Wirless Networks And Mobile Applications

Year 2022-2023

Authors:
Alessandro Cavaliere
Brugnolaro Filippo

Disclaimer

Hello guys!
These notes contain all the concepts and arguments which are explained during professor's lessons. However they are not intended in any sense as a replacement for professor's lessons, but as a help for studying and preparing the exam. There could be also the presence of some errors and we don't take any responsibility for them. If you like to contribute for any correction, here is the link to the repository:

`https://github.com/filippobrugnolaro/WNMA-notes`

You can create a new branch with all modifications and create a pull request. We'll be pleasured for any correction in order to improve the quality of the document.
Hope it could be useful.
Cheers :)

Contents

1 Introduction

1.1 Wireless Development

Present
it is constantly growing due to higher use of laptops or devices which can connect to internet. This implied an important growth of WiFi and n-G (3G, 4G, 5G) technologies also thanks to the emerging of apps with both low and high data demand. Smartphones open to new wireless scenarios such as AR, VR, MR, tele-presence...
Other topics are Tactile Internet (combination of low latency, high availability, reliability and security) and Web Squared (integration of web 2.0 with technologies of sensing).

Future
it is based on ubiquitous communication among people and devices. So this implies to take into account some requirements such as bandwidth, delay, energy and connectivity.

Challenges

- Wireless channels are a difficult and capacity-limited broadcast communications medium (with respect to the wired counterpart);
- Traffic patterns, user locations, and network conditions are constantly changing;
- Applications are heterogeneous with hard constraints required by the network;
- Energy and delay constraints change design principles across all layers of the stack.

Multimedia requirements

	Voice	Data	Video	Game
Delay	low	irrelevant	low	low
Packet Loss	low	no	low	low
Bit Error Rate	10^{-3}	10^{-6}	10^{-6}	10^{-3}
Data Rate	8-32 Kbps	1-100 Mbps	1-20 Mbps	32-100 Kbps
Traffic	Continuous	Bursty	Continuous	Continuous

One-size-fits-all protocols and design

- are used by wired networks → poor results;
- do not work well → Crosslayer design.

Crosslayer Design

It's made of 5 layers:

Application	→ Meet delay, rate and energy constraints
Network	→ Adapt across design layers
Access	→ Reduce uncertainty through scheduling
Link	→ Provide robustness via diversity
Hardware	

1.2 Wireless Systems

There are different types of current wireless systems:

- Cellular Systems;
- Wireless LANs;
- Satellite Systems;
- Bluetooth;
- ...

And others which are emerging:

- Ad hoc Wireless Network;
- Mesh Network;
- Sensor Network;
- Distributed Control Network;
- MANET/VANET/FANET;
- Underwater Networks;
- RFID;
- Nano-networks;
- ...

1.2.1 Cellular Systems

Characteristics:

- every geographic region is divided into cells
  - → more transmission distance ⇒ more power;
- frequency/timeslots/codes are reused at separated locations;
- co-channels interference between same color cells;

- base stations has control of functions and handoff;
- it can be shrinked to increase capacity and relax networking burden.
- it supports both voice (continuos) and data (bursty) requiring different:
  - → access
  - → routing strategies
- About connectivity:
  - → 3G: packet-based switching for both voice and data (up to 7.2 Mbps)
  - → 4G - 5G: are more focused on data (high bandwidth, high reliability, low latency)

1.2.2 Wireless Local Area Networks (WLANs)

Characteristics:

- devices are connected (wireless) to an AP[1]
  → it is wired-connected to internet;
- breaks data into packets (≈ 1500 B) → AP[1] in even smaller size (500 B);
- MAC layer control access to shared channel (random access);
- backbone internet provides best-effort service
  - → bandwidth cannot be determined!
  - → users pay subscription only for home-access provider distance
    ⇒ it can be bottleneck if the backbone is faster
  - → having QoS (subscription) here can increase digital gap

$$\text{Server} \to \text{Internet} \to \text{Access Provider} \to \text{Access Point} \to \begin{cases} \text{device1} \\ \text{device2} \\ \ldots \\ \text{deviceN} \end{cases}$$

There are different versions (802.11):

- b (old gen): only 2.4 GHz, speed 1-11 Mbps, range 100m
- g (legacy std): 2.4-5 GHz, speed up to 54 Mbps
- n (current gen): 2.4-5 GHz, speed up to 300 Mbps, multiple I/O
- ac (emerging gen): 2.4-5 GHz, speed up to 500 Mbps, multiple I/O
- s: used for mesh networks
- p: used for vehicular networks

[1] Access Point

1.2.3 Satellite Systems

Satellites haven't been used so much until starlink which is gaining popularity because, even if they make light pollution, they are very lightweight and easy to wake up. There are many types of satellites:

- GEO (Geostationary Earth Orbit);
- MEO (Medium Earth Orbit);
- LEO (Low Earth Orbit).

In particular satellites:

- can cover large areas depending on their height in the space:
  - → $>$ height $\Rightarrow$ $>$ covered area, $>$ latency, $<$ bandwidth
  - → $<$ height $\Rightarrow$ $<$ covered area, $<$ latency, $>$ bandwidth
- for one-way transmission are optimised (i.e. radio and movie broadcasting);
- for two-way transmission are given up because of costs and few ambitions.

1.2.4 Bluetooth

Characteristics:

- it is a low cost replacement for cables;
- it covers a short range up to 100m with multihop
  → it requires exponential energy as distance grows
- frequency 2.4 GHz
- 4 channels (3 for voice, 1 for data up to 700 Kbps)
- Widely supported by telecommunications, PC...
  → it is a standard de facto (also BLE...)

1.2.5 Ad Hoc Networks

Characteristics:

- it is a peer-to-peer communications (born for military purposes)
- there isn't any backbone infrastructure
- routing is very hard because of:
  - → dynamic topology;
  - → typically multihop → to extend coverage area or reduce interferences

Problems:

- hops;
- bandwidth;
- collsions handling;
- energy consumption;
- topology;
- dependency on device.

1.2.6 Mesh Networks

Characteristics:

- Ad hoc opportunistic extension of a fixed urban infrastructure
  → full of wireless acess point which can connect to other ones
- it is easier than ANET because of almost static topology;
- creation of wireless coverage which is:
  - → low-cost
  - → easily deployable
  - → high performancing
- Challenges to face:
  - → QoS
  - → routing protocols optimisation for fairness and load balancing
  - → automatic setup on infrastructure's failures

1.2.7 Sensor Networks

Characteristics:

- there is at least one sensor as device in the network;
- energy is the principal constraint (low or no battery)
- data flows to centralised locations;
- low per-node rate → up to 100K nodes and they can cooperate in:
  - ⋆ transmission
  - ⋆ reception
  - ⋆ compression
  - ⋆ signal processing

1.2.8 Distributed Control over Wireless Links

Characteristics:

- it is a possibile scenario where there is contorl over something;
- it has to be robust to failures;
- Packet loss and delays impact controller performance;
- used mainly on autmated vehicles such as cars, UAVs...

1.2.9 Mobile Ad Hoc Networks (MANET)

Characteristics:

- ANET with a dynamic topology using:
  - → Infrastructure Network (WiFi or 3G/4G)
  - → Ad Hoc Multihop wireless Network
- Instantly deployable and re-configurable (for temporary needs);
- Portable (i.e. sensors) and mobile (i.e. cars);

1.2.10 Opportunistic Ad Hoc Networks

Characteristics:

- they are created when needed;
- Driven by “commercial” application needs:
  - → Indoor WLAN extended coverage
  - → Bluetooth sharing
  - → Peer-to-Peer networking on vehicles
- Access to internet available
  → BUT if too costly or inadequate ⇒ replacement with Ad Hoc Network

1.2.11 Vehicular Ad Hoc Networks (VANET)

Characteristics:

- ANET for vehicles
- it has 1000m range
- it supports 5.9 GHz
- it has 6-27 Mbps data rate depending on range
- it is more predictable → it may deduce infos ⇒ useful for crosslayers

1.2.12 Flying Ad Hoc Networks (FANET)

Characteristics:

- ANET for flying objects (i.e drone, mixed vehicles. . .)
- there is a 3D topology → protocols needs to be redesigned

1.2.13 Underwater Sensor Networks

Characteristics:

- communication happens by sound → messages propagate in circles;
- important to compute when message arrives → avoid collisions.

1.2.14 Radio Frequecy IDentification (RFID)

Characteristics:

- it is based on tags (low cost), readers (high cost) and eventually a server;
- tags can have:
  - ⋆ no battery → emitter charges the tag with energy (steal control,...)
  - ⋆ battery → tag periodically emits its ID (check of product history, control with sensors,...)
- systems can be built:
  - → lot of tags + one emitter ⇒ cheap
  - → lot of emitters + one tag ⇒ expensive
- it can identify specific instance of a product! (not only type like barcode)

2 Radio Frequency

Most wireless communications are based on this technology.

2.1 Properties

Here is some characteristics and properties of radio freuquency:

- Antenna:
  - → it has high frequency alternate current ⇒ generates electromagnetic energy
  - → it converts wired current to radio frequency and viceversa
  - → it can produce radio frequency with different frequency/amplitude
    → as signal propagates ⇒ it becomes weaker and weaker
- Frequency → it is the number of waves in a second:
  - → there is a wireless spectrum (regulated and free areas)
  - → wavelenght = $\frac{c}{\text{freq}}$ ⇒ distance between spikes
    → it gives antenna's recommended lenght
    → it works better if size is $\frac{1}{2^n}$ lenght of wavelenght
- Amplitude:
  - → higher amplitude signals ⇒ it goes further
  - → transmission power = $\frac{\text{energy}}{\text{time}} \rightarrow \frac{\text{joule}}{\text{s}}$
- Coverage:
  - → as distance grows ⇒ signal becomes weaker in an exponetial decline
    → you can detect a weak signal → but you can't really use it
    (weak for exchanging messages)
  - → problems:
    - ∗ obstacles → can reflect or absorbe waves
      → it depends on material and frequency
      → rules of thumbs
      - · high frequency → short distances, more affected by obstacles
      - · low frequency → long distances, less affected by obstacles
    - ∗ phase shifting → positve/negative aspects → early/late wavefront
      → signals can be null and overlap each other
  - → polarisation → phisical orientation of antenna
    - ∗ radio frequency is made up of 2 perpendicular fields (electric/magnetic) ⇒ the presence of:
      - · Horizontal polarisation → electric field parallel to ground
      - · Vertical polarisation → electric field perpendicular to ground → if 2 antennas are perpendicular to ground ⇒ better transmission

2.2 Wireless Transmission

It happens through elettromagnetic waves. There is a dependency on amplitude, frequency and phase values → each combination produces a new signal

Characteristics:

- Range:
  → Transmission: communication possible, low error rate
  → Detection: detection of signal, no exchanging messages
  → Interference: no detection for too much noise depending from many factors (distance, enviroment...)

  Detection requires more energy than communication
- Propagation:
  → it is at the light speed in free spaces
  → receiving power dipends from distance between sender/receiver
  rp = $\frac{1}{d^2}$ → rp influenced by:
    * fading (dependent on frequency)
    * shadowing (obstacles)
    * reflection (large obstacles)
    * refraction (density of obstacles)
    * scattering (small obstacles)
    * diffraction (at edges)

  → signal can follow different paths due to refraction, scattering, diffraction. So there is:
    * Time dispersion → signal is dispersed over time
    * Phase shifting → signal is distorted
- Power measurement
  → It is the Decibel (dB) → expression power loss
  → It is more pratical to use logarithmic decay → easy calculations
  → Decibel measures the logarithmic relative strenght between 2 signals
  → Values of power measuements:
    * positive → power gain
    * negative → power loss

2.3 Antennas

Characteristics:

- it converts electrical energy in radio frequency waves (transmission) and viceversa (reception)
- its size → depends on radio frequency of transimission/reception
- its shape → depends on radio frequency radiation pattern
- position important to have max coverage

There are different types of antennas:

- Omnidirectional antennas
- Semi-directional antennas
- Highly-directional antennas
- Sectorised-directional antennas

2.3.1 Omnidirectional antennas

Characteristics:

- radio frequency power is equally distributed in all direction around Y-axis
- used when:
  → need of uniform radio coverage
  → point-to-multipoint connections (star topology)
- Tilt → it is degree of inclination of antenna with respect to Y-axis
- Example of dipole antenna
  → passive gain due to concentration of radiations
  → active gain obtained with power amplifiers
  → signal is weak near the dipole
  → there is also:
    * low gain → high signal near antenna, low far
    * high gain → low signal near antenna, high far

2.3.2 Semi-directional antennas

Characteristics:

- radio frequency power is equally distributed only on $\frac{1}{2}$ direction (also few goes behind that direction)
- Types:
  → Patch → flat antennas mounted on walls
  → Panel → flat antennas mounted on walls
  → Yagi → rod with tines sticking out

2.3.3 Highly-directional antennas

Characteristics:

- radio frequency power is distributed on a specific direction and antenna could be as:
  - → parabolic dish
  - → grid
- it is used for long distances → point-to-point link
- there is what is called LoS (Line of Sight):
  - → straight line between sender and receiver
  - → needs no obstruction
- there is also the Freshnel Zone:
  - → it is an area which is centered on LoS axis
  - → most additive radio frequency signal is concentrated here
  - → there is the need of no obstacles
    (useless increasing power if Freshnel Zone is not free)
  - → it depends on distance and frequency
    ⇒ there is no dependency from type, degree, gain of antennas

2.3.4 Sectorised-directional antennas

Characteristics:

- there are multiple antennas → each one points to a direction
- it is applied the space multiplexing (channel reuse)
  ⇒ assigned the same frequency for antennas which do not collide each others

3 Wireless Physical Layer

There are different frequency areas which can be regulated or free.

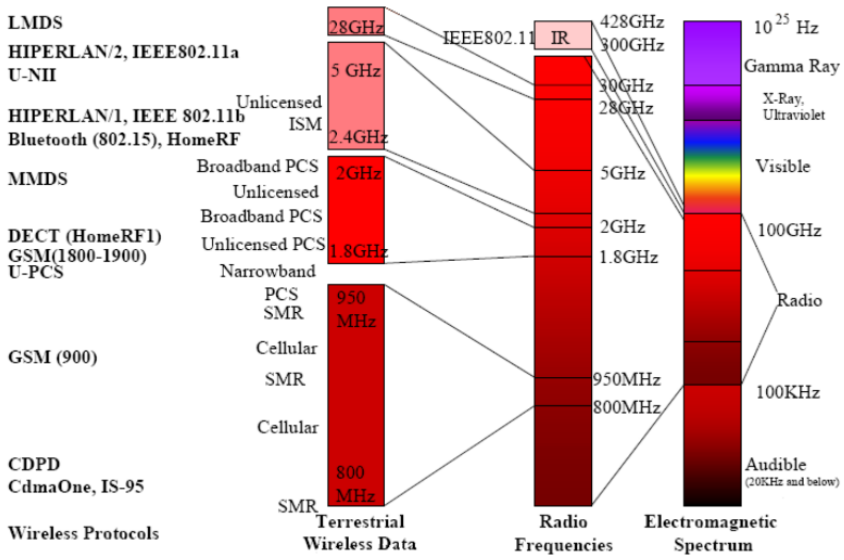


Figure 1: Wireless spectrum

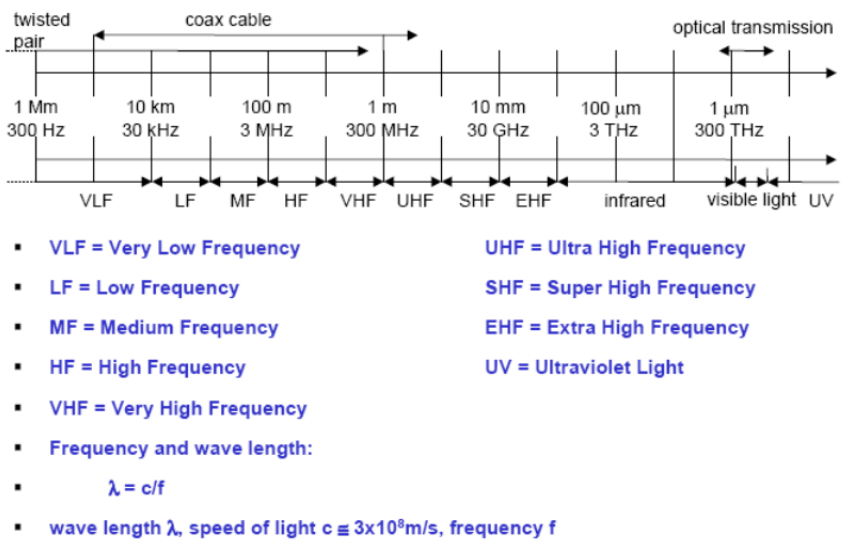


Figure 2: Wireless frequency

3.1 Characteristics

In this section there is some description about the main concepts of wireless physical layer

Bandwidth → maximum transfer capacity

- it can vary between each wireless channel
- bits go at the same speed (light physical limit) → gain in encoding/decoding
- spectrum can be bigger → more space ⇒ more risks (errors, interferences, ...)
- time to accomodate (less time, ...)

Coverage

- both isolated ⇒ they can't hear each others
- if A receives B, but B don't receive A ⇒ unidirectional link
- if A receives B and viceversa ⇒ bidirectional link
- Bidirectional links can be:
  - → symmetric: A & B communicate with same speed
  - → asymmetric: A & B communicate with different speed

Technology

There are different types of technologies used for wireless networks:

- Narrowband Radio System
  - → used for long distance, LoS needed
  - → send/receive using a single, licensed, narrowing radio frequency
  - → cross-talks require coordination/license for each site (low rate)
- Spread Spectrum it can be of 2 types:
  - → Frequency Hopping Spread Spectrum
    - * it can changes frequency in the way which is known by the receiver/transmitter
    - * uninteded receivers may listen to FHSS[2] as impulse noise
    - * lower power/cost/throughput than DSSS[3]
  - → Direct Sequence Spread Spectrum
    - * reduntant bit pattern spreded over a large spectrum
      → long chips can increase the possibility to recover the original bits
      ⇒ it may avoid retransmission

[2] Frequency Hopping Spread Spectrum
[3] Direct Sequence Spread Spectrum

    * uninteded receivers may listen to DSSS[4] as low power wideband noise
    * high performance, low interferences, good security, more expensive

- Infrared
  → it is just below visible light ⇒ it can't go beyond obstacles
  → LoS is the key (it limitates mobility) → short range (indoor, LANs, ...)
  → high data-rate potential
  → high bandwidth, easily obstructed, inexpensive

	PROS	CONS
Frequency Hopping Spread Spectrum (FHSS)	• Use less power than DSSS • Lower cost • Increased security due to frequency switching	• Lower throughput than DSSS
Direct Sequence Spread Spectrum (DSSS)	• High performance • Low interference • Increased security due to chip coding	• Expensive
Narrowband Microwave	• Long distance	• Line-of-sight with satellite dish • Requires FCC license • Not designed for WLAN use
Infrared	• High bandwidth	• Easily obstructed • Inexpensive

Figure 3: Wireless technologies comparison

Coverage Areas

There are different coverege areas:

- Wireless Wide/Metropolitan Area Network (WWAN & WMAN)
  It is characterised by the use of:
  → satellites
    * GEO → 3 of them cover the entire world → 500ms Round Trip Time
    * LEO → more mobility, low coverage → nodes have to switch between them
  → cellular/multistructure WLAN
    * lots of Access Point all connected to local Mobile terminals
    * local Mobile terminals connected to internet backbone

[4] Direct Sequence Spread Spectrum

- Wireless Local Area Network (WLAN)
  It can be of 2 types:
  - → Ad-Hoc
    - * it is a Peer-to-Peer "on the fly" communication
    - * there is no adminstration, no setup, no costs
  - → Infrastructure
    - * it is a centralised control unit (Access Point + Local Server)
    - * there is roaming between cells
    - * there is resource sharing and backbone connection
- Wireless Personal Area Network (WPAN)
  - → it is used for alternative cable connection for in-home/offices
  - → common protocols are HomeRF, Bluetooth, ...

Enviroment

There are some challenges to take into account:

- capability to maintain needs for apps/services
- limited resources such as bandwidth, energy (battery constraints) ...
- device limits (I/O, keyboards, mouse, ...)
- mobility(number of users in the system, ...)
- QoS[5] problems, reliability, negotiation...

Multiplexing

- Goal → to reach the multiple use of a shared channel
  ⇒ bandwidth to a large amount of devices
- There are multiple options and each one needs to have a guard spaces
  ⇒ avoid interferences, ...
- Types:
  - → Space Multiplexing:
    - * devices are far away from each other
    - * devices have all the same frequency → no interference
    - * guard → safety physical space
  - → Frequency Multiplexing:
    - * channel's spectrum is divided into smaller bands
    - * host use a single piece for the whole time

[5]Quality of Service → guarantee a certain amount of bandwidth

- * guard → safety frequency between bands
- * Pros:
  - · no dynamic coordination
  - · it works also for analog systems
- * Cons:
  - · inflexibility → traffic unbalanced ⇒ bandwidth waste

→ Time Multiplexing:

- * one carrier (round-robin) at a time uses the whole bandwidth
- * guard → time between transitions
- * Pros:
  - · high throughput for many users
- * Cons:
  - · require precise synchronization

→ Code Multiplexing:

- * how it works:
  1. each channel has a unique code
  2. each medium transmits at the same time
  3. messages overlapping
  4. signal combination
  5. receiver decode only what of interest
- * Pros:
  - · no synchronization
  - · more bandwidth
  - · good protection in security/interferences
- * Cons:
  - · lower data rates
  - · more expensive → it needs to regerate the signal (receiver)

3.2 Wireless vs Wired

Here there is a comparison between wireless and wired networks.

Attribute	Wireless PAN/LAN	Wired PAN/LAN
Throughput	10-100 Mbps	10-100 Mbps (and more)
Integrity & Reliability	Subject to interference	Highly reliable
Simplicity/ Easeof Use	• No need to pull cable • Set up time is significantly lower • Moves, additions & changes much simpler	• Cable required • Set up time is significantly higher
Security	• Suscptible to interception • Encrption	• Not as susceptible to interception
Cost	• Initial HW investment high • Intallation expenses and maintainance low	• Initial HW investment low • Intallation expenses and maintainance high
Scalability	Simple to complex networks	Simple to complex networks
Safety	Little exposure to radio frequency energy	No exposure to radio frequency energy
Mobility	Provides access to real-time info anywhere	Does not support mobility

Figure 4: Wireless vs wired comparison

4 MAC Layer

4.1 Introduction

Multiple Access Control (MAC) layer:

- it is a media access control protocol in which there is:
  - → coordination and scheduling of transmissions
  - → hosts competing for having the channel
- Access control
  - → it is referred to shared channel
  - → broadcast of wireless transmission (at the light of speed)
  - → who can transmit when/where
  - → collisions → avoid/recover from them with detection or not
    ⇒ the problem is receiving at the same time (NOT SENDING)
- Goals:
  - → low latency
  - → good channel utilization (no collisions → using it as much as possible)
  - → best effort + real time support

  As in a human conversation:
  - → Everybody should have the chance to talk
  - → Do not speak until it is your turn
  - → Do not monopolize the conversation
  - → Raise your hand if you have to ask for something
  - → Do not interrupt while somebody is talking
  - → Do not fall asleep while somebody is talking

  So the most important concepts are:
  - → efficiency in the bandwidth use → the maximum possible
  - → resilience → avoid collisions
  - → fairness → given n nodes and a bandwidth b, each one should have a bandwidth $b_n = \frac{b_{tot}}{n}$
  - → robustness → decentralised, no single point of failure
  - → simplicity → easy to implement
- Channel Access Problem
  - → there is a multiple nodes share channel
    ⇒ simultaneous communication is not possible

→ MAC proocols give schemes to schedule communication
  * maximise number of communication → avoid collisions
  * guarantee fairness among all transmitters
→ trivial solution is Transmit and Pray
  ⇒ plenty of collisions → poor throughput at high
→ Carrier Sense Multiple Access (CSMA):
  * it provides a fix to Transmit and Pray
  * transmitters listen to the channel before sending → waiting when signal on channel
  * collisions:
    · can still occur due to propagation delay
    · when it happens the entire packet could be lost → time wasted

4.2 MAC Protocols

MAC protocol → coordinates transmissions from different stations
⇒ minimize or avoid collisions

There a 3 different types of protocols:

- Channel partitioning (TDMA, FDMA, CDMA)
- Random Access (CSMA, MACA)
- Taking turns (polling)

Approaches to MAC layer are:

- Random Access:
  → Without carrier sensing → Pure Aloha, Slotted Aloha
  → With carrier sensing → CSMA, CSMA/CD, MACAW
- Controlled Access:
  → Centralized → entity regulate channel's access (FDMA, TDMA, CDMA)
  → Distributed → distributed apps with peer nodes regulate channel's access (Token ring)

Random Access Protocols

Characteristics:

- node transmits at random at full channel data rate
- if nodes collide then they retransmit at random times
- each one dectects/recovers form collision in a different way

Here there is the description of the most important protocols.

4.2.1 Slotted Aloha

Characteristics:

- time is divided into equal size slots → equal to full packet size
- newly arriving station transmits at the beginning of the next slot
- if collision occurs:
  → assumption of the presence of channel feedback
  → retransmission of packet at each slot with probability P, until successful
- Successful of transmission:

  given:
  - N = number of stations
  - P = probability that each station transmits in the slot
  - S = probability of successful of transmission

  the value of S is:
  - $S = p(1\text{-}p)^{(N\text{-}1)}$ by a single node
  - $S = Np(1\text{-}p)^{(N\text{-}1)}$ by any of N nodes
- throughput efficiency is about $\frac{1}{e}$ → and:
  1. obtaining $p = \frac{1}{N}$ (p should be tailored based on N)
  2. substituting p to $S = Np(1\text{-}p)^{(n\text{-}1)} \Rightarrow S = N\frac{1}{N}(1\text{-}\frac{1}{N})^{(N\text{-}1)}$
  3. solving S at the limit obtaining $S = \frac{1}{e}$
- it is fully decentralised

4.2.2 Pure Aloha

Characteristics:

- it doesn't require time slots → no synchronization
- nodes can transmit at any time ⇒ collision may increase
- Successful of transmission:

  given:
  - N = number of stations
  - P = probability that each station transmits in the slot
  - S = probability of successful of transmission

  the value of S is:
  - $S = p(1\text{-}p)^{2(N\text{-}1)}$ by a single node
  - $S = Np(1\text{-}p)^{2(N\text{-}1)}$ by any of N nodes

- throughput efficiency is about $\frac{1}{2e}$ → every transmission can occupy 2 slots → and:
  1. obtaining p = $\frac{1}{2(N-1)}$ (p should be tailored based on N)
  2. substituting p to S = $Np(1-p)^{2(N-1)} \Rightarrow S = N\frac{1}{2(N-1)}(1-\frac{1}{2(N-1)})^{2(N-1)}$
  3. solving S at the limit obtaining S = $\frac{1}{2e}$

4.2.3 Considerations Pure & Slotted Aloha

Both are:

- not efficient at all → a lot of retransmissions:
  - ⋆ Pure Aloha throughput → 18.4 %
  - ⋆ Slotted Aloha throughput → 36.8 %
- unfair → aggressive senders can capture the channel
- robust → decentralized
- simple:
  - ⋆ Pure Aloha → no coordination
  - ⋆ Slotted Aloha → just synchronization

4.2.4 Carrier Sense Multiple Access (CSMA)

Characteristics:

- Aloha protocols are less performing → lack of coordination among nodes
- Each node continuously listens to channel → awareness of channel's freedom ⇒ improve in efficiency

There are different types of CSMA:

- 1-persistent CSMA
- non-persistent CSMA
- p-persistent CSMA

4.2.4.1 1-persistent CSMA

Characteristics:

- how it works:
  1. nodes listen to the channel
  2. the channel can be:
     - → free → immediate transmission
     - → busy → waiting until channel is free → $P_R = 1$

⇒ P_R = probability of retransmission
(if there is a collision → node waits for a random time and retries ⇒ desynchronization)

- propagation time
  - → impact on performance
  - → more time ⇒ more collisions
    Example:
    A can't hear B → B is trasmitting for so much time and A want to transmit → channel is free for A but it is not ⇒ collision
  - → even with no propagation time
    Example:
    if two nodes transmit and a third is occupying the channel
    → when channel is free → all 2 transmit at same time ⇒ collision

4.2.4.2 Non-persistent CSMA

Characteristics:

- how it works:
  1. nodes listen to the channel
  2. the channel can be:
     - → free → immediate transmission
     - → busy → waiting a random time and then retry to listen
- it is less aggressive than 1-persistent CSMA

4.2.4.3 P-persistent CSMA

Characteristics:

- it is slot based
- how it works:
  1. nodes listen to the channel
  2. the channel can be:
     - → free → transmission with probability p
     - → busy → wait with probability (1-p) and then retry to listen
- Aggressiveness:
  - → it depends on p
  - → p can be choose depending to the number of nodes:
    - * many → it may be conservative
      ⇒ bandwidth waste depending on number of collisions
    - * few → it may be aggressive
      ⇒ bandwidth waste depending on time of channel not used

4.2.4.4 CSMA with Collision Detection (CSMA/CD)

Characteristics:

- it is like CSMA → but collisions are detected within few bit times
- when it is detected → transmission aborted ⇒ reduction of channel wastage
- transmission is typically implemented persistently
- collision detection can approach channel utilization = 1 in LANs
  → it can detect immediately if something is wrong
- easy detection in wired LANs → it can measure signal strength
  → on the line, or code violations, ...
- collision detection can't be done in wireless LANs
  Example:
  the receiver shut off while transmitting → avoid damaging it with excess power

4.2.5 Wireless Medium Access Control

Some basics:

- transmission strength drops exponentially as the distance grows
- there is the SINR (⇒ signal internface noise ratio)
  → calculation of how strong is signal compared to interference
- SINR threshold → bound in which signal can't be detected anymore
  - → C can hear but not receive correctly the message
  - → A can't send/listen at the same time
    Example:
    collision with A → D may not; B/C maybe
- Collision detection:
  - → A is out of C range (and viceversa), both have B on range
    → they send together ⇒ collsion at receiver B
  - → Both:
    - ∗ don't know their position
    - ∗ can only hear themselves → no listening while transmitting
    - ∗ can't determine the signal quality at receiver
  - → Two problems:
    - ∗ Hidden Terminal Problem → nodes don't know the topology
      → they transmit to same node without knowing other's transmission
      ⇒ collision
    - ∗ Exposed Terminal Problem → nodes are in each oteher range
      → transmission to different receivers → even if channel is free
      → one don't transmit thinking channel is busy

4.3 802.11 Protocol

Characteristics:

- it is a standard ratified in 1999
- aim is to have a common way to allow communication between nodes
- it is used in WLAN indoors with various version (n/ac/...)
  → frequency used are unlicensed → 2.4/5 GHz, 900 MHz
- WLAN configuration with access point or ad-hoc netowrk
- it defines both MAC and physical layer (radio frequency, header, size, ack, ...)
- definition of some terms:
  → DIFS (Distributed Inter Frame Space): time waiting for channel to be free
  → if channel is occupied ⇒ timer restarts from the beginning
  (low priority → for asynchronous data service)

  → SIFS (Short Inter Frame Space): time useful to process some procedures like:
    * CTS (Clear To Send)
    * Datas
    * ACK (Acknowledgement)

  ⇒ high priority

  → CW (Contention Window):
  → slots to be waited after a successful DIFS → 1 slot = 1 SIFS
  → if channel is occupied ⇒ timer stops and restart from there
  → if there is a collision → CW is increased at max 1024 slots
  → when succeding → CW reset to the value

  → NAV (Network Allocation Vector): time the sender declares to hold
  the medium → other nodes can go to sleep ⇒ sparing energy

There are different versions of 802.11 protocol and for accessing to MAC layer which are explained in the next sections.
Access methods are:

- MAC-DCF CSMA/CA:
  → collision avoidance via randomized back-off mechanism
  → minimum distance between consecutive packets
  → ACK packet for acknowledgements (not for broadcasts)
- MAC-DCF CSMA/CA with RTS/CTS
  → Distributed Foundation Wireless MAC
  → avoids hidden terminal problem
- MAC- PCF
  → access point polls terminals according to a list

4.3.1 CSMA version

- nodes listen before transmitting
- if the channel is:
  - → free → node begins to transmit datas
  - → busy → NAV defer access to medium
    → if it was in:
    - * DIFS → it restarts the timer
    - * CW → it stops and restarts at same timer position when newly free
- receiver returns to emitter ACK after SIFS amount of time
- how it works:
  1. transmitter waits a DIFS time ($\approx 16\mu$s)
  2. if the channel is:
     - → busy → it restarts the DIFS counter (point 1.)
     - → free → it goes to CW (point 3.)
  3. transmitter waits in the CW
  4. if the channel is:
     - → busy → it stops the timer and restarts at the sime time of CW
     - → free → it begins to transmit (point 5.)
  5. transmitter sends datas (for a max of 33μs)
  6. receiver sends back an ACK after SIFS time (9μs)
     → automatic retransmission of packets in case of transmission errors
- it is subjected to the hidden terminal problem ⇒ use of CSMA/CA

4.3.2 CSMA/CA version

It works similarly as CSMA, but it improves hidden terminal problem (not solved).

- it uses the collision avoidance (CA).

  In particular it adds:
  - → RTS (Request To Send) → it freezes stations near the transmitter
  - → CTS (Clear To Send) → freezes stations near the receiver
    → station could be possibly hidden from transmitter
    ⇒ this prevents collisions by hidden station during data transfer

  ⇒ RTS and CTS are very short → collisions during data phase are very unlikely
- nodes listen before transmitting

- if the channel is:
  - → free → nodes begin to send the RTS/CTS and datas
  - → busy → NAV defer access to medium
    → if it was in:
    - ∗ DIFS → it restarts the timer
    - ∗ CW → it stops and restarts at same timer position when newly free
- receiver returns to emitter ACK after SIFS amount of time
- how it works:
  1. transmitter waits a DIFS time
  2. if the channel is:
     - → busy → it restarts the DIFS counter (point 1.)
     - → free → it goes to CW (point 3.)
  3. transmitter waits in the CW
  4. if the channel is:
     - → busy → it stops the timer and restarts at the sime time of CW
     - → free → it begins to transmit (point 5.)
  5. transmitter sends a RTS to receiver
  6. receiver sends back a CTS to transmitter after SIFS time
  7. transmitter sends datas after SIFS time
  8. receiver sends back an ACK after SIFS time
     → automatic retransmission of packets in case of transmission errors

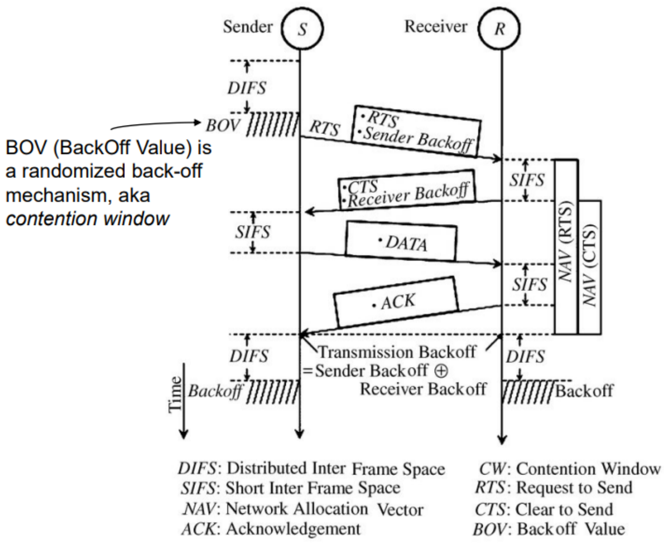


Figure 5: CSMA/CA

4.3.3 Point Coordinating Function (PCF)/Polling version

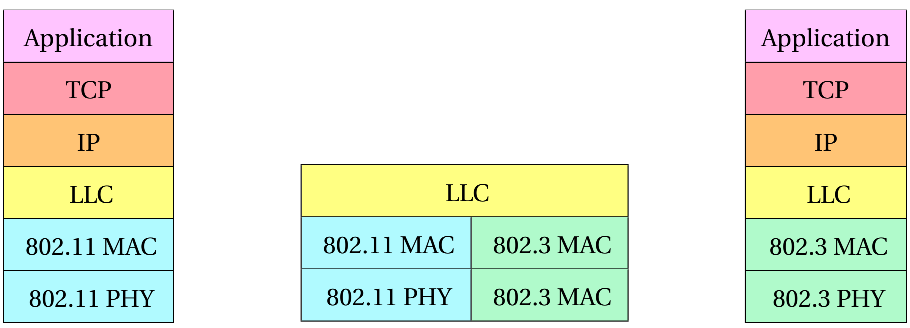
Characteristics:

- Access Point has complete control over transmissions
- it asks to each node if it has something to transmit → managed by round-robin
  ⇒ no collisions, ok with many nodes
- how it works:
  1. AP announces if it supports PCF in the beacon
  2. The AP periodically broadcasts beacons
  3. Nodes use these beacons to learn about AP
  4. The node and the AP authenticate each other:
     (a) node associates with that AP
     (b) node sends an association request management frame
     → here node announces to the AP if:
       ⋆ pollable
       ⋆ capable to transmit during the contention free period (CFP)
     (c) AP replies with an association response

4.3.4 Considerations CSMA

Some considerations about CSMA:

- exposed terminal problem → it is not improved → with CSMA is even worse
  → enlarge the detection ⇒ there are potentially more nodes
- it is always better to use RTS/CTS on CSMA/CA and polling versions because:
  → more bandwidth consumed → but probability of collision is smaller
  ⇒ it is an improvement at the cost of limited overhead of transmission
  → if data packets are very small (as RTS ones) → it is worse
- positioning → can deal with different MAC layers (802.11, 802.3)



4.3.5 Synchronization in 802.11

Characteristics:

- AP send beacons in infrastructure networks
- beacons are scheduled in beacon interval → transmission may be delayed by CSMA deferral
- timestamp contains timer value at transmit time
- Power Management approach:
  - → allow idle stations to go to sleep → save mode stored in AP
  - → AP buffers packets for sleeping stations → AP announces which station has packets buffered → message is sent with TIM[6] interval
  - → power saving station wake up periodically to listen to beacons
  - → TSF[7] assures AP and power saving stations are synchronized
  - → there is also dTIM → less frequently → stations give priority to dTIM → used for broadcasting/multicasting
- Scanning:
  - → used for
    - ∗ finding/joining networks
    - ∗ finding a new AP while roaming
    - ∗ initialising a new ad hoc network
  - → MAC layer uses common mechanism for all physical
  - → it could be:
    - ∗ active → it looks explicitly for AP
      On each channel ⇒
      send a probe → wait for probe response
      send an association request → wait for association request response
    - ∗ passive → only listen for beacons

4.3.6 Congestion Avoidance (DCF)

Characteristics:

- how it works actually:
  - → after DIFS → randomly choose a backoff time interval
  - → Countdown the backoff interval when medium is free
    → it goes stand-by if medium becomes busy in the range [0,CW]
  - → When backoff time interval reaches 0 → transmit packet (or RTS)

[6] Traffic Indicator Map
[7] Timing Synchronization Function

- Congestion control → dynamically adjusting the CW
- Counting down backoff time intervals contributes to MAC overhead
- Binary Exponential Backoff → a node fails to receive CTS
  ⇒ it double up the CW (typically max size is 1024)
  → when node successfully completes transfer ⇒ it restores CW to CW_{min}
- So about the dimension of CW:
  - → Large CW ⇒ large backoff time intervals ⇒ can result in larger overhead
  - → Small CW ⇒ probabilistically to a larger number of collisions

4.3.7 MILD Algorithm MACAW

Characteristics:

- node fails to receive CTS → it multiplies CW by 1.5
  ⇒ less aggressive than 802.11 which multiplies by 2
- node successfully completes a transfer → it reduces CW by 1
  ⇒ more conservative than 802.11 where CW is restored to CW_{min}
- 802.11 reduces cw much faster than it increases it
- MACAW: cw reduction slower than the increase
  ⇒ Exponential Increase and Linear Decrease
- MACAW can avoid wild oscillations of CW when congestion is high

4.3.8 Fairness Issue

Characteristics:

- Definition:
  - → nodes should receive equal bandwidth
  - → bandwidth should be tailored to how much they want to transmit
    ⇒ otherwise waste of time/bandwidth
- unfairness → one node has backed off much more than some other node
  (≈ channel dominance)
  → A transmits many packets before B is transmitting its first
- how MACAW tries to solve:
  1. a node transmits a packet → it appends on packet its current CW value
  2. All nodes hear CW value → use it for their future transmission attempts
  3. The effect is to reset all competing nodes to the same level
- Weighted Fair Queuing → it is assigned a weight to each node
  ⇒ bandwidth used by each node → proportional to the weight assigned

- Distributed Fair Scheduling (DFS)
  - → it is fully distributed algorithm for achieving weighted fair queueing
  - → it works well on a LAN
  - → how it works:
    1. Chooses backoff intervals proportional to packet size/weight
    2. DFS attempts to follow the centralized Self-Clocked Fair Queueing

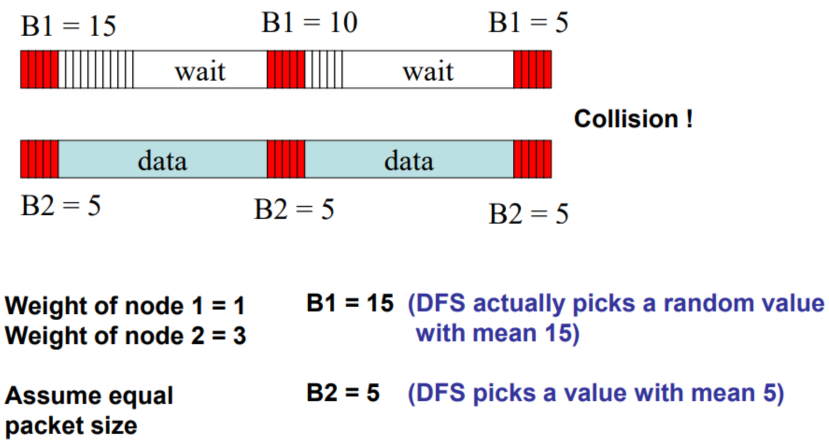


Figure 6: Distributed Fair Scheduling (DFS)

5 Network Layer

5.1 Routing protocol

Characteristics:

- it is difficult to have a direct path to destination (in ad hoc networks)
  → goal is having a good path from source to destination
  ⇒ good can be:
  - → the shortest
  - → the less expensive
  - → the fastest
- Graph abstraction for algorithms:
  - → Nodes → routers
  - → Edges → physical links
- Classification:
  - → information can be:
    - * Global → all router have complete topology
      ⇒ Ex: link state algorithm
    - * Decentralised → routers know topology only of their neighbours
      → routing table build when needed ⇒ exchange of information
      ⇒ Ex: Distance vector algorithm
  - → algorithm can be:
    - * Static → topology fixed all the time → it changes slowly
    - * Dynamic → topology changes frequently → periodic update of nodes
- Example of link state algorithm ⇒ Dijkstra algorithm:
  - → net topology → link costs known to all nodes
    - * accomplished via link state broadcasting
    - * all nodes have same info
  - → it computes least cost paths from one node to all the others
    ⇒ it gives forwarding table for that node
  - → how it works:

    Notation:
    - * $c(x, y)$: link cost from node x to y; initially = $+\infty$
    - * $D(v)$: current value of cost of path from source to destination v
    - * $p(v)$: predessor node along path from source to destination v
    - * N': set of node whose least cost path is known

Algorithm:

Initialization:
$N' = \{u\}$
for all nodes v **do**
    if v is adjacent to u **then**
        $D(v) = c(u, v)$
    else
        $D(v) = +\infty$
    end if
end for

Iterations:
repeat
    find $w \notin N' \mid D(w)$ is a minimum
    add w to N'
    for all v adjacent to w & $v \notin N'$ **do**
        $D(v) = min(D(v), D(w) + c(w, v))$ //update $D(v)$
    end for
until all nodes $\in N'$