 11 Mbps
- 802.11a/g: 2.4 & 5 GHz, 20 MHz channels, OFDM, up to 54 Mbps
- 802.11n: 2.4 & 5 GHz, 20/40 MHz channels, OFDM, MIMO (up to 4 streams)
- 802.11ac: 5 GHz, OFDM, MIMO (up to 8 streams), 20/40/80/160/80+80 MHz channels, 2/4/16/64/256 QAM, MultiUser-MIMO, Explicit channel feedback + Beamforming
  - 2.4 GHz ISM band: 3 non-overlapping 20 MHz channels, 30 dBm power limit in the US
  - 5 GHz ISM band: 25/12/6/2 non-overlapping 20/40/80/160 MHz channels currently in US

What's next?

- Beyond 11ac → 11ad, 11af, 11ah, 11ai, 11ak, HEW
- ad for 60GHz band (7-9GHz bandwidth), very high data rates (4.6Gbps and 7Gbps) but short range
  - aj special case for China with less bandwidth (5GHz around the 60GHz and 3GHz around the 45GHz)
- af for TV WhiteSpaces (VHF/UHF TV channels that are no longer used) around the 600 MHz band
  - Longer range (2.5 to 3 times bigger than that of 2.4 GHz)
  - Data base access to know what frequency to use depending on the location

What's next?

- ah for unlicensed spectrum < 1 GHz (including TVWS)
- ai for very fast link set-up (<100ms) many simultaneous connections trains, buses, etc.
- ak better interoperability between 802.11 and 802.3 (Ethernet) for supporting 802.1q (VLANs) and QoS for audio and video
- HEW High Efficiency WLAN, group formed in 2013 to maintain and enhance the presence of WiFi in 2.4GHz and 5GHz, will become a task group in mid 2014

WiFi for positioning

- 802.11k/v provide the tools for several location methods and services:
  - Exchange of known location data in either Civic (address) or Geo (long./lat.) format
  - Fine Timing Measurement protocol for round trip time (RTT) based range estimate
    - Using the captured timestamps to compute the round trip time and estimate the distance between two devices. A device can estimate its location by performing ranging with multiple peers whose locations are known as priori
  - Location Tracking protocol: Multiple APs use time difference of arrival (TDOA) to calculate device location
  - Location Identifier Report: receive an indirect database website reference that can be used to gather the device's location value

Part 4:
IEEE 802.15.4

LR-WPAN

- ✓ IEEE 802.15.4 specifies the MAC and Physical layers for Low Rate Wireless Personal Area Network
- ✓ It is the basis for ZigBee, WirelessHART and ISA100.11a (just like IEEE 802.11 is the basis for WiFi)

What's a LR-WPAN?

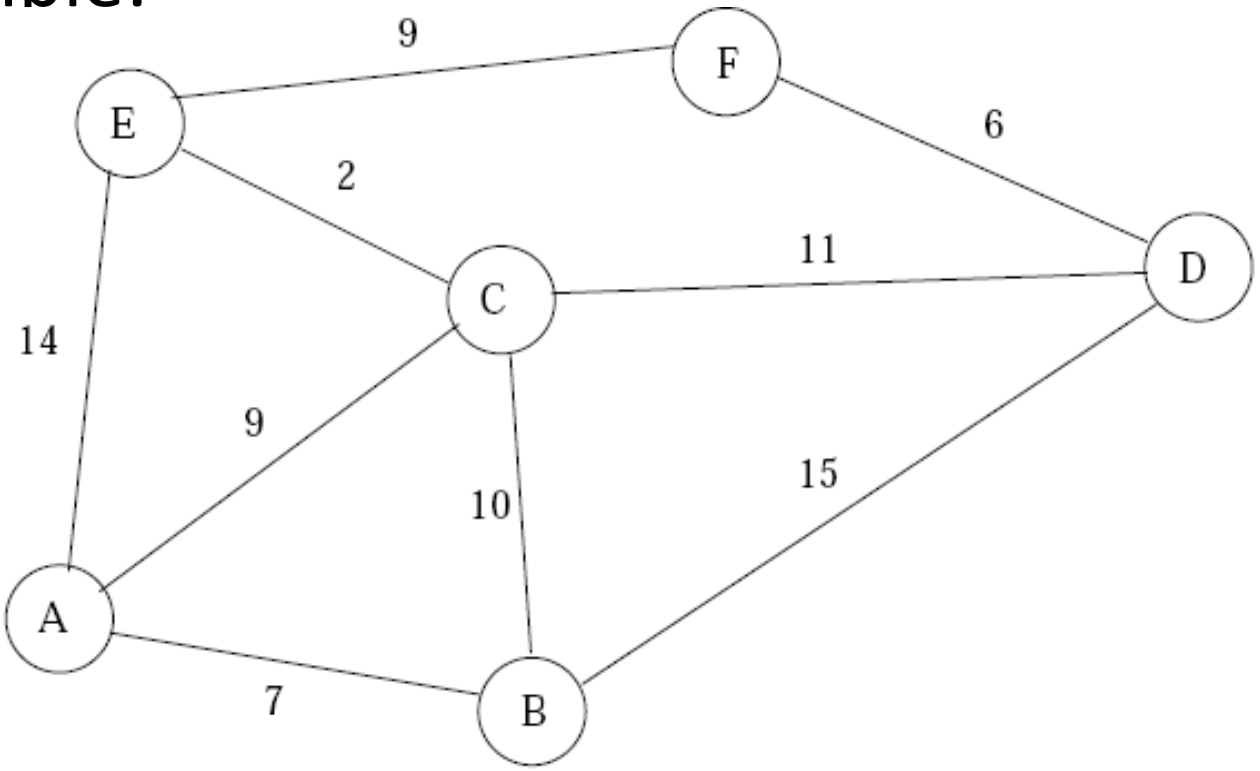
- It is a network that is supposed to work at low rate and consumes very little energy
- Wireless sensor networks (WSNs) are an example of a LR-WLAN or LR-WPAN depending on the size of the network
- It is a type of wireless mobile ad hoc network

What's an Ad hoc network?

- Generally referred to as MANET for Mobile Ad hoc NETwork
- It has the following characteristics:
  - Multi-hop Wireless links
  - Absence of infrastructure equipment such as Access Points, routers or switches
  - Auto-configuration
  - All nodes can be routers and participate in the routing activity

Representation of a MANET

- A MANET is usually represented as a graph, example:



MAC and routing issues in MANET

- Routing: find a route from source to destination
  - Limited communication range
  - Limited vision of topology

→ Nodes need to cooperate to maintain routes

- MAC: manage the access to the medium
  - Deals with collision avoidance
  - Bandwidth sharing and Interferences

→ Centralized/distributed medium sharing

Ad hoc routing protocols

- There are 2 main families of routing protocols:
  - Distance Vector
    - Each node maintains a table that indicates the cost to reach each destination in the network (the distance) and the neighbor through which the message should be sent (the vector)
  - Link State
    - Each node broadcasts to the whole network the list of its neighbors
    - By collecting these lists, every node is able to build a graph of the network connectivity

Proactive and Reactive routing protocols

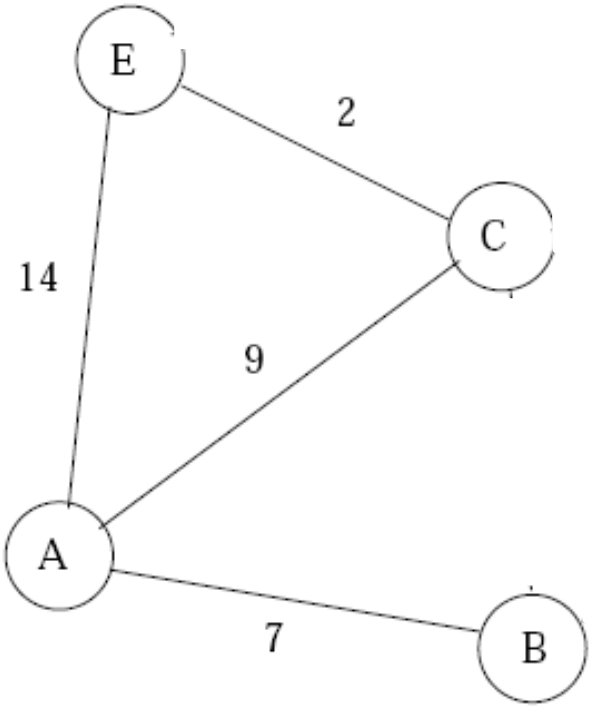
- Routing protocols can also be divided into proactive and reactive protocols
- In proactive mode, the routing protocol maintains routes towards all the possible destinations
- In reactive mode, routes are only built on demand for active destinations

Distance Vector steps

- Each node in the network will do the following steps:
  - 1. Estimate the cost of each link with its neighbors
  - 2. Send this information to its neighbors
  - 3. Update its routing table according to its information received from neighbors

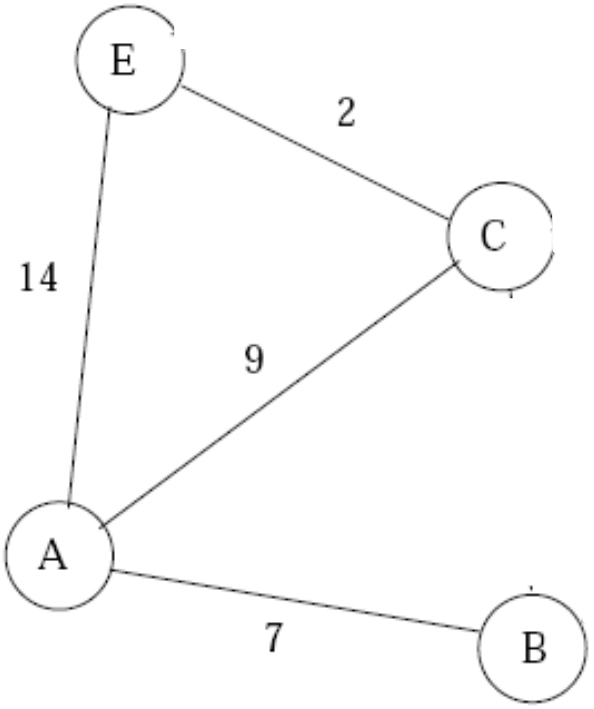
Example of Distance Vector (1)

- At T = 1:
  - Routing table of A contains:
    - A --> B : 7 via B
    - A --> E : 14 via E
    - A --> C : 9 via C
  - Routing table of B contains:
    - B --> A : 7 via A



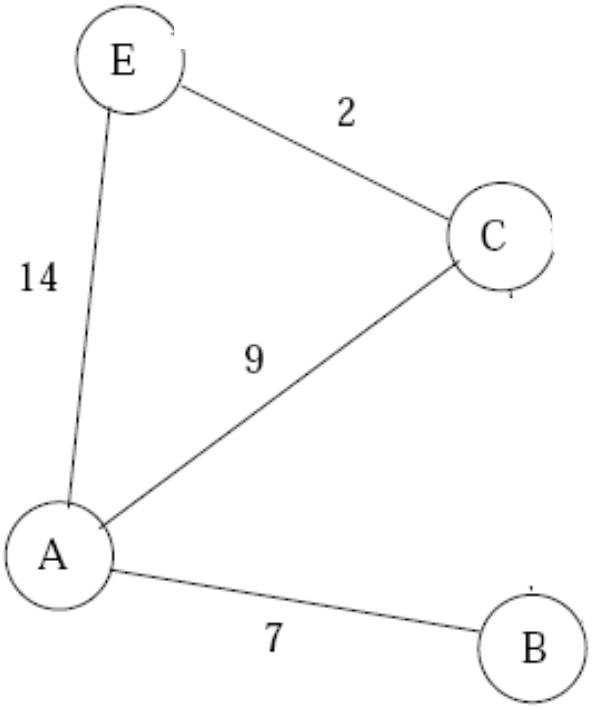
Example of Distance Vector (2)

- At T = 2:
  - Routing table of A contains:
    - A --> B : 7 via B
    - A --> E : 11 via C
    - A --> C : 9 via C
  - Routing table of B contains:
    - B --> A : 7 via A
    - B --> C : 16 via A
    - B --> E : 21 via A



Example of Distance Vector (3)

- At T = 3:
  - Routing table of A contains:
    - A --> B : 7 via B
    - A --> E : 11 via C
    - A --> C : 9 via C
  - Routing table of B contains:
    - B --> A : 7 via A
    - B --> C : 16 via A
    - B --> E : 18 via A

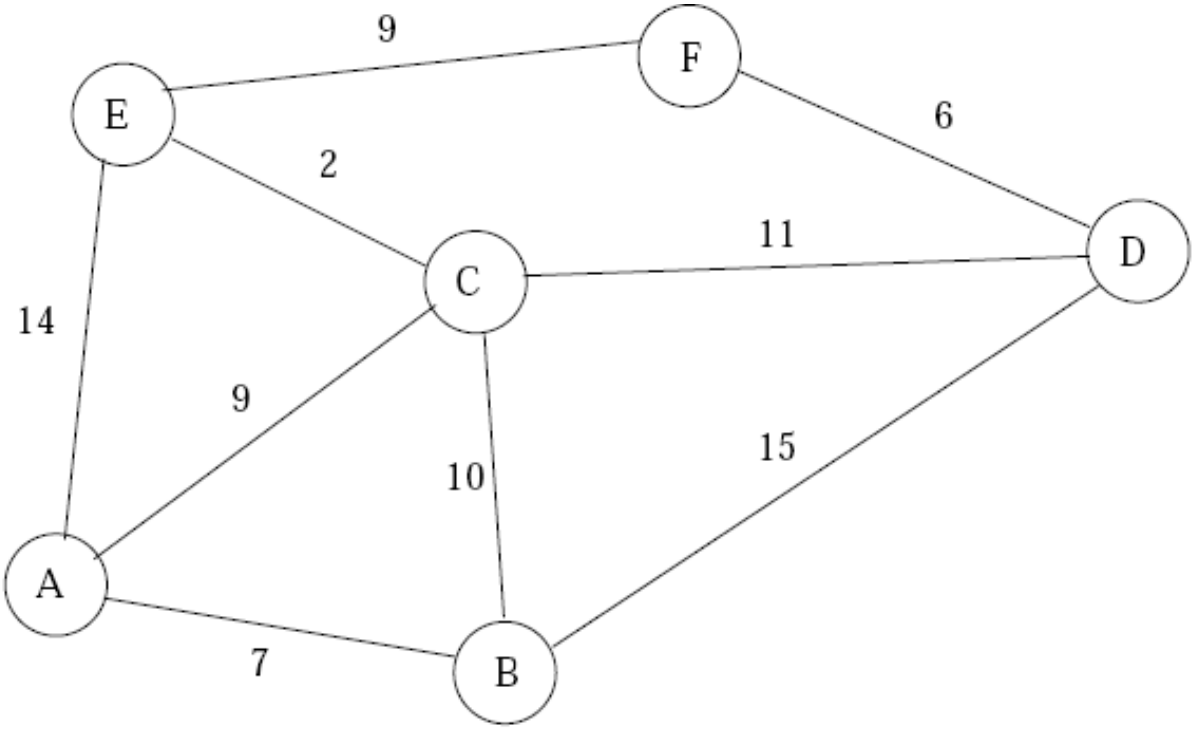


Link State steps

- Each node in the network will do the following:
  - 1. Estimate the cost of each link with its neighbors
  - 2. Broadcast this information the whole network
  - 3. Construct the graph of the network by collecting the neighborhood information of all the other nodes
  - 4. Apply an algorithm that gives the routes towards all the nodes in the network

Example of Link State

- Let us suppose that nodes were able to build such a graph (this graph should be the same for all nodes)



Dijkstra

- Dijkstra is an algorithm that gives the shortest path starting from a given node towards all the destination in a given graph
- The shortest path is calculated according to criteria such as:
  - Link bandwidth
  - Link State (BER, PER)
  - Number of hops

Dijkstra steps

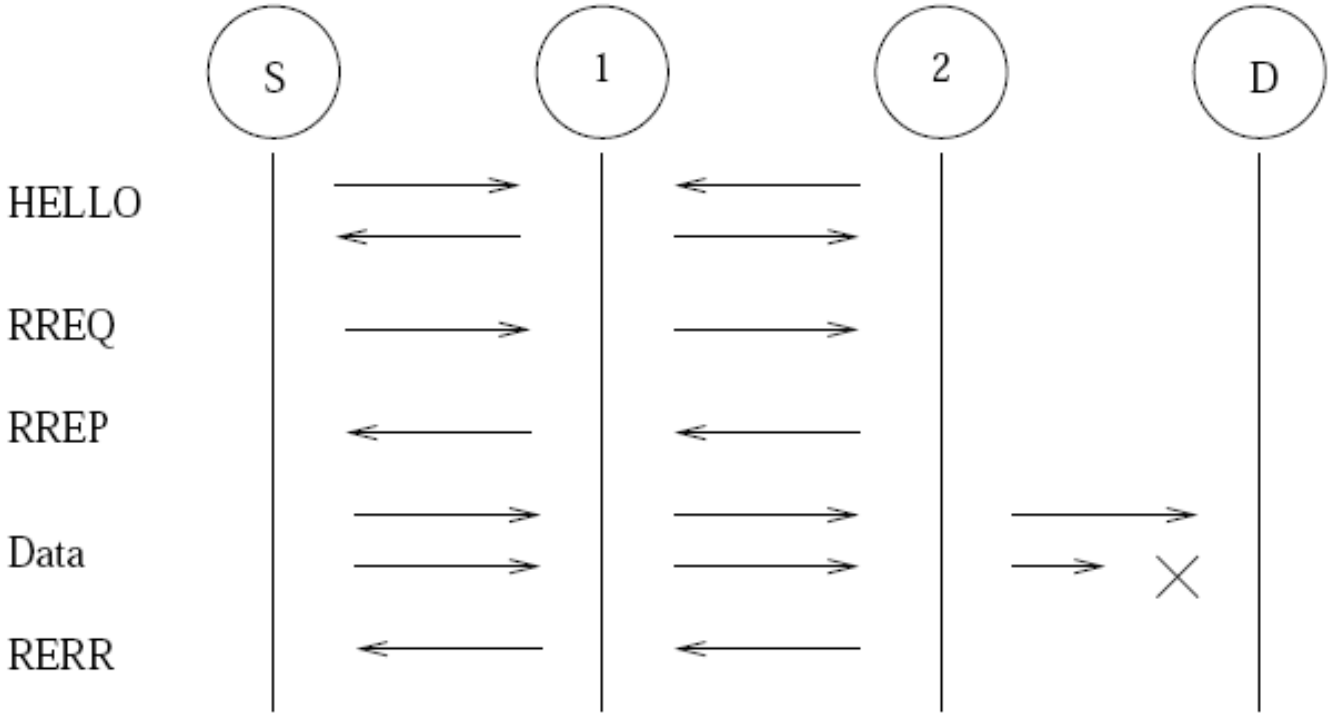
- 1. Starting from the source node, we consider that the cost to reach all the other nodes is ∞
- 2. We replace ∞ by the cost of each link with the neighbours
- 3. We choose as a next hop the node with the smallest cost
- 4. We add the cost to reach the neighbors of that node to the cost to reach the chosen node
- 5. Return to step 3 until the destination is reached

Example of Distance Vector protocol: AODV

- Ad hoc On demand Distance Vector routing protocol
- Routes are constructed only when needed:
  - A RREQ (Route REQuest) is broadcast by the source node
  - An intermediate node propagates the RREQ if (1) it is not the destination, (2) has not already received the same RREQ, and (3) does not know how to reach the destination
  - When the destination is found, a RREP (Route REPly) is sent in a unicast mode towards the source node (every intermediate node adds its ID to the RREQ)

Example of AODV

- S needs to reach D, node 1 does not know how to reach D, D is the neighbor of node 2



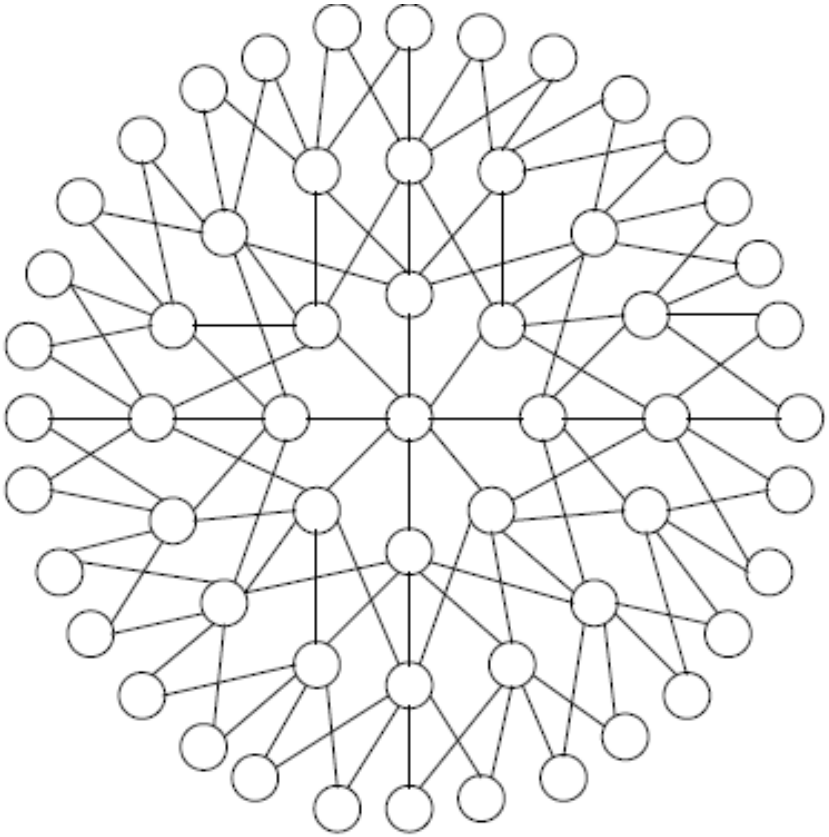
Example of Link State protocol: OLSR

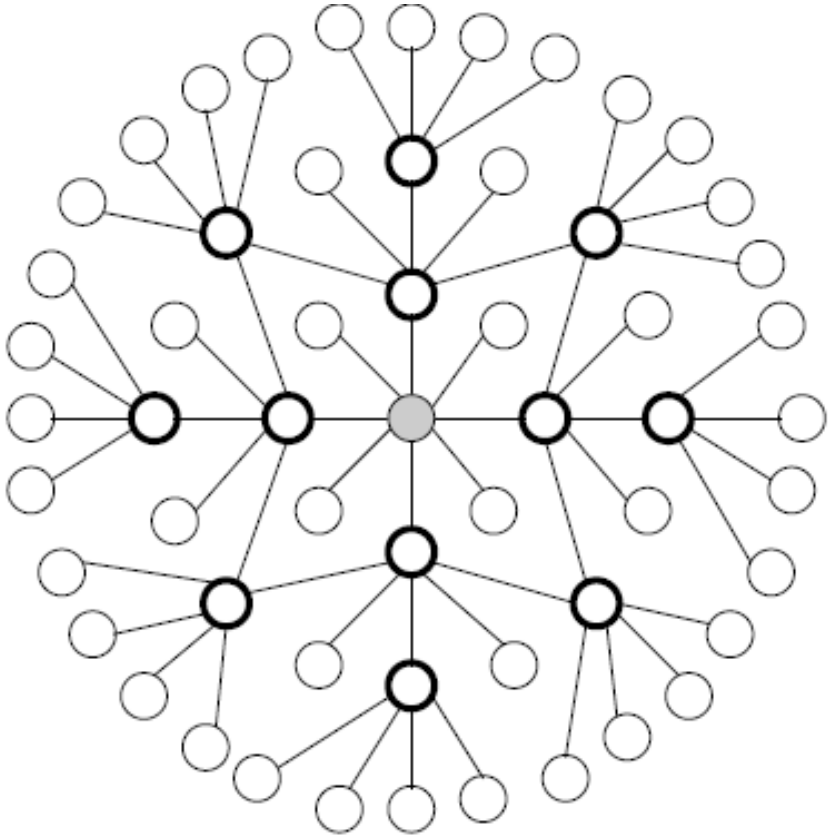
- OLSR: Optimized Link State Routing protocol
- Nodes do not put all the neighbors in the broadcast list: only MPR nodes are included in the list
- MPR: Multi-Point Relay nodes are a subset of neighbors that allow a node to reach all its 2-hop neighbors

OLSR

- Each node sends the list of its MPRs to its neighbors
- Each node broadcast the list of nodes for which it was elected as MPR
- Main advantages: smaller neighbor lists, less broadcast messages (only MPR participate in broadcasting)

Example of OLSR graph





Hybrid protocols

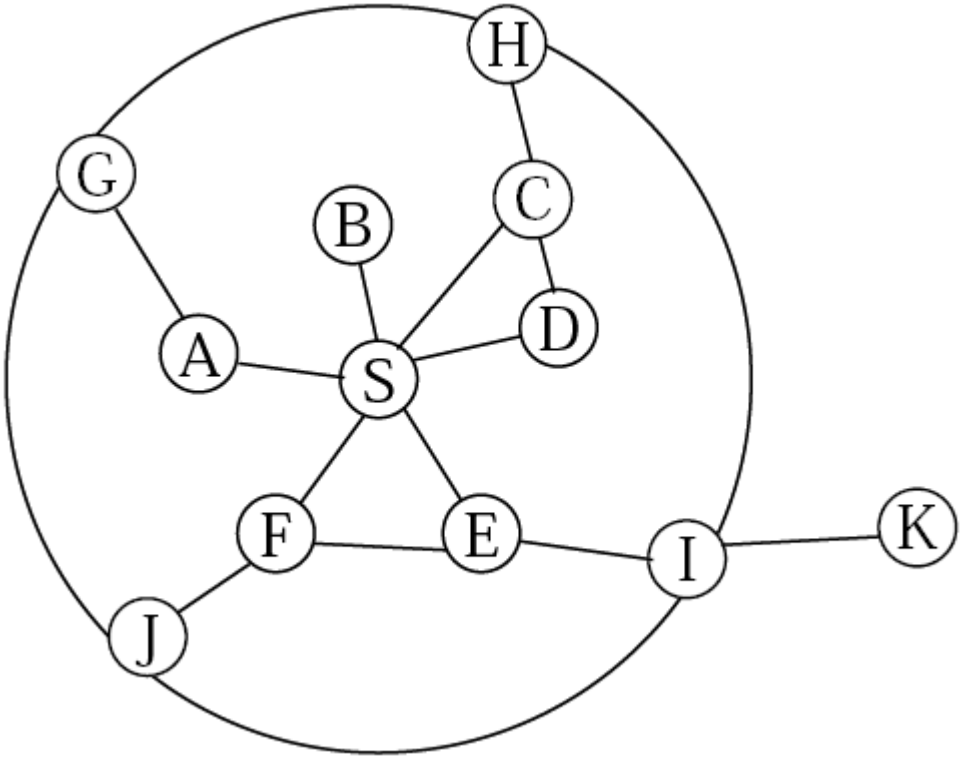
- Some routing protocols can function in both modes: proactive and reactive
- Routes towards close destinations are maintained proactively
- Routes towards far destinations are built on demand

Example of a hybrid protocol: ZRP

source : Nicklas Beijar, Zone Routing Protocol (ZRP)

- Zone Routing Protocol uses a proactive routing protocol for reaching nodes inside a predefined zone (IARP, IntrA zone Routing Protocol),
- It uses a reactive routing protocol for reaching nodes outside that zone (IERP, IntEr zone Routing Protocol)
- A zone is defined in terms on number of hops, example: 2-hop neighborhood of a node

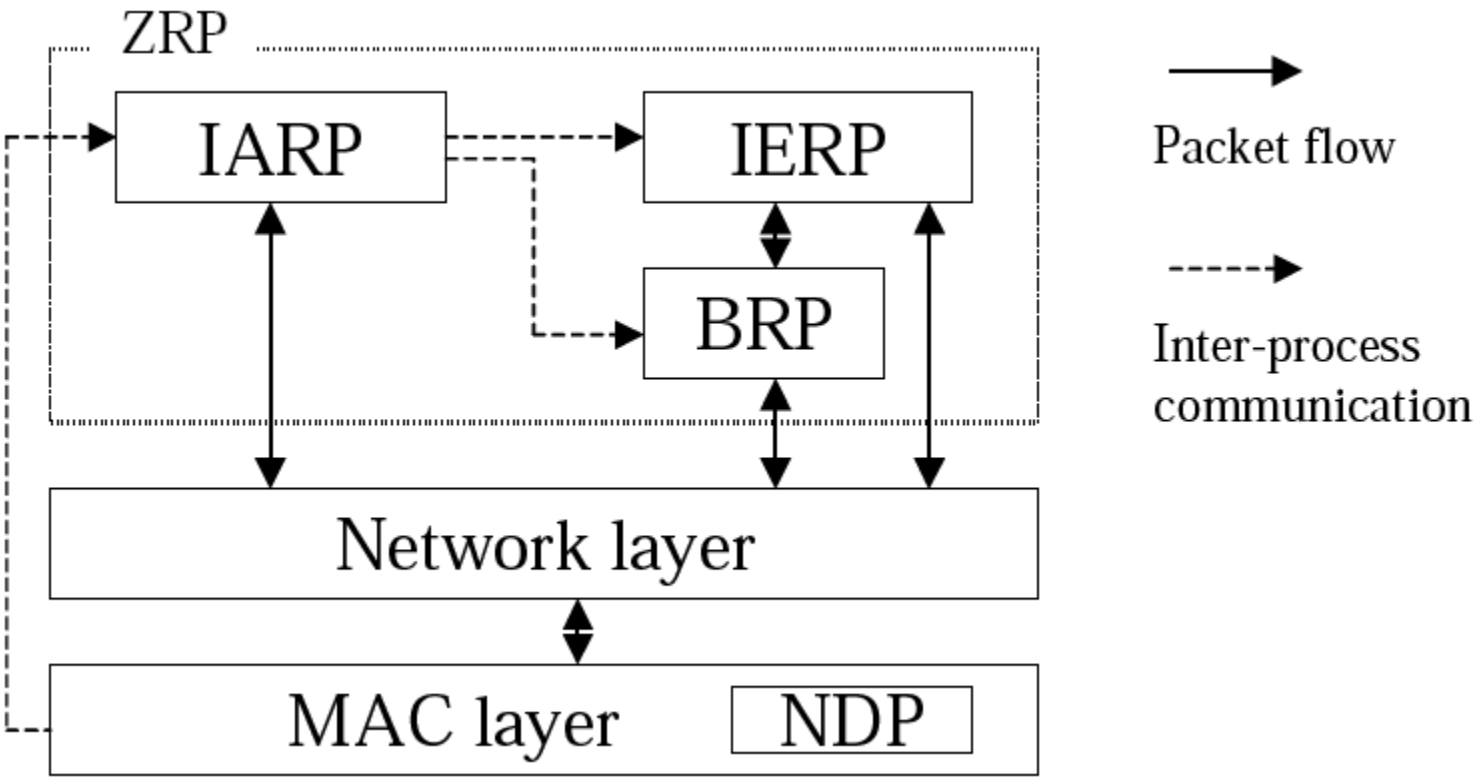
Example of a zone for node S



Additional protocols

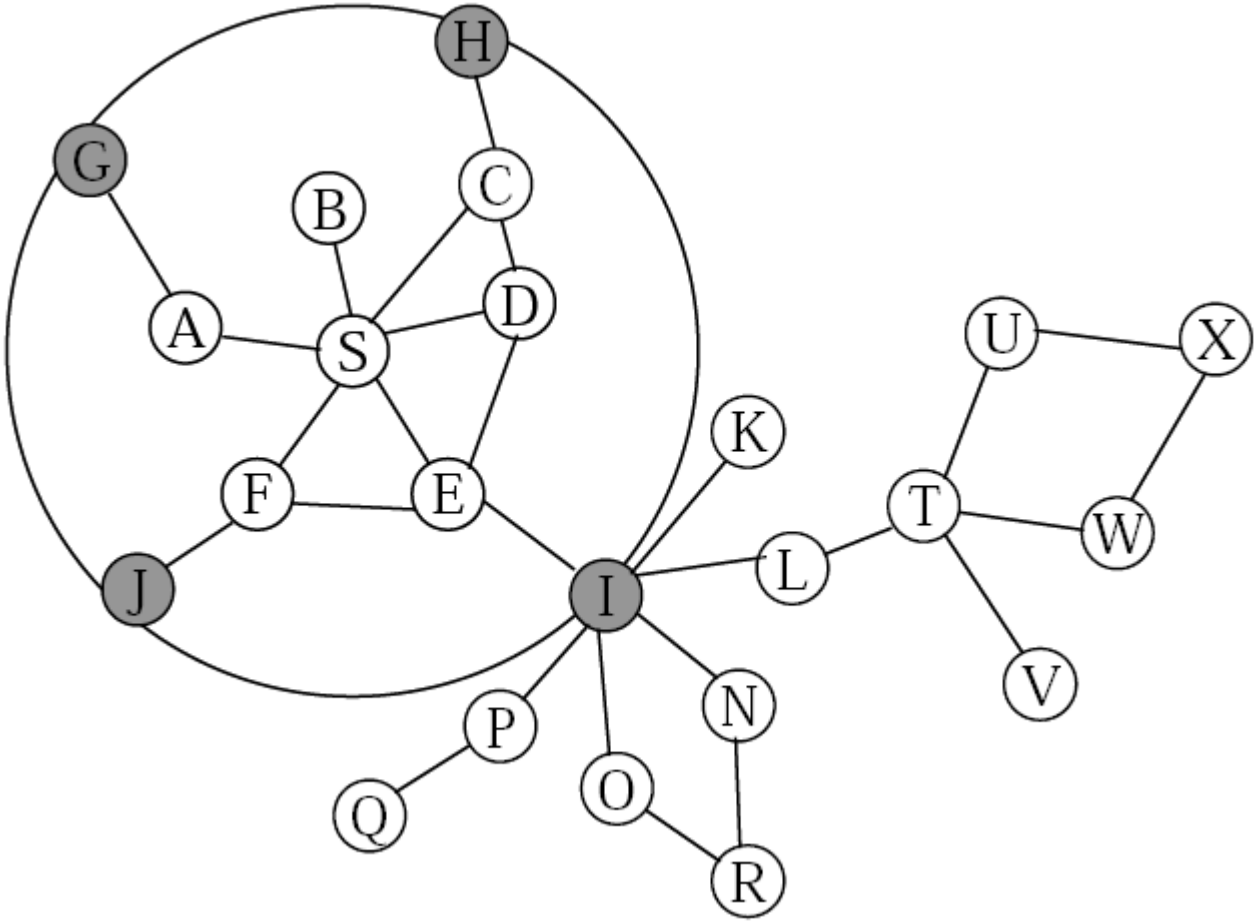
- Bordercast Resolution Protocol (BRP): this protocol helps reach nodes that are on the border of the zone (example: in a zone that covers nodes in 2 hops, it will give the list of 2-hop neighbors)
- Neighbor Discovery Protocol: this protocol helps maintain the list of neighbors

ZRP protocol architecture



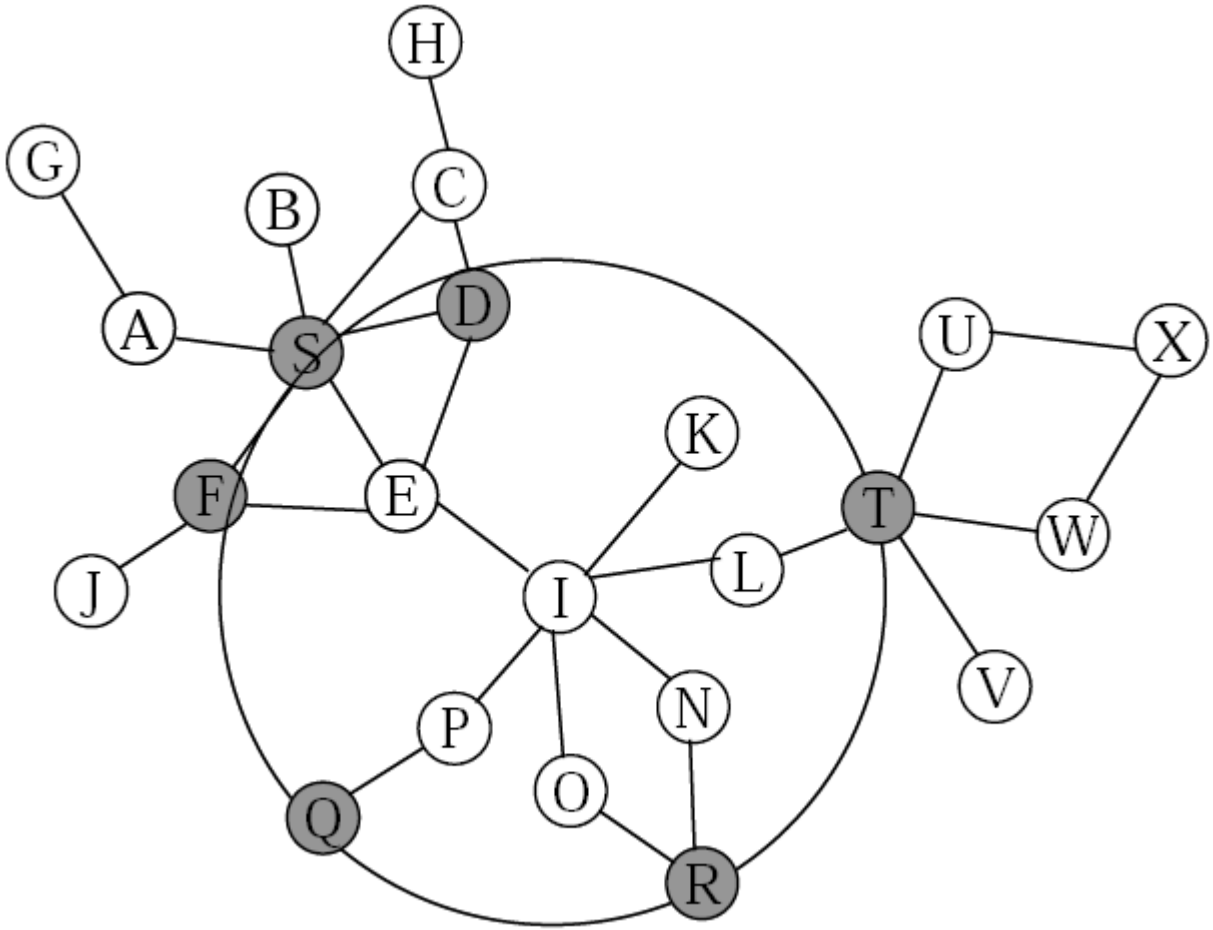
A routing example with ZRP: S→X

- S detects that X is not in the list of nodes of its zone (IARP)
- S sends a Route Request to border nodes (BRP)



A routing example with ZRP: S→X

- I receives the request and sends it to its border nodes (BRP)
- T receives the request and finds X in its zone (IARP)
- T appends the route towards X and sends back a route reply



Geographical routing protocols

- The goal for geographical routing protocols is to reduce the broadcast zones for route requests
- With the help of the geographical position of a node, the route request direction can be optimized to go towards the potential position of the destination

LAR: Location-Aided Routing protocol

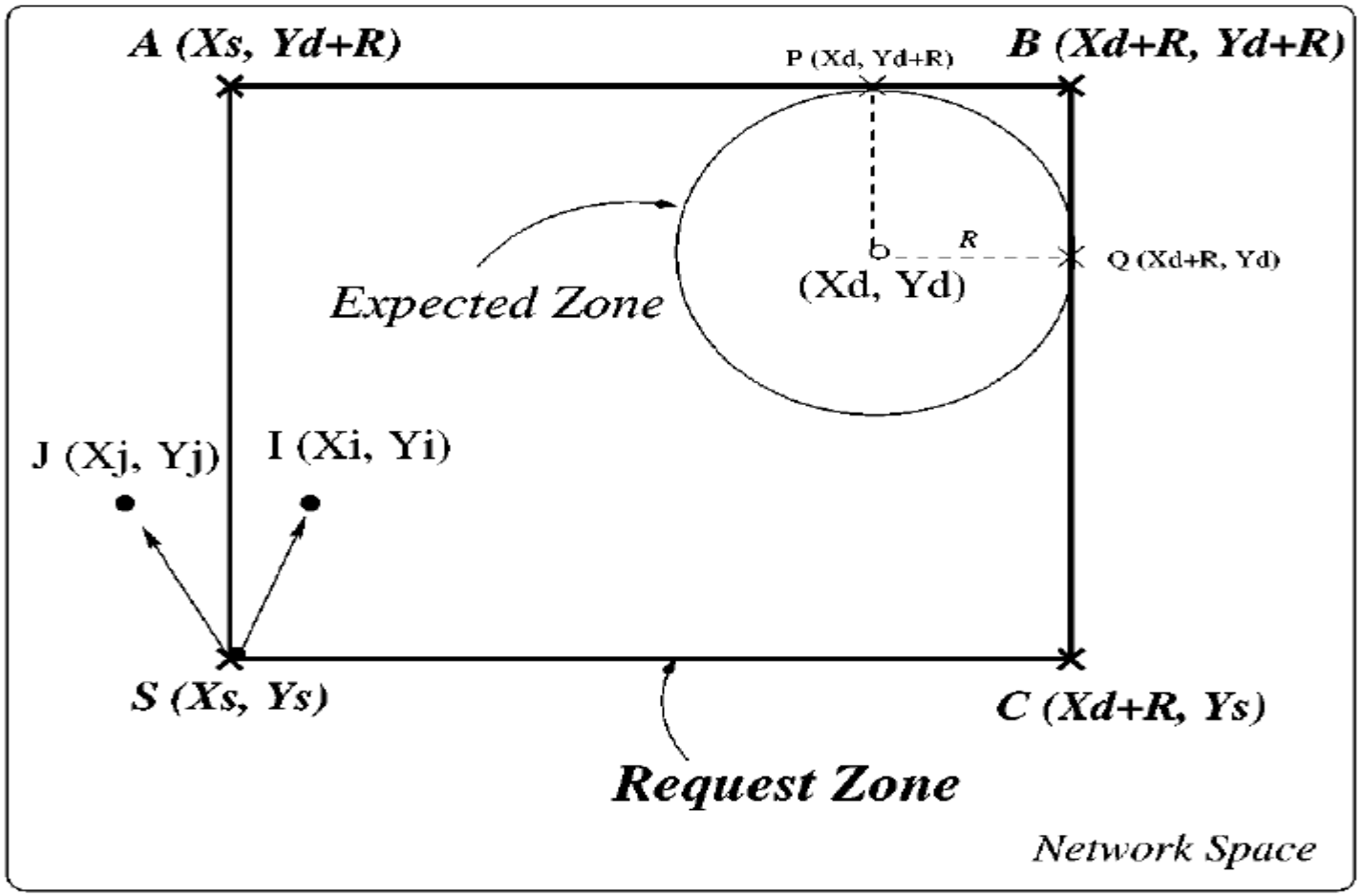
Young-Bae Ko and Nitin H. Vaidya, Location-Aided Routing (LAR) in mobile ad hoc networks

- Nodes estimate the current position of the destination based on the last known position and speed
- This gives an expected zone: disk with a radius $R = speed*(t_1 - t_0)$ and the last known position as the center
- An error margin is used to compensate speed variation and time synchronization: $R = error + speed*(t_1 - t_0)$

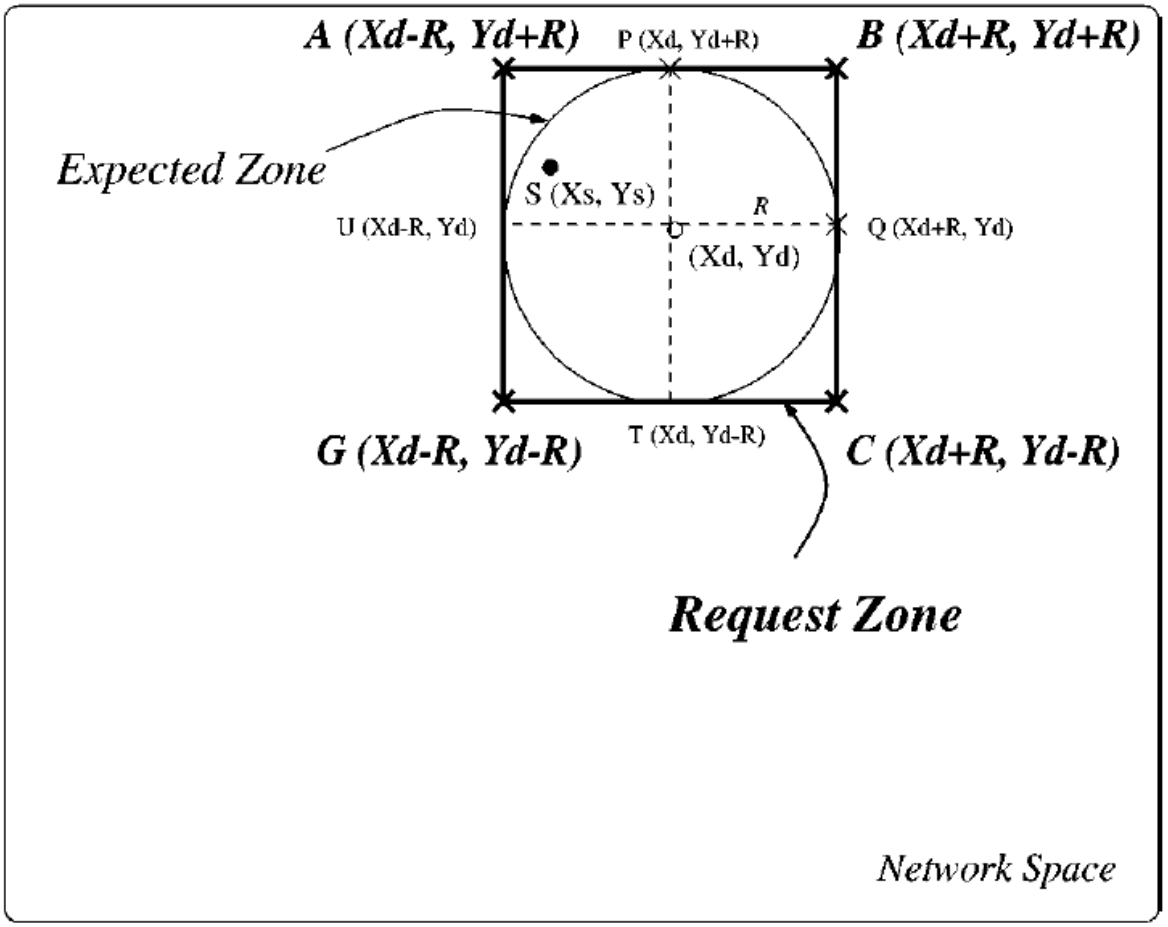
Request Zone

- A Request Zone is the zone that covers the nodes that should participate in the propagation of the route request
- Request Zone ≥ Expected Zone
- The bigger the Request Zone is, the higher the probability to find the destination is
- The smaller the Request Zone is, the less traffic is generated to propagate the route request

Example with LAR: source node is outside the expected zone



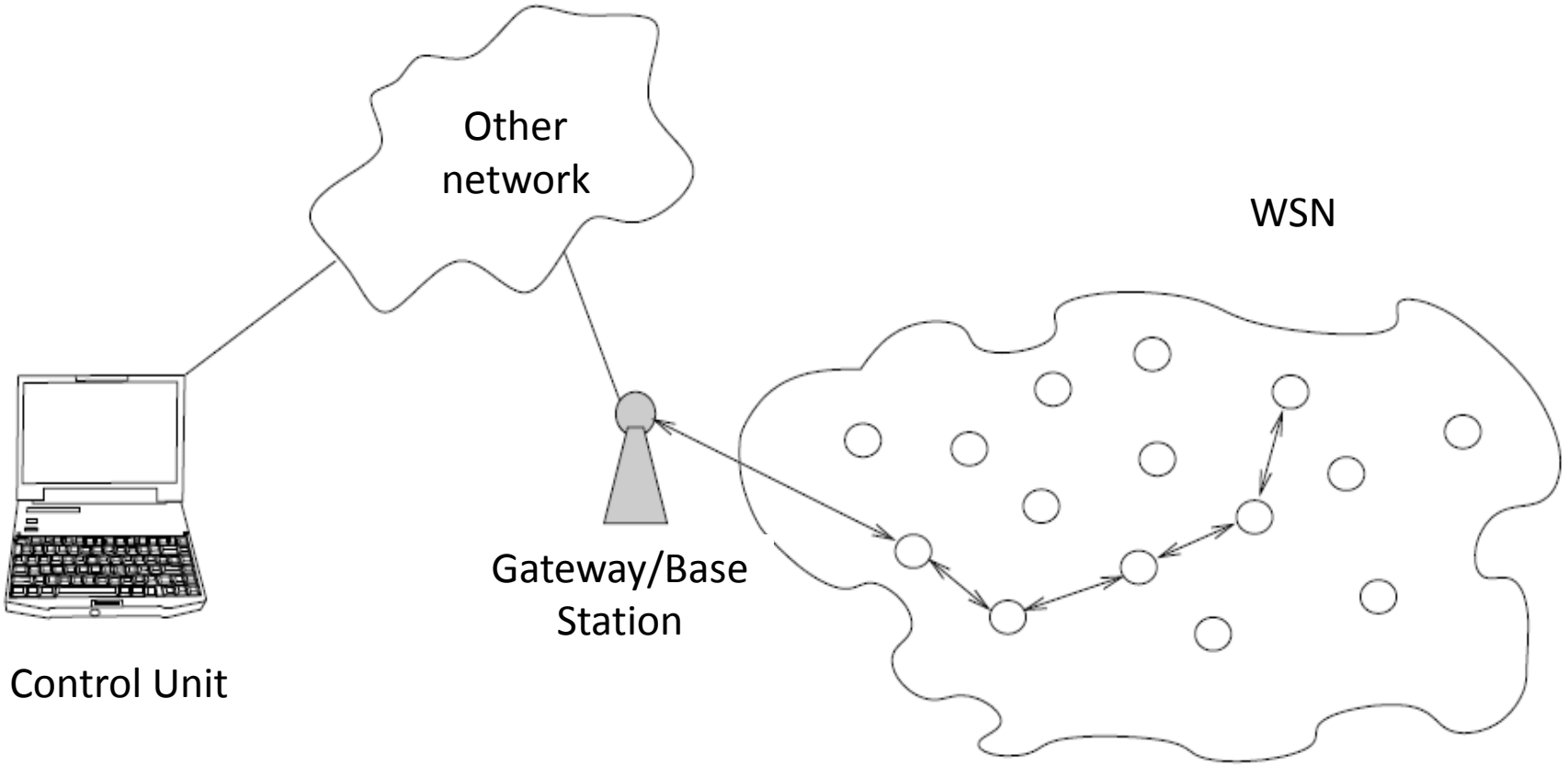
Example with source node inside the expected zone



What makes Wireless Sensor Networks different?

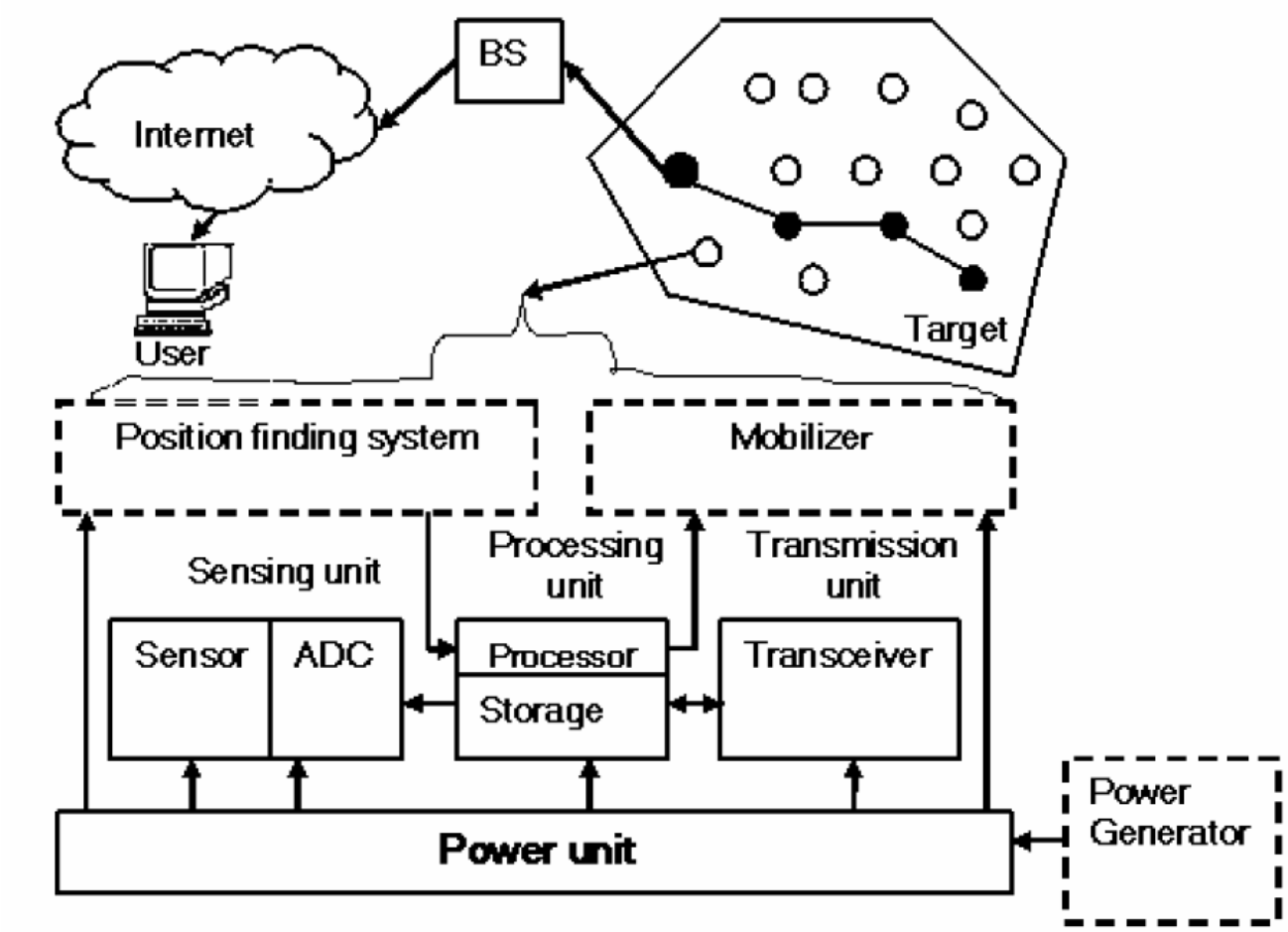
- Compared to Ad Hoc Networks, wireless sensor networks:
  - Are bigger
  - Have lower rates
  - Have more limitations (energy and computing resources, transmission rate and power, memory capacities)
- But they share most issues of wireless communications

Typical WSN deployment



Typical wireless sensor node

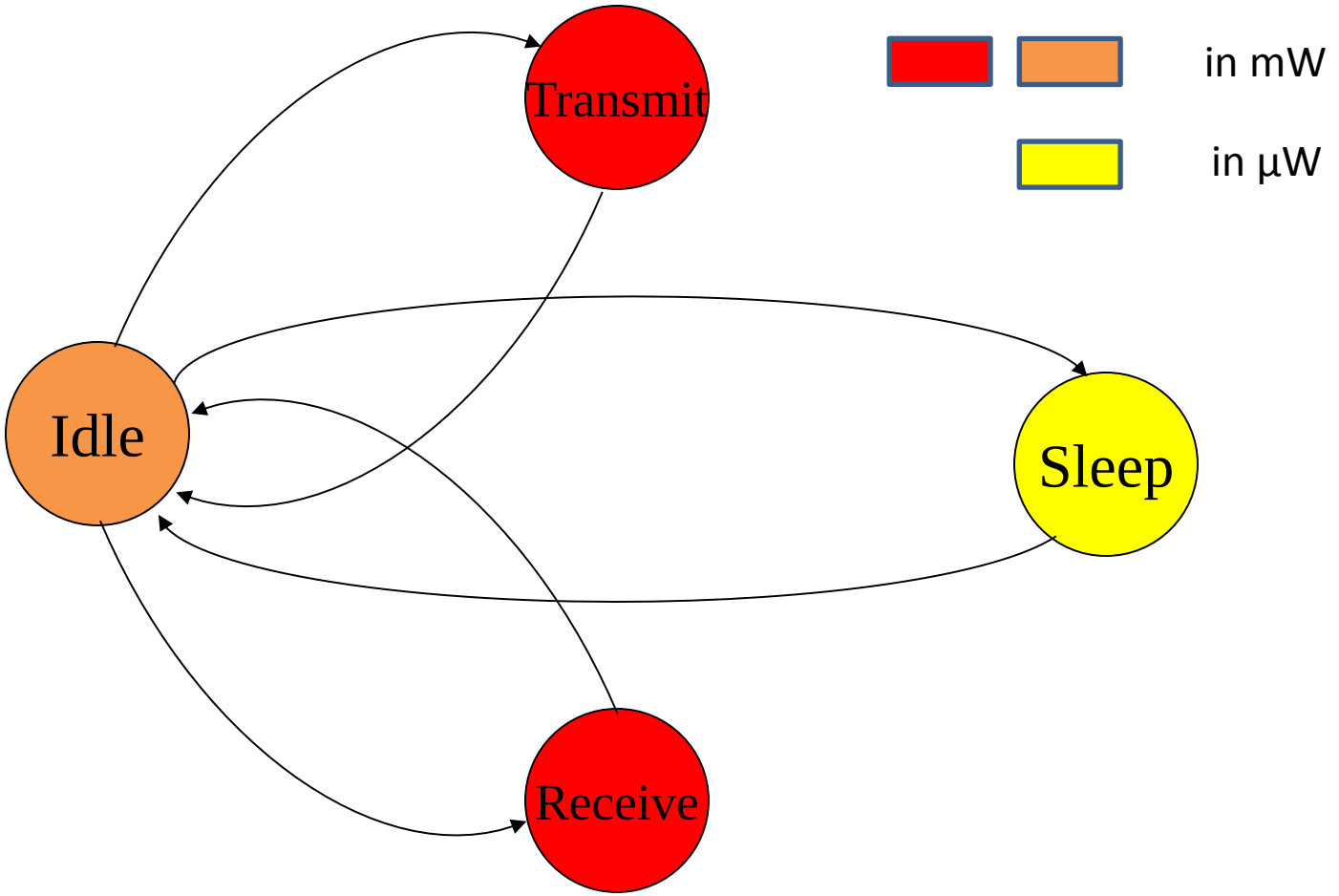
source : Classification and comparision of routing protocols in wireless sensor networks, UbiCC Journal – Volume 4



Energy efficient MAC protocols

- Components that consumes energy in a sensor node are:
  - The micro processor
  - The radio interface
  - The sensor
- MAC protocols control the radio interface, they decide when to transmit and when not to, they also have an effect on the processor

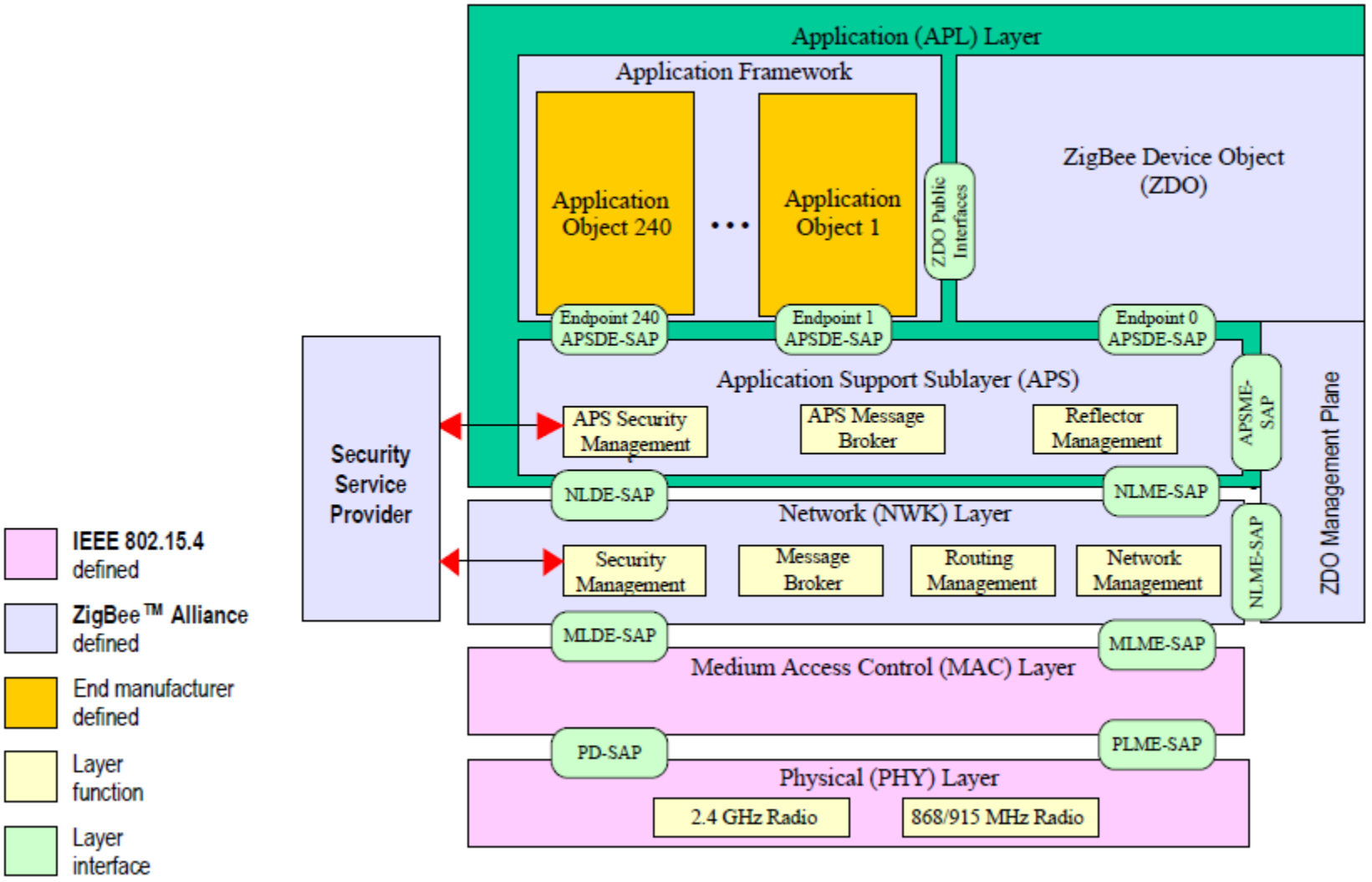
States of a radio transceiver



Energy wastage sources

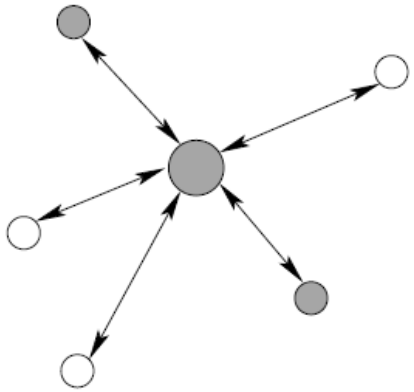
- An energy efficient MAC protocol will try to put the radio transceiver in a sleep mode as long as possible and when active will try to avoid the following:
  - Collisions
  - Idle listening
  - Overhearing
  - Overhead

The 802.15.4/ZigBee protocol stack



Network devices and topologies

FFD: Full Function Device → ZigBee coordinator and routers
RFD: Reduced Function Device → End-devices

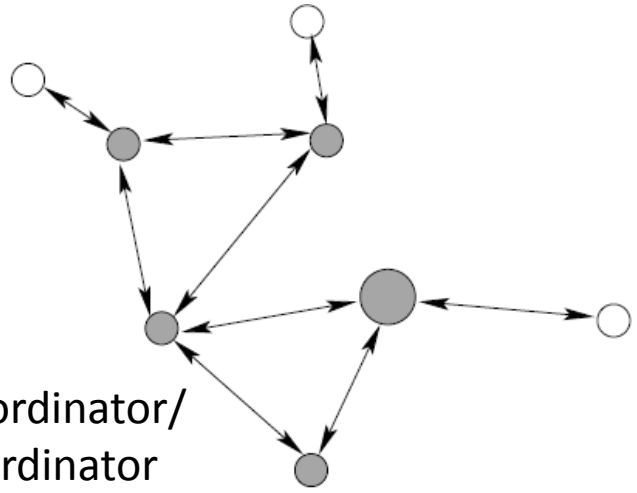


Star topology

Network Coordinator/
ZigBee Coordinator

Coordinator/Router

End-device



Mesh topology

Physical Layer

- Frequency bands: 779-787MHz (China), 868-868.6MHz (Europe), 902-928MHz (North America), 950-956MHz (Japan), 2400-2483.5MHz (Worldwide)
- Supported modulations: O-QPSK (Offset Quadrature Phase Shift Keying), BPSK (Binary), MPSK (M-ary, 16, China), ASK (Amplitude Shift Keying), GFSK (Gaussian, Japan)
- DSSS is the dominant transmission mode used

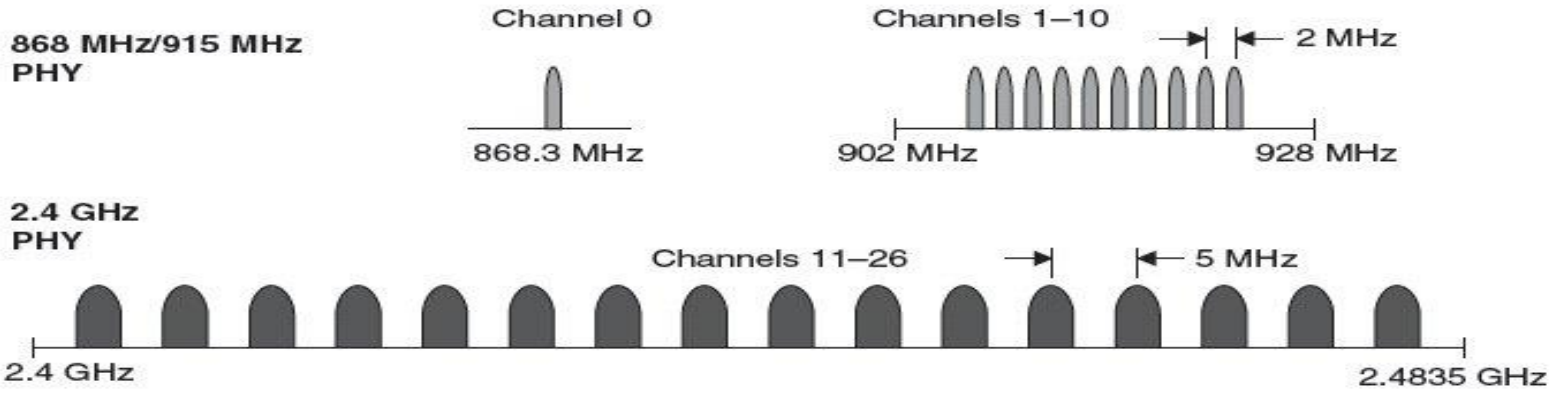
Symbol to chip mapping in 802.15.4 2.4GHz

Table 73 — Symbol-to-chip mapping for the 2450 MHz band

Data symbol	Chip values (c_0 c_1 ... c_{30} c_{31})
0	1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0
1	1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0
2	0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0
3	0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1
4	0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1
5	0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0
6	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
7	1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1
8	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
9	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1
10	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1
11	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0
12	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
13	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
14	1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
15	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

Channels

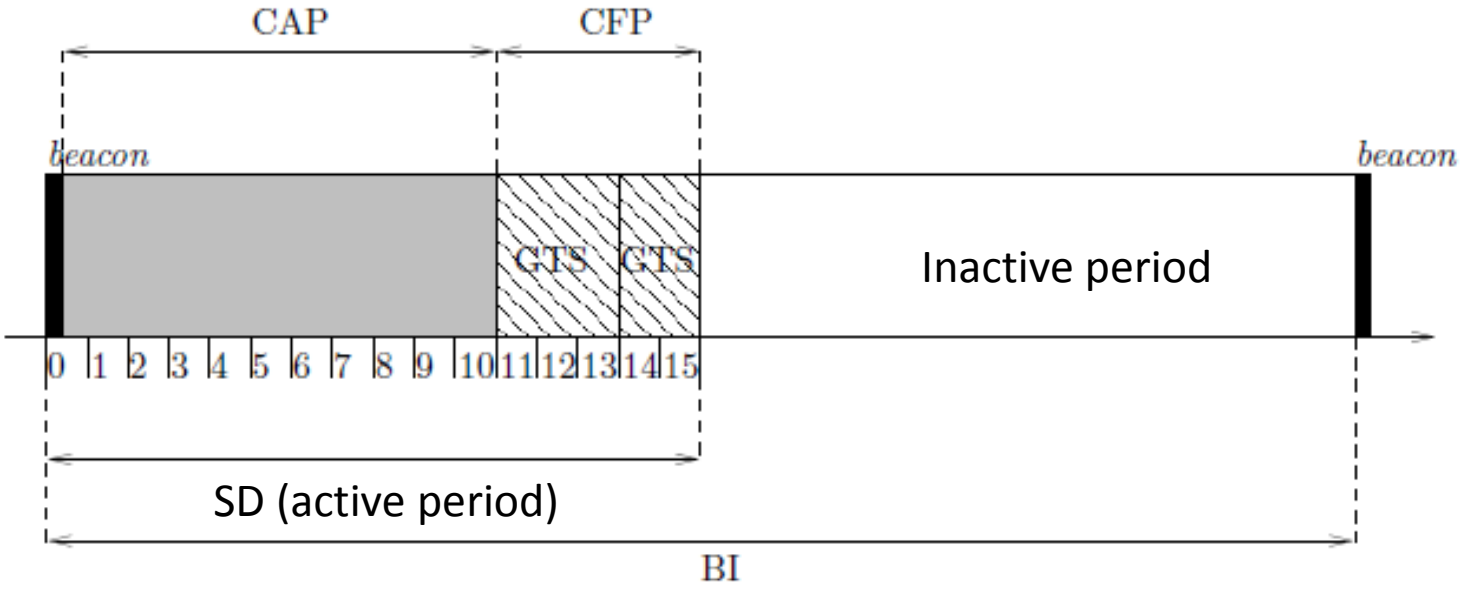
- 49 channels:
  - 16 channels in the 2.4 GHz band (worldwide)
  - 30 (10 in 2003) channels in the 900 MHz band (North America)
  - 3 (1 in 2003) channels in the 868 MHz band (Europe)



MAC Layer

- The MAC layer functions in 2 modes:
  - Beacon enabled mode: access to the medium is managed according to a Superframe structure. This mode allows the MAC layer to manage QoS through GTS (Guaranteed Time Slots)
  - Non beacon enabled mode: does not support QoS and beacons are not sent periodically

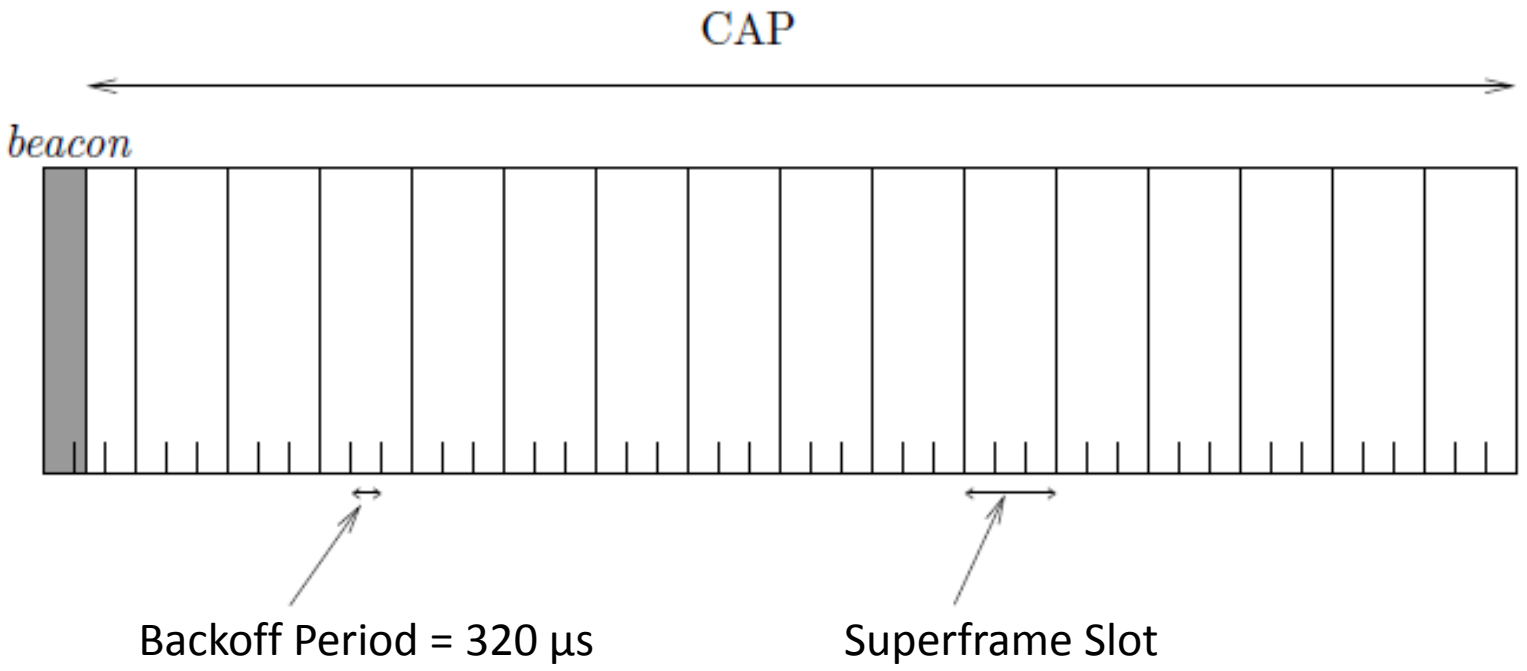
Superframe structure



$$\begin{cases} BI = aBaseSuperframeDuration.2^{BO}, \\ SD = aBaseSuperframeDuration.2^{SO}, \end{cases}$$

$$0 \leq SO \leq BO \leq 14$$

Zoom on the CAP



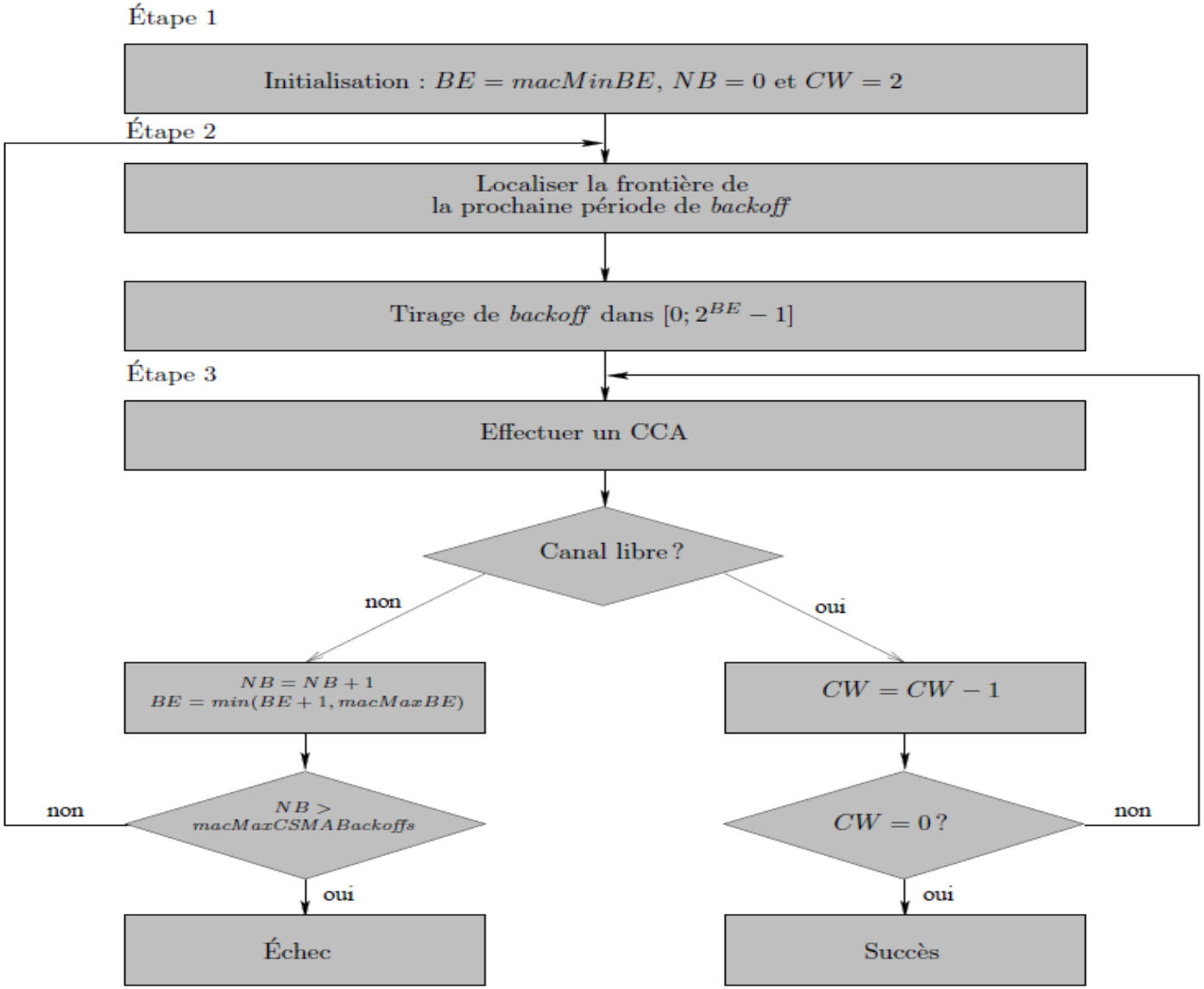
Some durations

- Minimum duration of a superframe: 15,36ms
- 15,36ms = 48 * 320µs
- For a SO = 0, the duration of the superframe slot is 0,96ms (3 * 320µs)
- If BO = SO = 15, the network activity does not respect the superframe structure
- What's the duration of the superframe on slide 160?

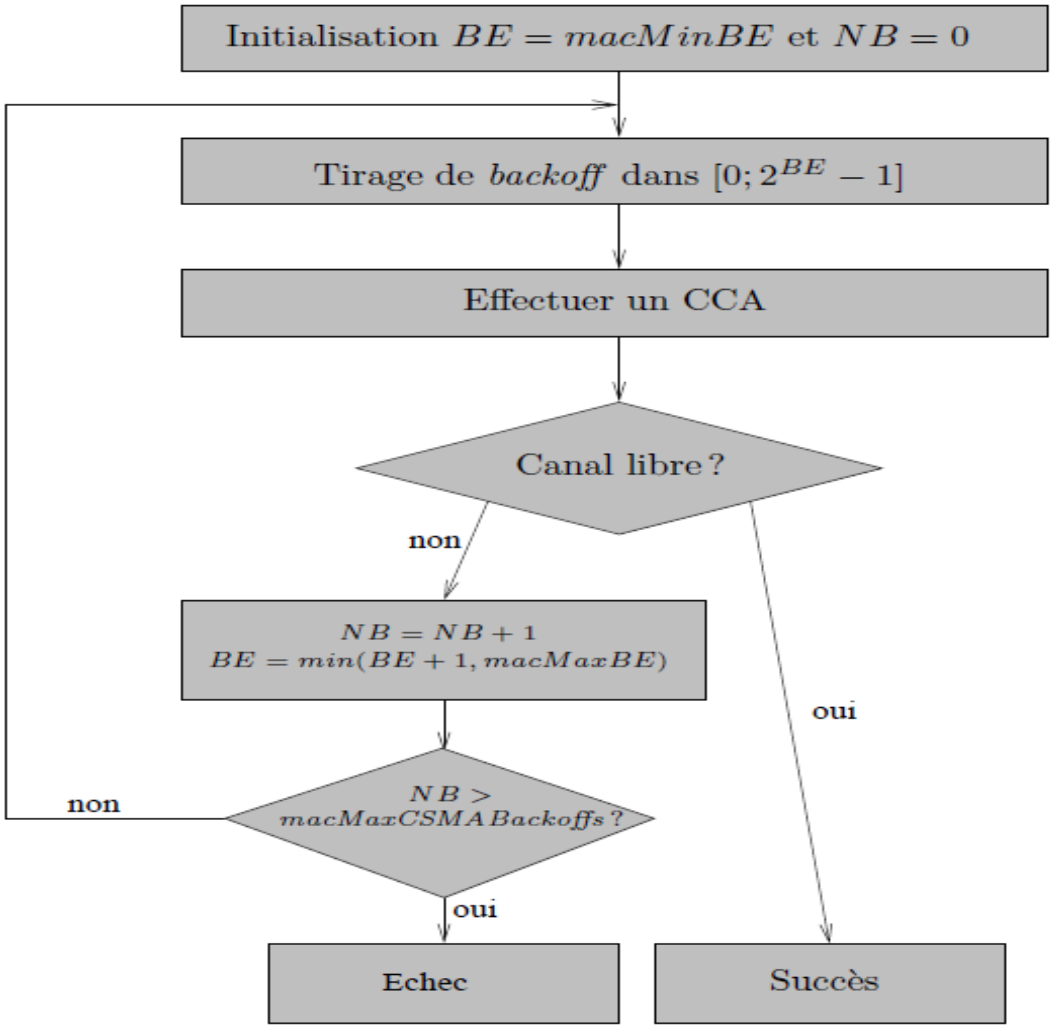
Slotted CSMA/CA

- 3 essential parameters:
  - BE: Backoff Exponent
    - Starting value: 3
  - NB: Number of Backoffs, number of times that a backoff has been chosen
    - Starting value: 0
  - CW: Contention Window, number of consecutive CCAs (different from the CW of 802.11!)
    - Starting value: 2

Slotted CSMA/CA algorithm



Unslotted CSMA/CA



Part 5:
ZigBee

ZigBee promoters

Routing protocols in ZigBee

- ZigBee uses 2 routing protocols:
  - A simplified version of AODV used in mesh topologies
  - Hierarchical routing protocol used in Cluster-Tree topologies
  - Many to One and Source Routing used when the number of destinations is small

Hierarchical addresses

- Hierarchical addresses are allocated according to nodes position in the topology
- The topology in which they are used is the Cluster-Tree
- Parents allocate addresses for its children
- Each intermediate node in the topology is also allocated an addresses pool
- These pools are separated to avoid conflicts

Pool allocation

- A formula called Cskip (Cluster Skip) is used to avoid conflicts in pools
- It is a function of depth (d), maximum allowed children (Cm), maximum allowed children routers (Rm), and maximum allowed depth (Lm)

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

Address allocation

- Only routers are allowed to allocate addresses
- During the join phase, if the new node joining the network is the n^{th} router his address will be:

$$A_n = A_{parent} + 1 + Cskip(d)*(n-1)$$

- If the new node is the n^{th} end-device, his address will be:

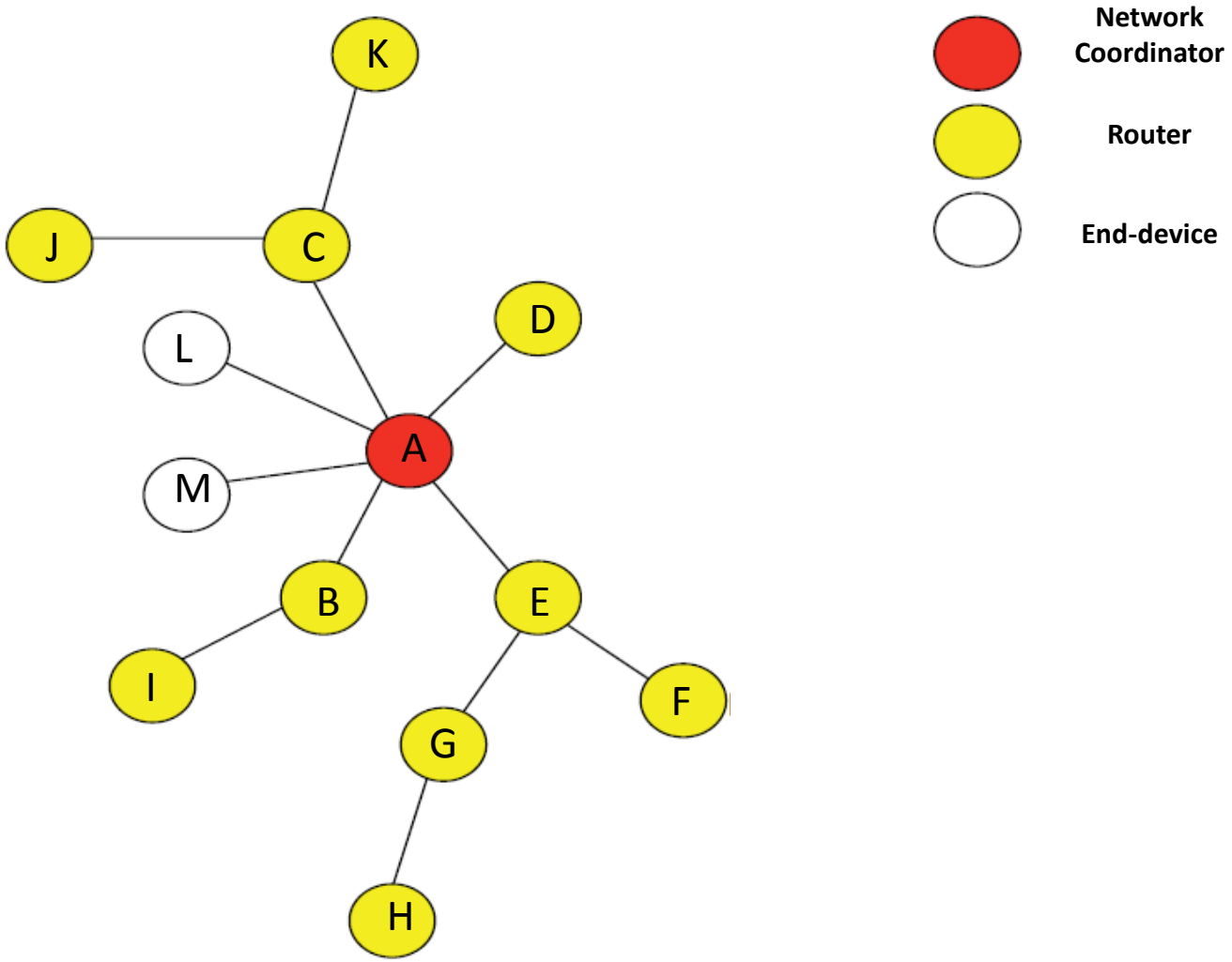
$$A_n = A_{parent} + Cskip(d)*Rm + n$$

- Where *d* is the depth of the parent

Example with Lm=3, Rm=4, Cm=6

Depth in the Network, *d*	**Offset Value, *Cskip(d)***
0	31
1	7
2	1
3	0

Address allocation



Hierarchical routing protocol

- Hierarchical addresses will allow nodes to route packets towards destinations without maintaining routing tables nor doing route requests
- The address of the node will indicate the next hop that will lead towards the position of the node in the topology

Next hop

- The next hop (N) for a given destination (D) is given as follows:
  - If *A < D < A + Cskip(d-1)* then
    - If *D > A + Cskip(d)*Rm* then

      N = D
    - Else

$$N = A + 1 + \left\lfloor \frac{D - (A+1)}{Cskip(d)} \right\rfloor \cdot Cskip(d)$$

  - Else

    N = parent address

References

- Unless otherwise specified, all figures are taken from open standards documents or personal documents