IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Medium Access Control (MAC) - Fundamentals

Georgios Z. **PAPADOPOULOS, PhD, HDR**

e-mail: georgios.papadopoulos@imt-atlantique.fr
web: www.georgiospapadopoulos.com
twitter: @gzpapadopoulos
youtube: www.youtube.com/c/gzpapadopoulos

OSI Protocol Stack: MAC Layer

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

The 7 Layers of OSI Model

Overview

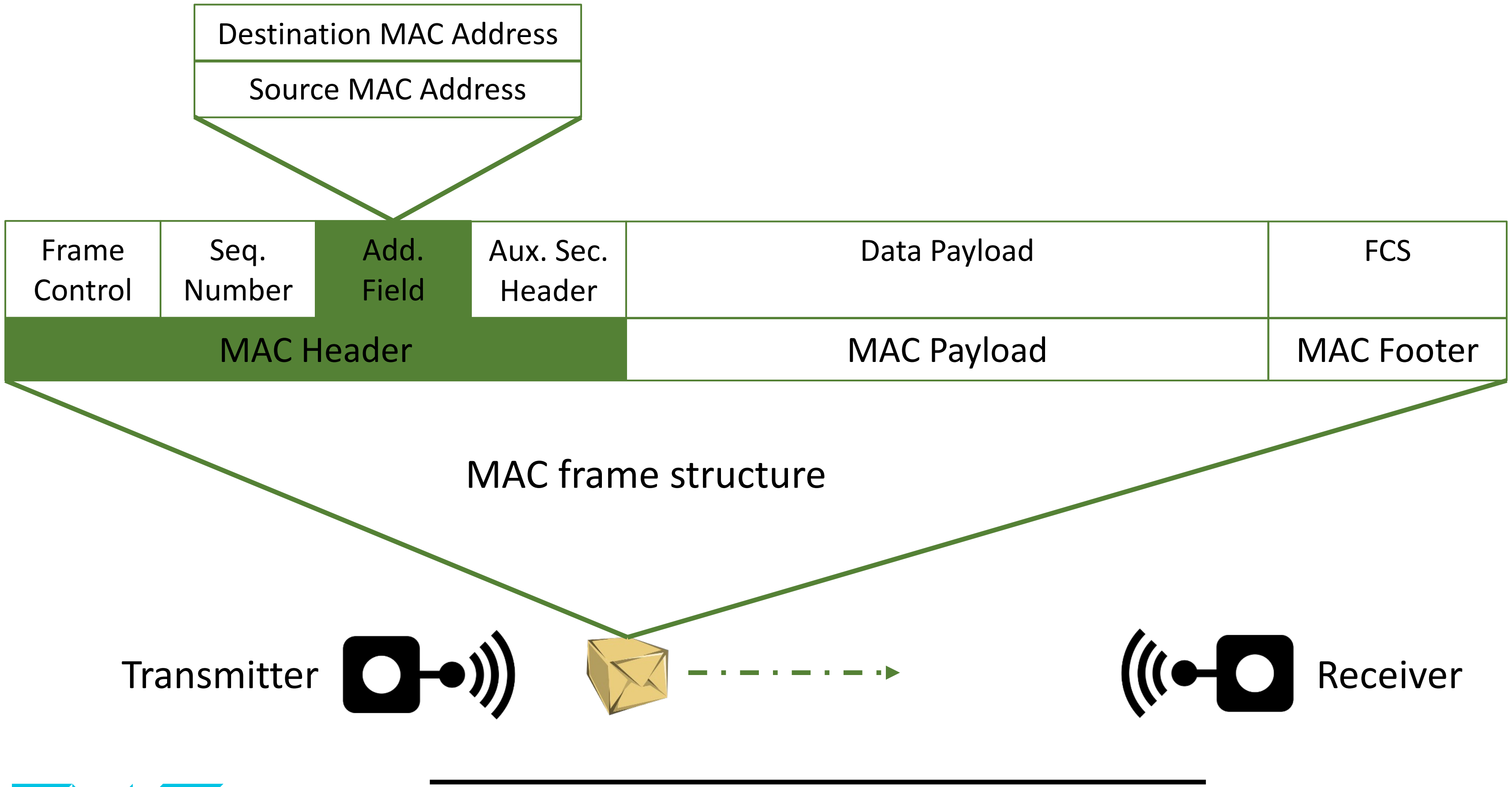
	Layer	Protocol data unit (PDU)
Host layers	7. Application	Data
	6. Presentation	Data
	5. Session	Data
	4. Transport	Segments, Datagram
Media layers	3. Network	Packets
	2. Data Link	Frames
	1. Physical	Bits

2. Data Link:

- Logical Link Control (LLC)
- Media Access Control (MAC)

Medium Access Control (MAC)

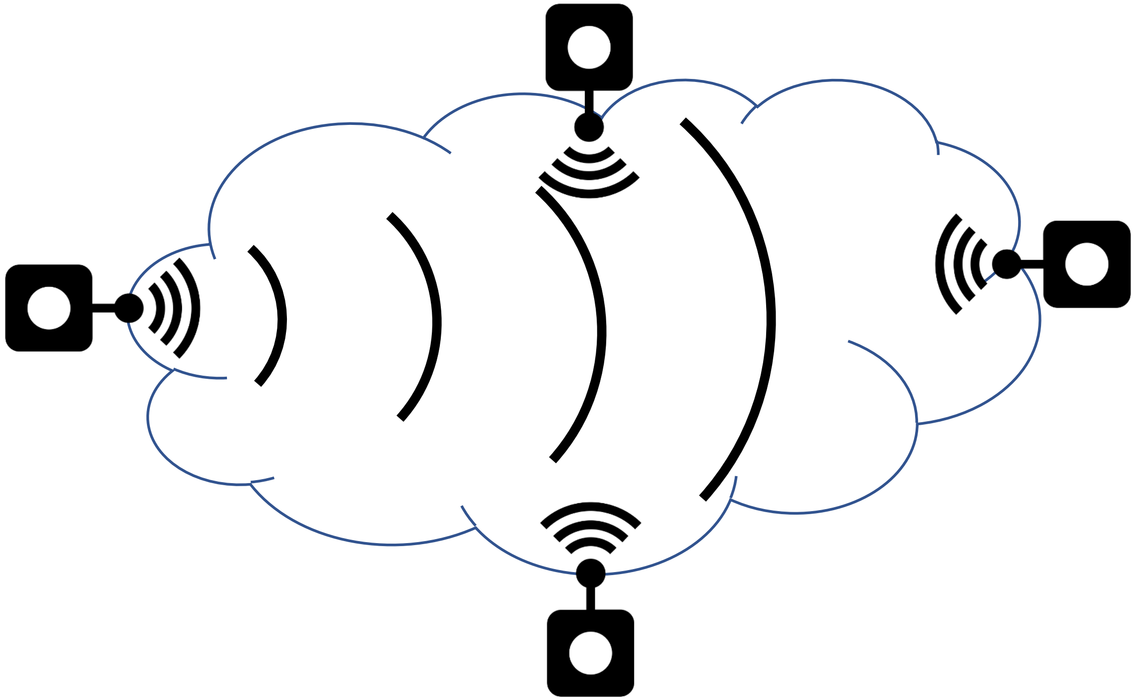
Overview



MAC frame structure

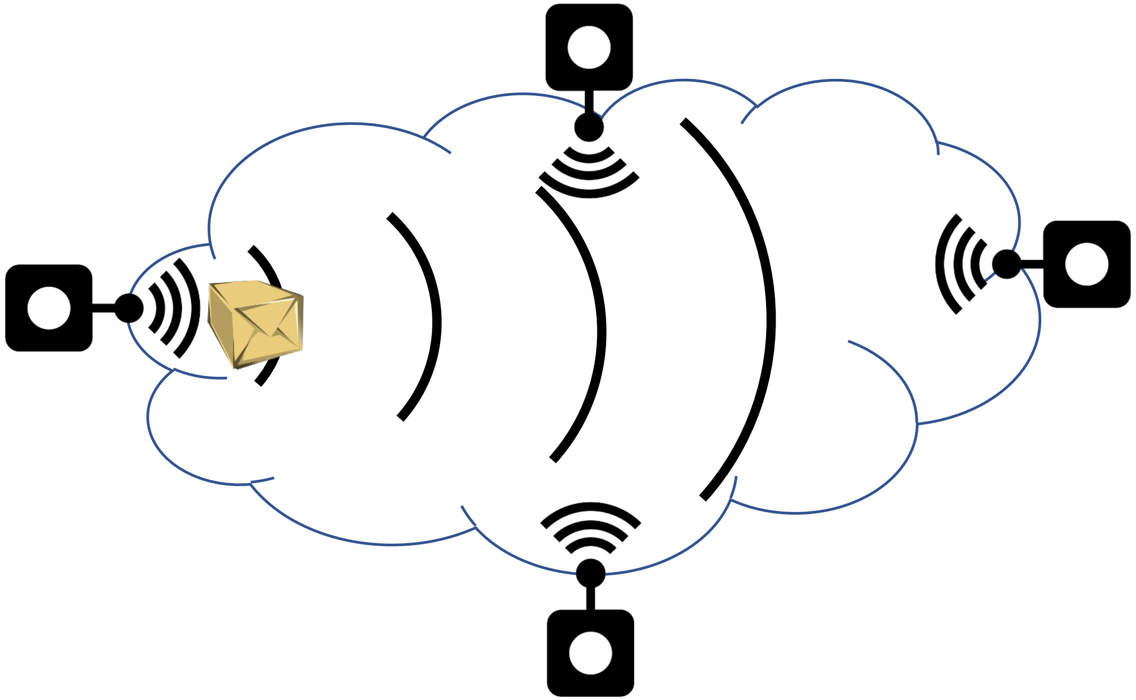
Shared Medium

Overview



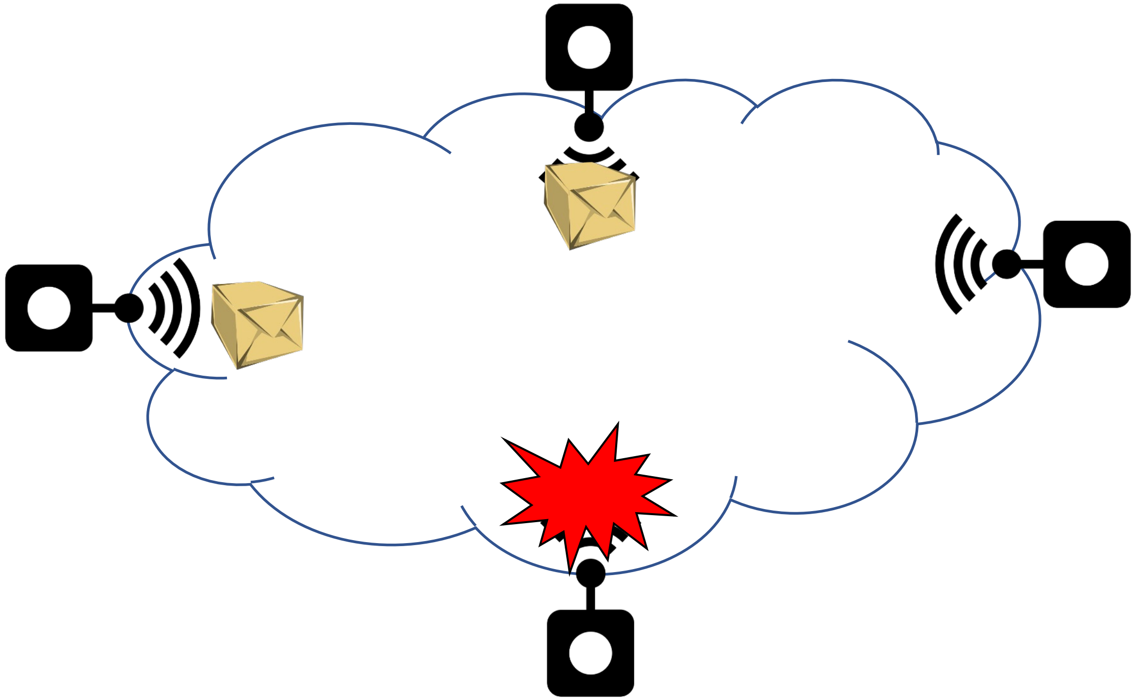
Shared Medium

Overview



Shared Medium

Overview

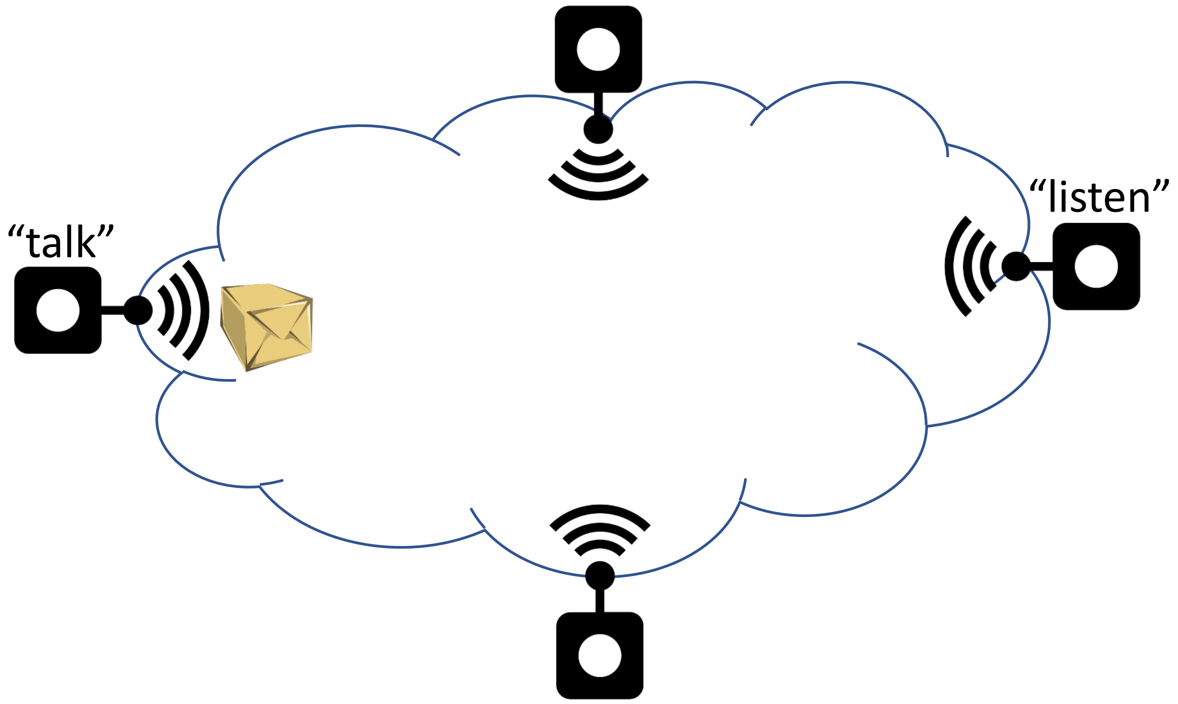


MAC Sublayer
Overview

“The MAC sublayer proposes mechanisms to avoid multiple nodes that are within the propagation range transmitting at the same time and over the same radio channel.”

MAC: regulates

Overview



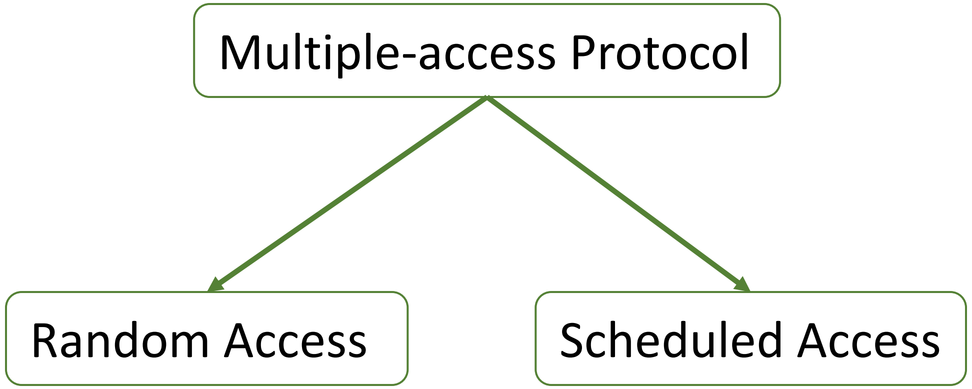
MAC: regulates

Overview

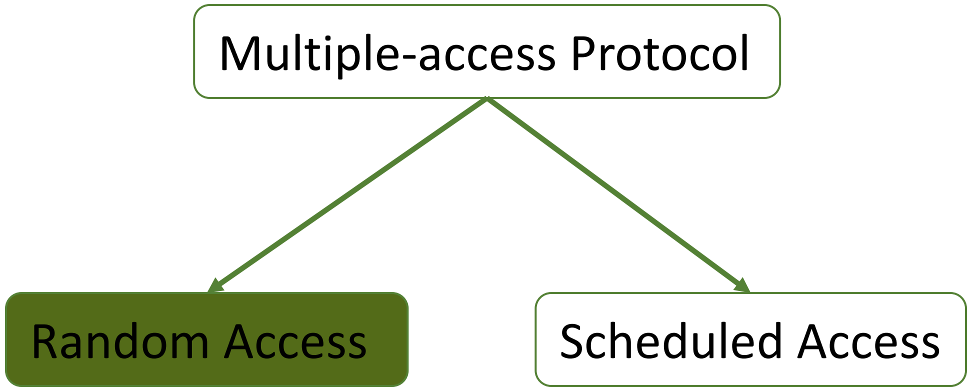
- A MAC protocol aims at :
  - Fairness: in terms of channel access and/or throughput.
  - Reliability: to guarantee the success of the transmissions.
  - Scalability: the potential to increase the size of a network.
  - Latency: reducing the time of receiving a frame.

Channel (Medium) Access Methods

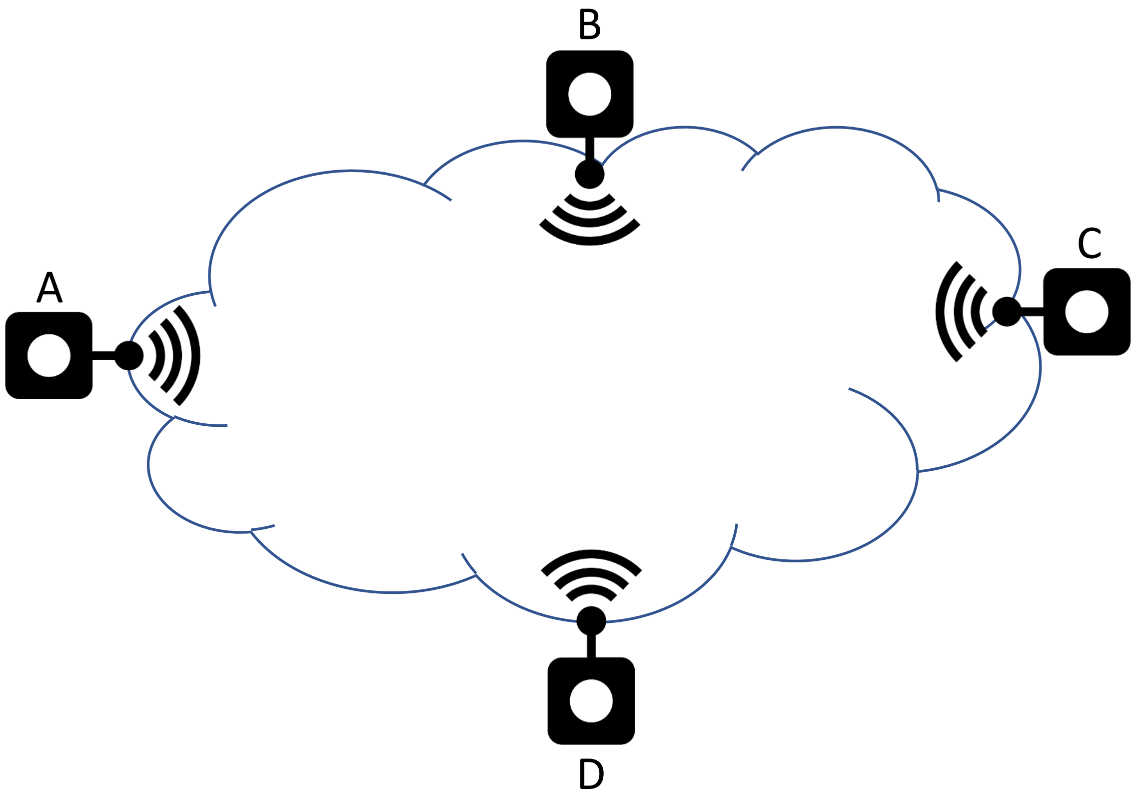
Overview



Channel (Medium) Access Methods
Overview



Random Access
Overview



All nodes are *equal*, there is not *primary/secondary* relationship.

Random Access
Overview

In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send. At each instance, a station that has data to send uses a procedure defined by the protocol to decide on whether or not to send.

Random Access

Delays

- Propagation Delay (T_p):
- Transmission (emission) Delay (T_e):
- Treatment (processing) Delay (T_t):
- Frame Transmission Time (T_{fr}):
- Round Trip Time (T_{RTT}):
- Back-off Time (T_B):

Random Access
Popular Protocols

- Pure ALOHA
- Slotted ALOHA
- CSMA (Carrier Sense Multiple Access)
- CSMA/CD (CSMA with Collision Detection)
- CSMA/CA (CSMA with Collision Avoidance)
  - CSMA/CA with ACK
  - CSMA/CA with RTS/CTS

Random Access
Popular Protocols

- Pure ALOHA
- Slotted ALOHA
- CSMA (Carrier Sense Multiple Access)
- CSMA/CD (CSMA with Collision Detection)
- CSMA/CA (CSMA with Collision Avoidance)
  - CSMA/CA with ACK
  - CSMA/CA with RTS/CTS

Check the relevant video
"*ALOHA Medium Access Control (MAC) Protocol(s)*"
on YouTube!

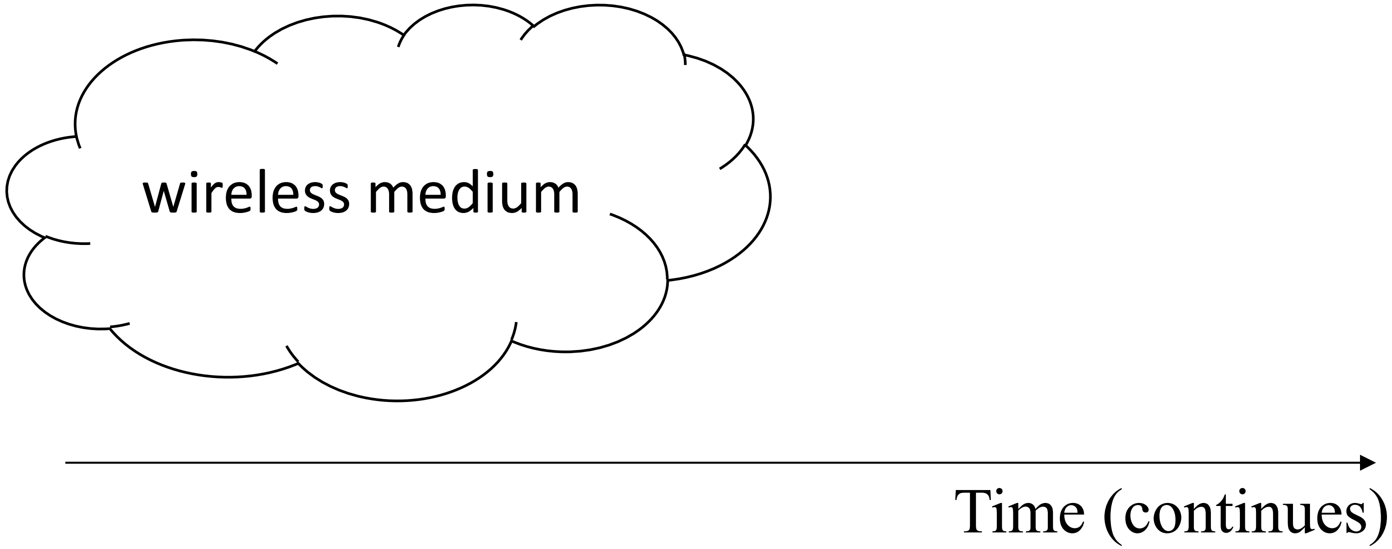
ALOHA MAC Protocols

ALOHAnet, also known as the ALOHA System, or simply ALOHA

- Dr. Norman Abramson, Dr. Franklin Kuo, and their colleagues developed the ALOHAnet at the University of Hawaii in the early 1970s to connect computers situated on different Hawaiian islands.
- In **June 1971**, the ALOHA packet radio data network began providing inter-island access to computing facilities at the University of Hawaii!
  - ***The stations of the ALOHA network transmit over the same radio channel whenever they have a packet to transmit.***
- That was the first time when a wireless packet data network was demonstrated publicly using simple **random-access protocols**, which is **one of the fundamental multiple-access protocols**.
- ALOHA is the “***father***” of multiple access protocols.

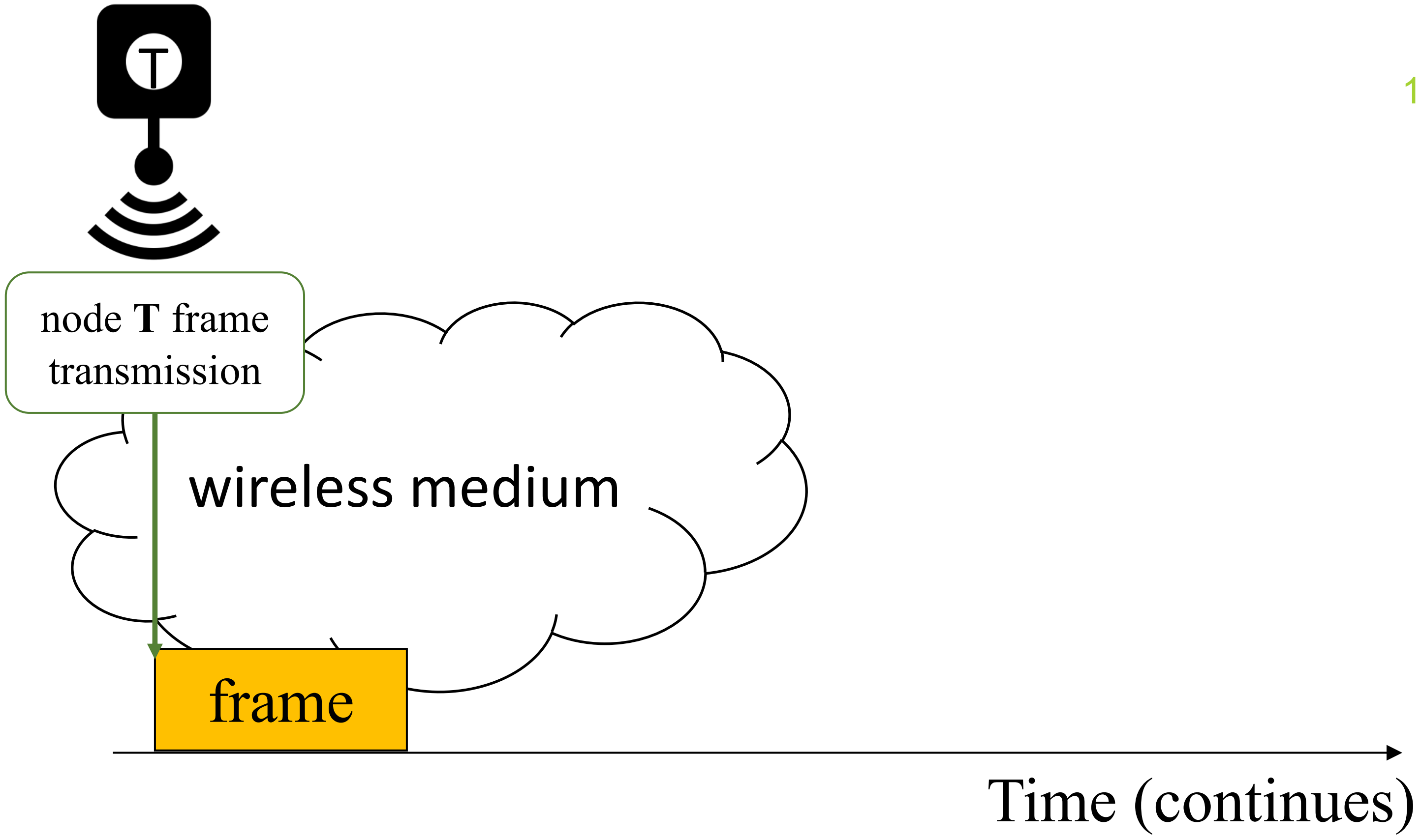
Hawaiian Islands

ALOHA MAC Protocols
Pure ALOHA



ALOHA MAC Protocols

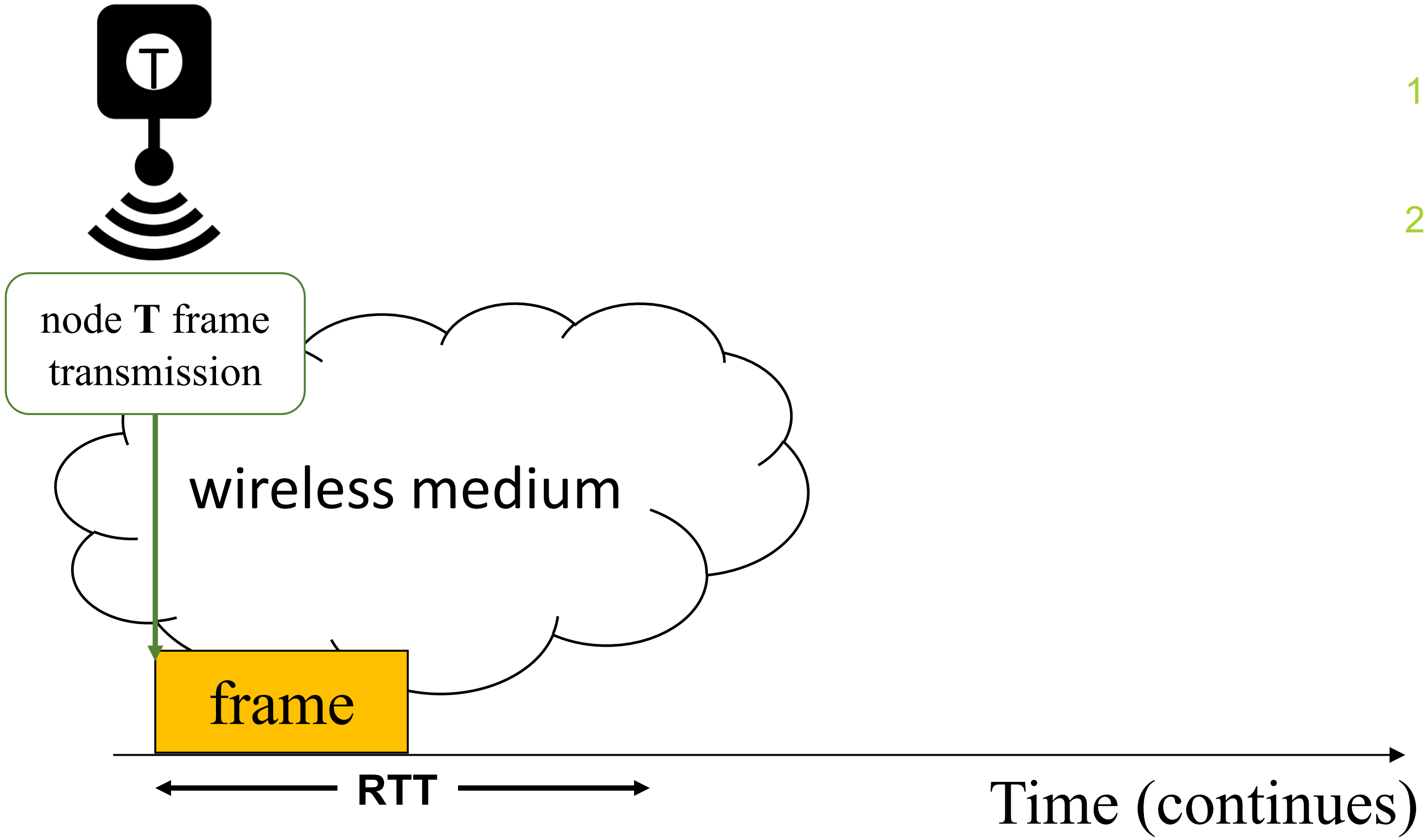
Pure ALOHA



1. Whenever a transmitting node (T) has a frame to transmit, it does so.

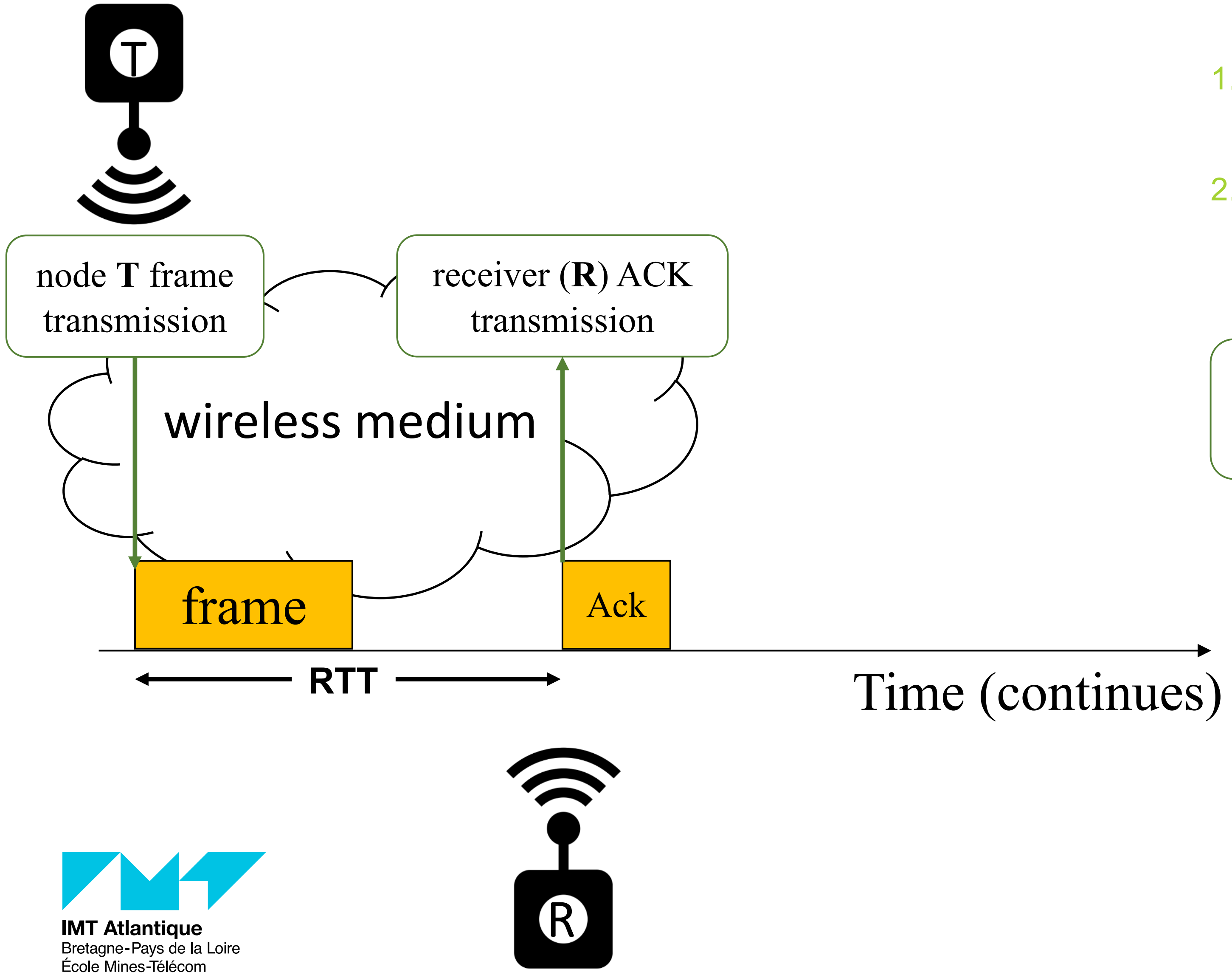
ALOHA MAC Protocols

Pure ALOHA



1. Whenever a transmitting node (T) has a frame to transmit, it does so.
2. The transmitter then listens the medium for Round Trip Time (RTT) to check if the transmission was successful.

ALOHA MAC Protocols
Pure ALOHA

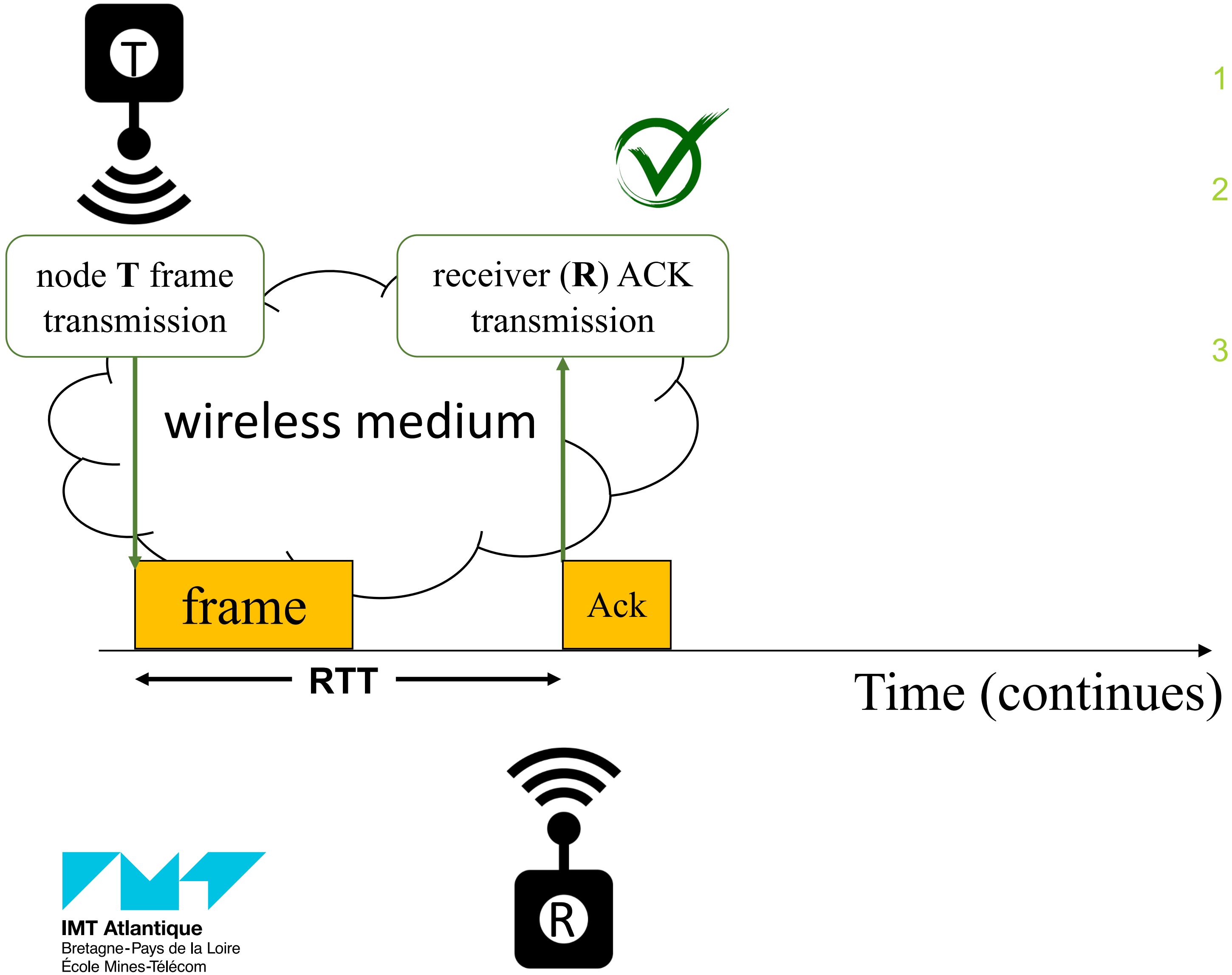


1. Whenever a transmitting node (T) has a frame to transmit, it does so.
2. The transmitter then listens the medium for Round Trip Time (RTT) to check if the transmission was successful.

In other words, it is waiting to receive the Acknowledgement from the receiver.

ALOHA MAC Protocols

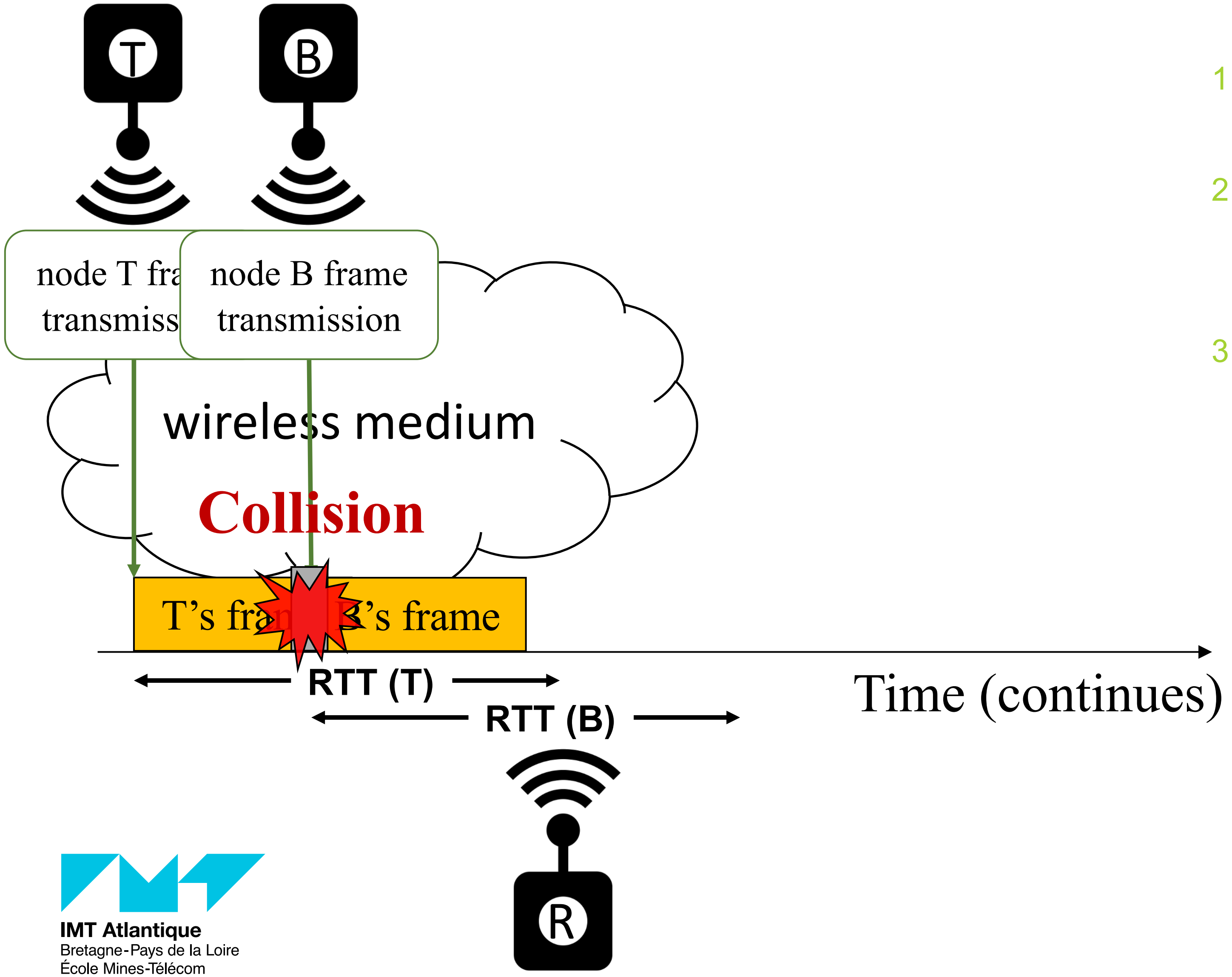
Pure ALOHA



1. Whenever a transmitting node (T) has a frame to transmit, it does so.
2. The transmitter then listens the medium for Round Trip Time (RTT) to check if the transmission was successful.
3. If the **ACK is received**, the transmission is considered as **successful**.

ALOHA MAC Protocols

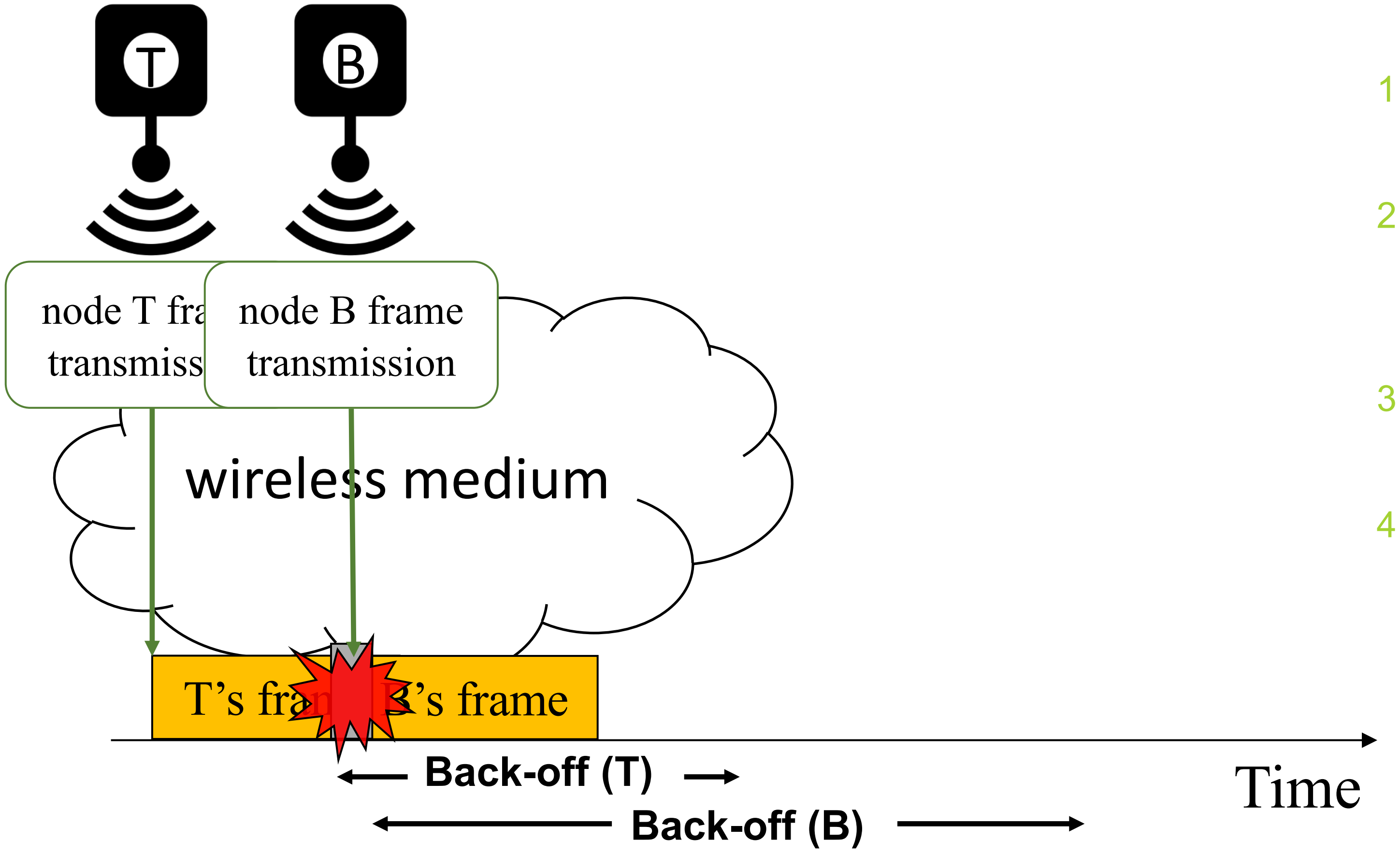
Pure ALOHA



1. Whenever a transmitting node (T) has a frame to transmit, it does so.
2. The transmitter then listens the medium for Round Trip Time (RTT) to check if the transmission was successful.
3. If **no ACK is received**, the transmission is considered as **unsuccessful**.

ALOHA MAC Protocols

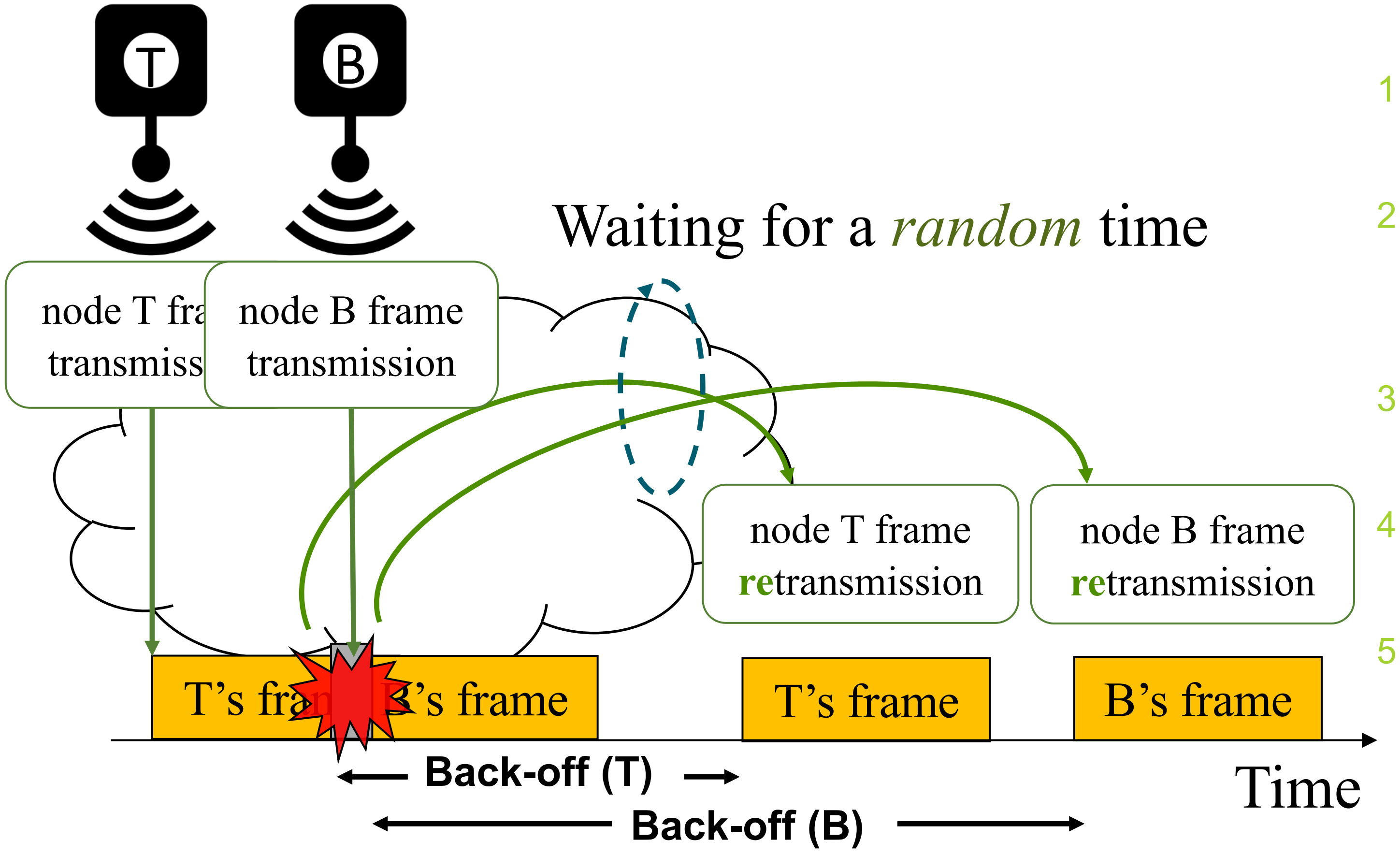
Pure ALOHA



1. Whenever a transmitting node (T) has a frame to transmit, it does so.
2. The transmitter then listens the medium for Round Trip Time (RTT) to check if the transmission was successful.
3. If **no ACK is received**, the transmission is considered as **unsuccessful**.
4. It waits then for a ***random*** amount (**back-off**) of time.

ALOHA MAC Protocols

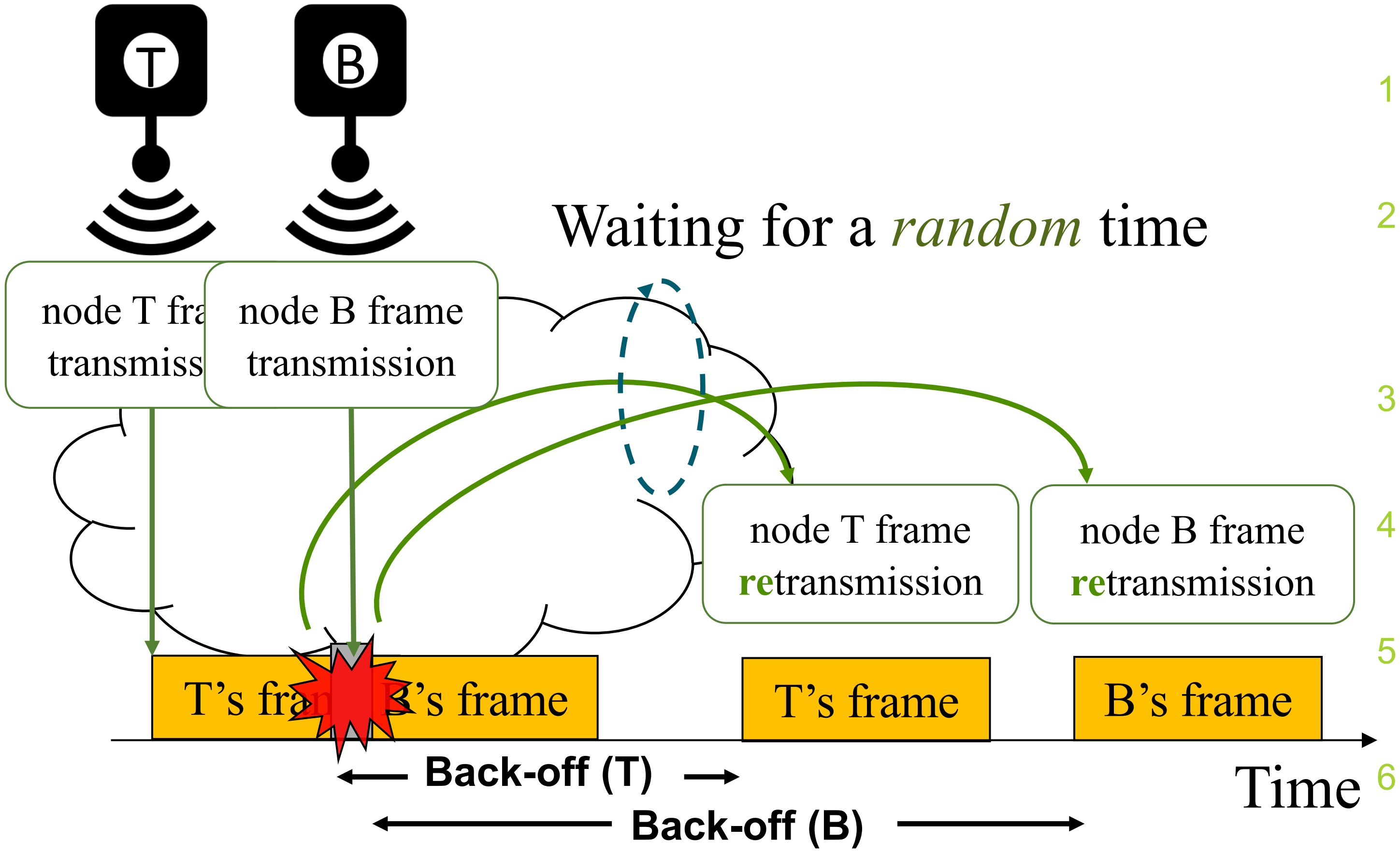
Pure ALOHA



1. Whenever a transmitting node (T) has a frame to transmit, it does so.
2. The transmitter then listens the medium for Round Trip Time (RTT) to check if the transmission was successful.
3. If **no ACK is received**, the transmission is considered as **unsuccessful**.
4. It waits then for a ***random*** amount (**back-off**) of time.
5. After completion of back-off time, the transmitter ***retransmits*** the same frame.

ALOHA MAC Protocols

Pure ALOHA



1. Whenever a transmitting node (T) has a frame to transmit, it does so.
2. The transmitter then listens the medium for Round Trip Time (RTT) to check if the transmission was successful.
3. If **no ACK is received**, the transmission is considered as **unsuccessful**.
4. It waits then for a ***random*** amount (**back-off**) of time.
5. After completion of back-off time, the transmitter ***retransmits*** the same frame.
6. It will continue to retry for a predefined number of times and then it drops the frame if there is no success.

PROS and CONS

- It works ***well*** when the traffic is limited!
- It is ***unstable*** when the network is loaded!

ALOHA MAC Protocols

Pure ALOHA: Summary

- Whenever a node has a frame to transmit, it does so.
- The transmitter listens the medium for Round Trip Time (**RTT**), to check if the transmission was successful (or not), i.e., for the ACK.
- If the **ACK is received**, the transmission is considered as **successful**.
- If **there is not ACK**, the transmitter then retransmits after a specified amount (**back-off**) of time.
- It will continue to retry for a predefined number of times and then it drops the frame if there is no success.

- The receiver checks Frame Check Sequence (FCS) and destination address to transmit the Acknowledgement.

ALOHA MAC Protocols

Collisions (1/2)

- Unsuccessful frame transmissions may be caused by radio channel ***noise*** or because other node(s) transmitted at the same time → ***collision***.
- Collision happens even when the last bit of a frame (of a node) overlaps with the first bit of another frame (of another node), then both frames are destroyed.

ALOHA MAC Protocols
Collisions (2/2)

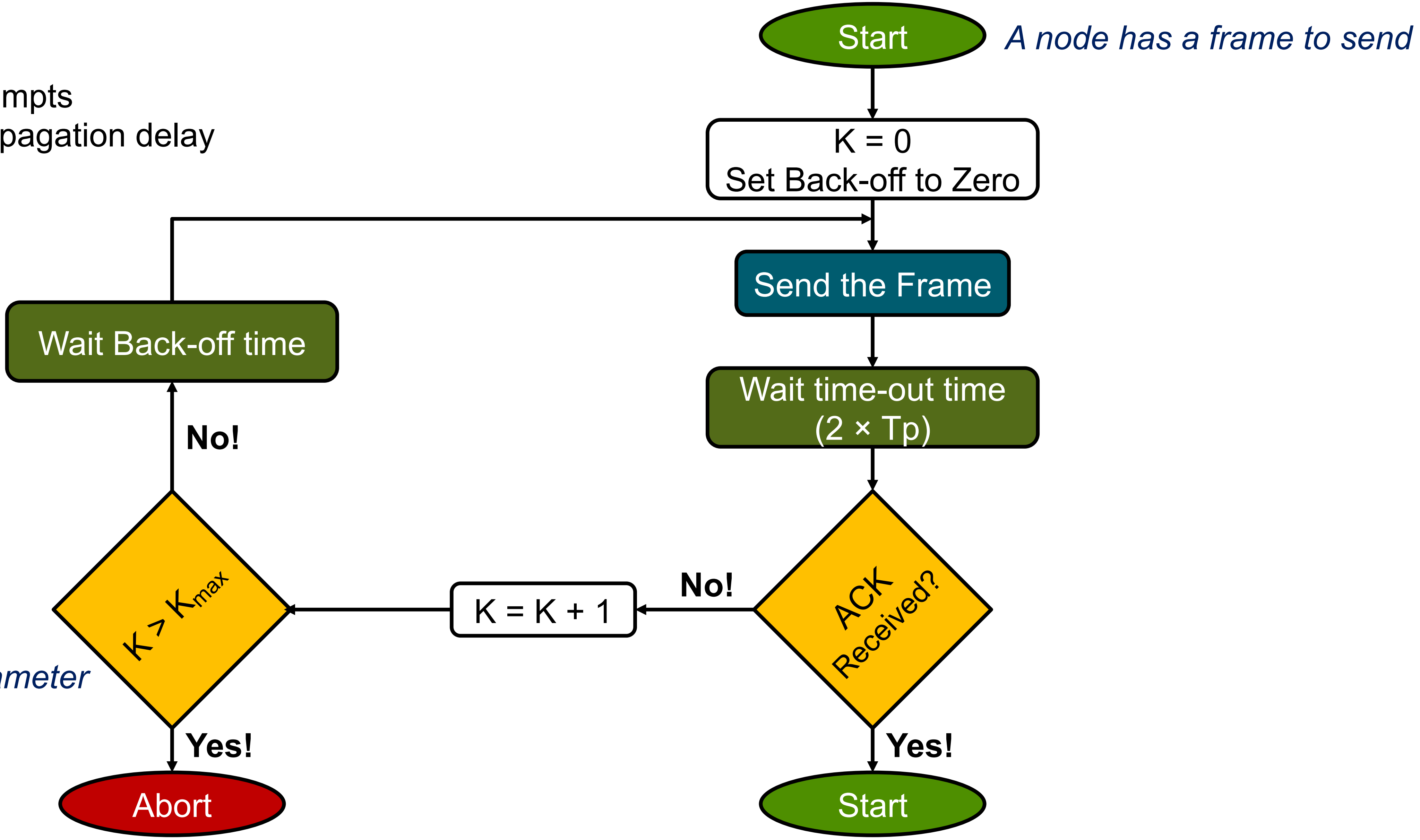
- Unsuccessful frame transmissions may be caused by radio channel ***noise*** or because other node(s) transmitted at the same time → ***collision***.
- Collision happens even when the last bit of a frame (of a node) overlaps with the first bit of another frame (of another node), then both frames are destroyed.

- Differences between regular errors (e.g., radio channel noise) and collisions:
  - Regular errors only affect negatively a single node.
  - Collision affects two or more nodes.
- The retransmission may collide again.

ALOHA MAC Protocols

Flowchart Operation

K: number of attempts
T_p: maximum propagation delay



K_{max} is a configurable parameter

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

ALOHA MAC Protocols

Back-off time (T_B)

- The **time-out period** is equal to the maximum Round-Trip Propagation Delay (T_p):
  - Twice the amount of time required to send a frame between the two most widely separated nodes ($2 \times T_p$).
- The **back-off time** (T_B) is a random value that depends on the number of unsuccessful transmission attempts (i.e., K), and it is implementation dependent.

T_p: The propagation delay is the time it takes for one bit to travel from one end of the link to the other.

ALOHA MAC Protocols

Back-off time (T_B)

- The **time-out period** is equal to the maximum Round-Trip Propagation Delay (T_p):
  - Twice the amount of time required to send a frame between the two most widely separated nodes ($2 \times T_p$).
- The **back-off time** (T_B) is a random value that depends on the number of unsuccessful transmission attempts (i.e., K), and it is implementation dependent.

- An example of T_B calculation would be the ***binary exponential back-off***:
- For each **re**transmission, the transmitting node will:
  - 1) **Select** a **random number R** between 0 and $2^K - 1$.
  - 2) **Multiply** with $\mathbf{T_p}$ (maximum propagation delay) or $\mathbf{T_t}$ (the average transmission delay).
  - Thus, $\mathbf{T_B = R \times T_p}$ or $\mathbf{R \times T_t}$
- In this procedure, the range of the random numbers increases after each collision till $K > K_{max}$.

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

T_p: The propagation delay is the time it takes for one bit to travel from one end of the link to the other.
T_t: The transmission delay is the time needed to push all the packet bits on the transmission link.

ALOHA MAC Protocols

Back-off time (T_b): Example

- Two nodes on a wireless ALOHA network are a maximum of 600 km apart. If we assume that signals propagate at 3×10^8 m/s. Find the $\mathbf{T_B}$ values for **K**=1, 2, & 3.

ALOHA MAC Protocols

Back-off time (T_b): Example

- Two nodes on a wireless ALOHA network are a maximum of 600 km apart. If we assume that signals propagate at 3×10^8 m/s. Find the $\mathbf{T_B}$ values for **K**=1, 2, & 3.

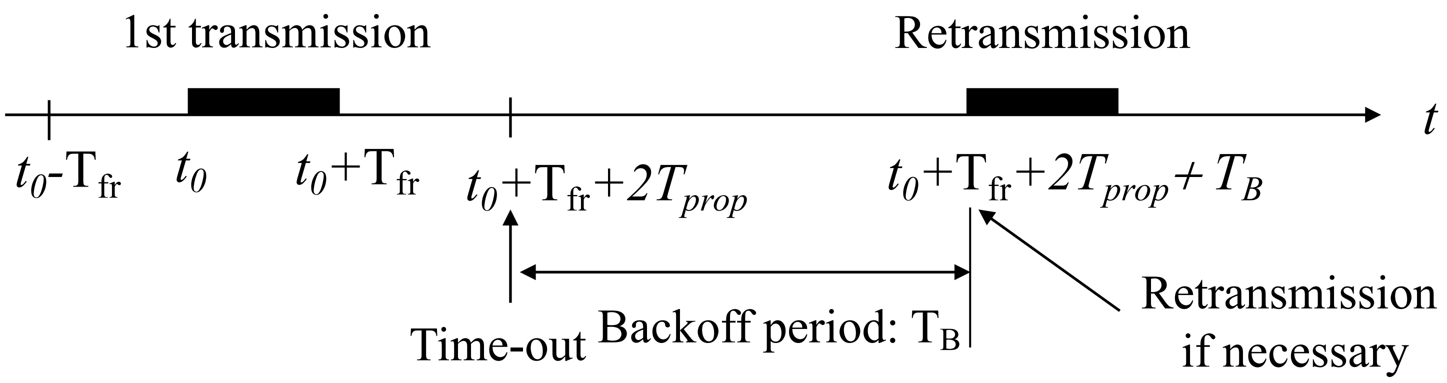
- Step 1 (Calculate the propagation delay T_p):
  - $T_p = D / S$, where D is the distance between two nodes, and S is the transmission speed.
  - $\boldsymbol{T_p = (600 \times 10^3) / (3 \times 10^8) = 2\ ms}$

- Step 2 (now, we can find the value of $\mathbf{T_B}$ for different values of **K**, $T_B = R \times T_p$):
  - For K = 1, the range is {0, 1}. This means that $\mathbf{T_B}$ is either 0 ms (0 × 2) or 2 ms (1 × 2), *based on the outcome of the random variable **R***.
  - For K = 2, the range is {0, 1, 2, 3}. This means that $\mathbf{T_B}$ can be 0, 2, 4, or 6 ms.
  - For K = 3, the range is {0, 1, 2, 3, 4, 5, 6, 7}. This means that $\mathbf{T_B}$ can be 0, 2, 4, . . . , 14 ms.

Note that if K > K_{max}, (K_{max} is a configurable parameter) then the frame is dropped.

ALOHA MAC Protocols
Pure ALOHA: Vulnerable Time

- Considering that **L** is the *frame length*, **R** is the *transmission rate*, and $\mathbf{T_t}$ is the *transmission delay*, which is calculated based on the following formula: $\mathbf{T_t = L / R}$.
  - 1. A node transmits a frame at $t = t_0$, and it completes the frame transmission at $t_0 + T_t$.
  - 2. If ACK is not received after $t_0 + T_t + 2T_p$, it will wait for a random time T_B.
  - 3. And it retransmits the frame at $t_0 + T_t + 2T_p + T_B$.

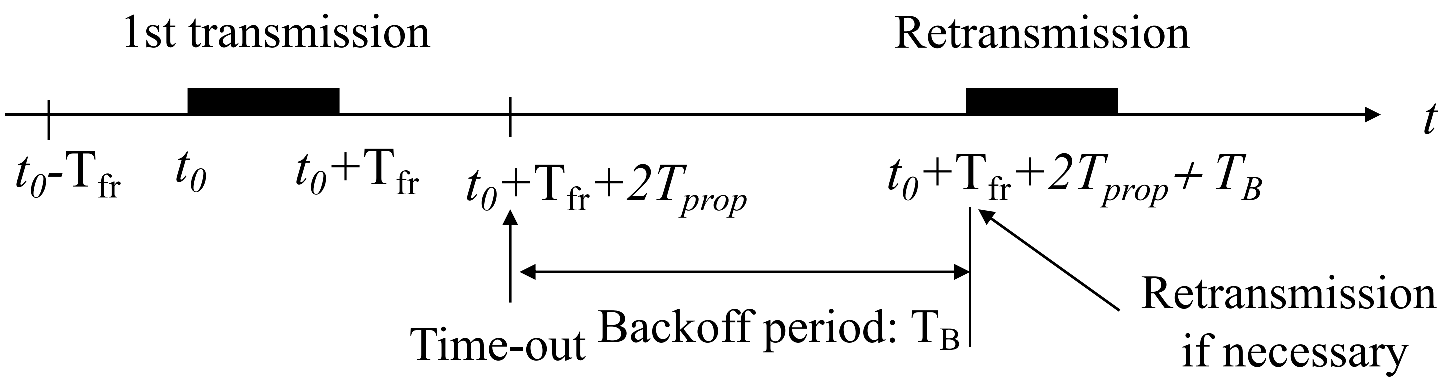


IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

ALOHA MAC Protocols

Pure ALOHA: Vulnerable Time

- Considering that **L** is the *frame length*, **R** is the *transmission rate*, and **T_t** is the *transmission delay*, which is calculated based on the following formula: **T_t = L / R**.
  - 1. A node transmits a frame at $t = t_0$, and it completes the frame transmission at $t_0 + T_t$.
  - 2. If ACK is not received after $t_0 + T_t + 2T_p$, it will wait for a random time T_B.
  - 3. And it retransmits the frame at $t_0 + T_t + 2T_p + T_B$.

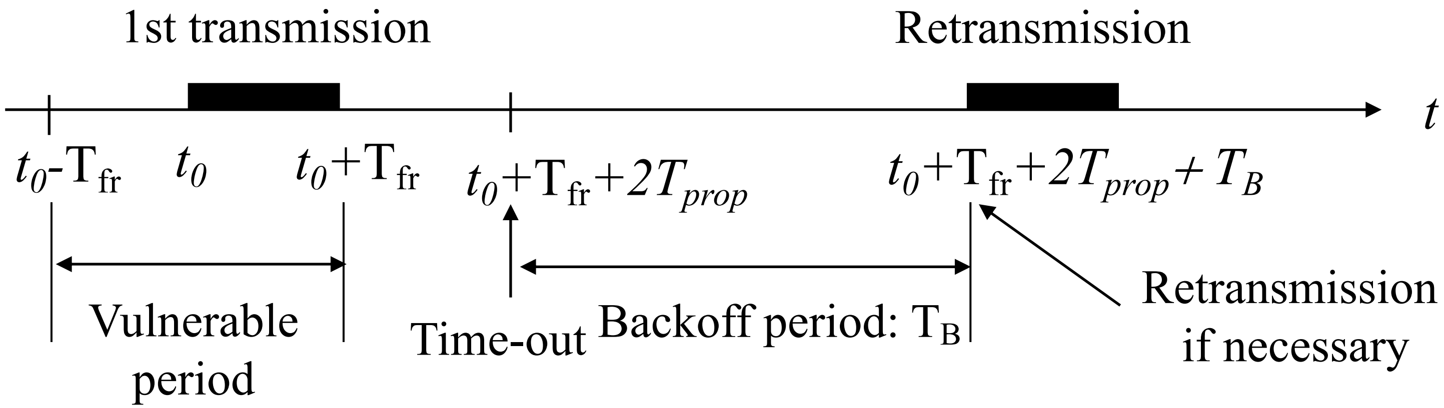


When collision occurs?

ALOHA MAC Protocols

Pure ALOHA: Vulnerable Time

- Considering that **L** is the *frame length*, **R** is the *transmission rate*, and $\mathbf{T_t}$ is the *transmission delay*, which is calculated based on the following formula: $\mathbf{T_t = L / R}$.
  - 1. A node transmits a frame at $t = t_0$, and it completes the frame transmission at $t_0 + T_t$.
  - 2. If ACK is not received after $t_0 + T_t + 2T_p$, it will wait for a random time T_B.
  - 3. And it retransmits the frame at $t_0 + T_t + 2T_p + T_B$.

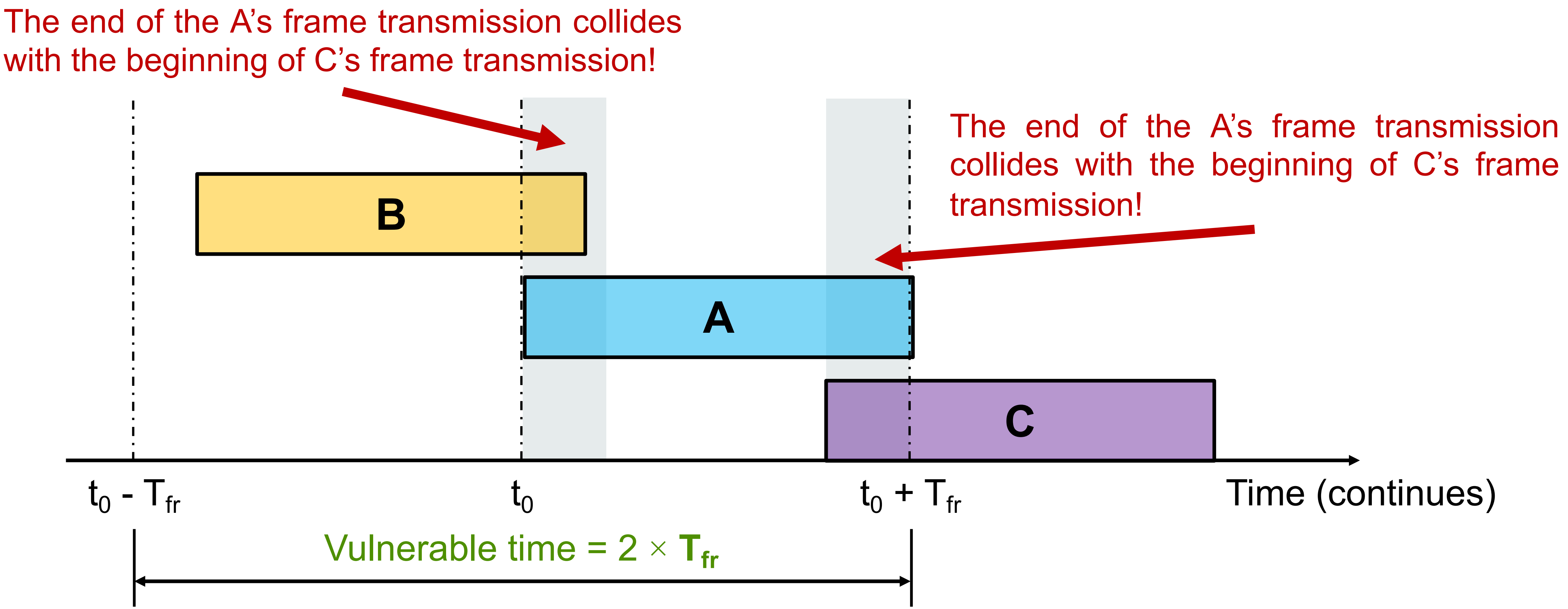


When collision occurs?

Vulnerable period is from t_0-T_t to t_0+T_t (2T_t seconds). If any other frames are transmitted during the period, the collision will occur!

ALOHA MAC Protocols

Pure ALOHA: Vulnerable Time



Node A transmits a frame at time *t*. Assuming that node B has already sent a frame between t - T_{fr} and t, this leads to a collision between the frames from nodes A and B. More specifically, the end of B's frame collides with the beginning of A's frame. Furthermore, suppose that node C transmits a frame between t and $t + T_{fr}$. Here, there is a collision as well between frames from nodes A and C. Indeed, the beginning of C's frame collides with the end of A's frame.

ALOHA MAC Protocols

Pure ALOHA: Vulnerable Time [**Example**]

- A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free?

ALOHA MAC Protocols

Pure ALOHA: Vulnerable Time [**Example**]

- A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free?

Solution

- Average Frame Transmission Time/Delay ($\mathbf{T_e}$ / $\mathbf{T_t}$ / $\mathbf{T_{fr}}$) = Length / Rate <=>
- Average Frame Transmission Time/Delay ($\mathbf{T_e}$ / $\mathbf{T_t}$ / $\mathbf{T_{fr}}$) = L/R <=>
- Average Frame Transmission Time/Delay ($\mathbf{T_e}$ / $\mathbf{T_t}$ / $\mathbf{T_{fr}}$) = 8L (in bits) / R

- Average frame transmission time $\mathbf{T_{fr}}$ is 200 bits/200 kbps or 1 ms. The vulnerable time is 2×1 ms = 2 ms.

- This means no node should transmit later than 1 ms before this node starts transmission and no node should start transmitting during the one 1-ms period that this node is transmitting.

Random Access

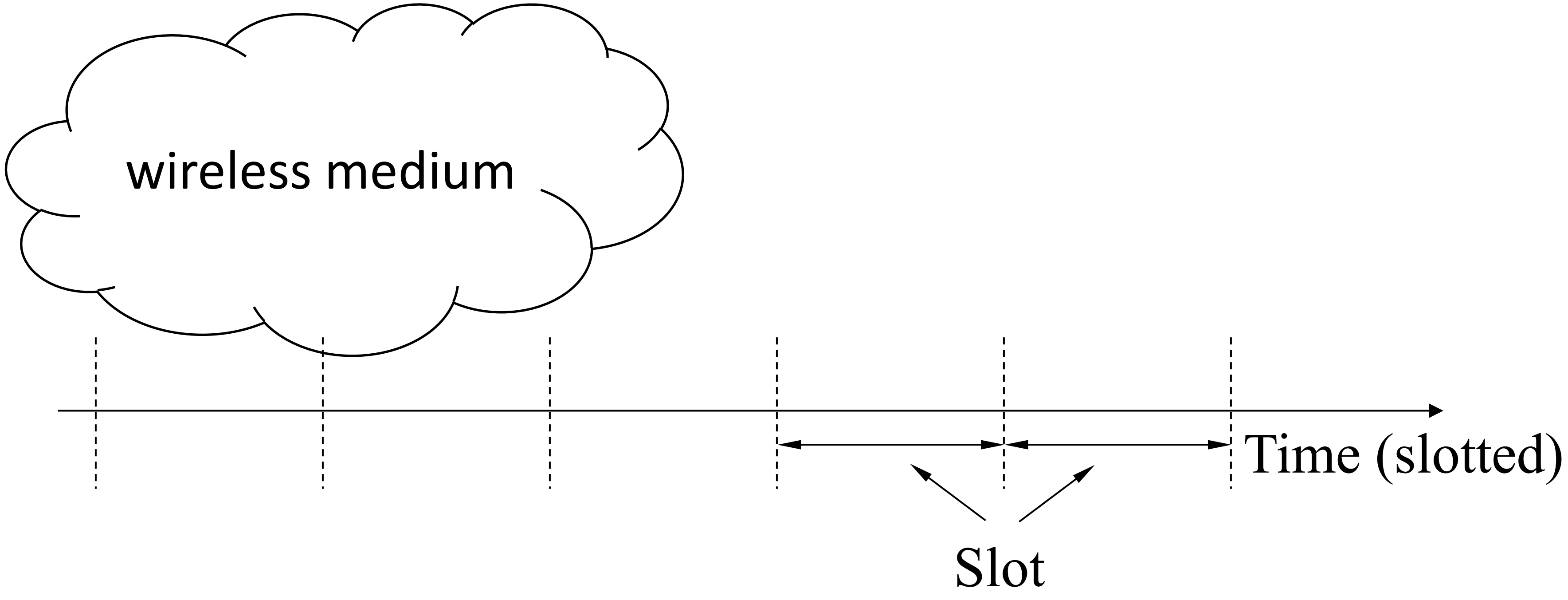
Popular Protocols

- ALOHA
- Slotted ALOHA
- CSMA (Carrier Sense Multiple Access)
- CSMA/CD (CSMA with Collision Detection)
- CSMA/CA (CSMA with Collision Avoidance)
  - CSMA/CA with ACK
  - CSMA/CA with RTS/CTS

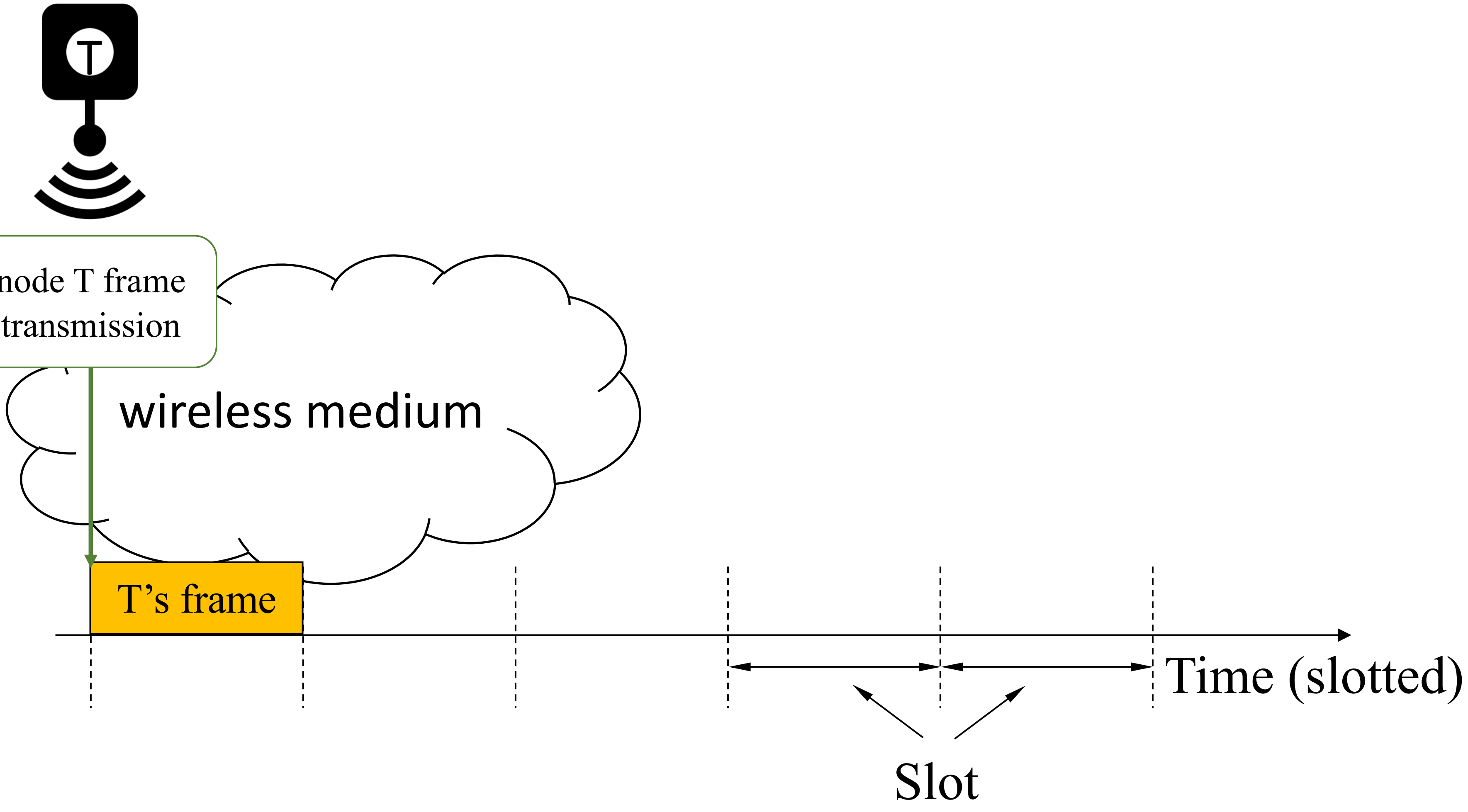
Check the relevant video
"*ALOHA Medium Access Control (MAC) Protocol(s)*"
on YouTube!

ALOHA MAC Protocols

Slotted ALOHA

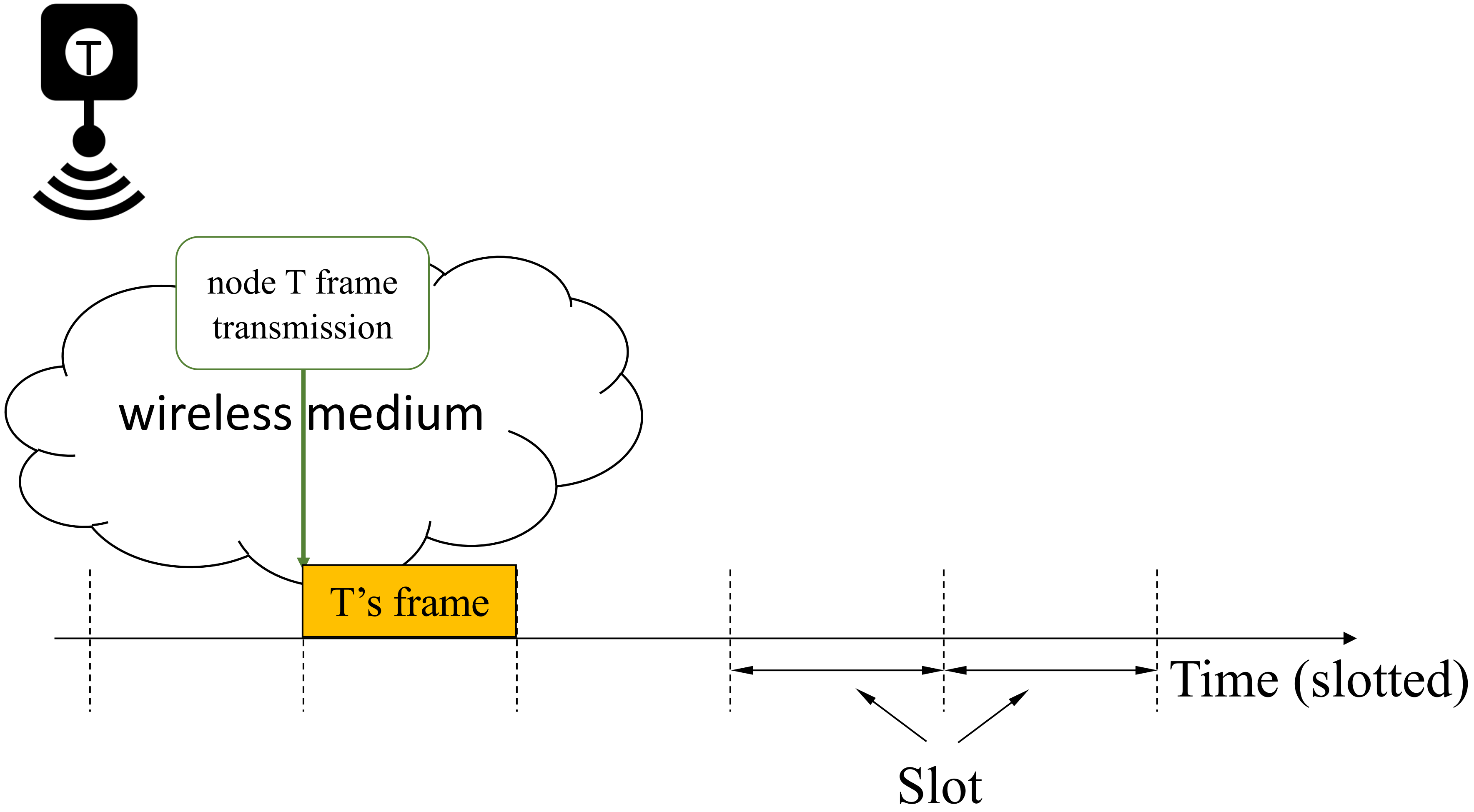


ALOHA MAC Protocols
Slotted ALOHA



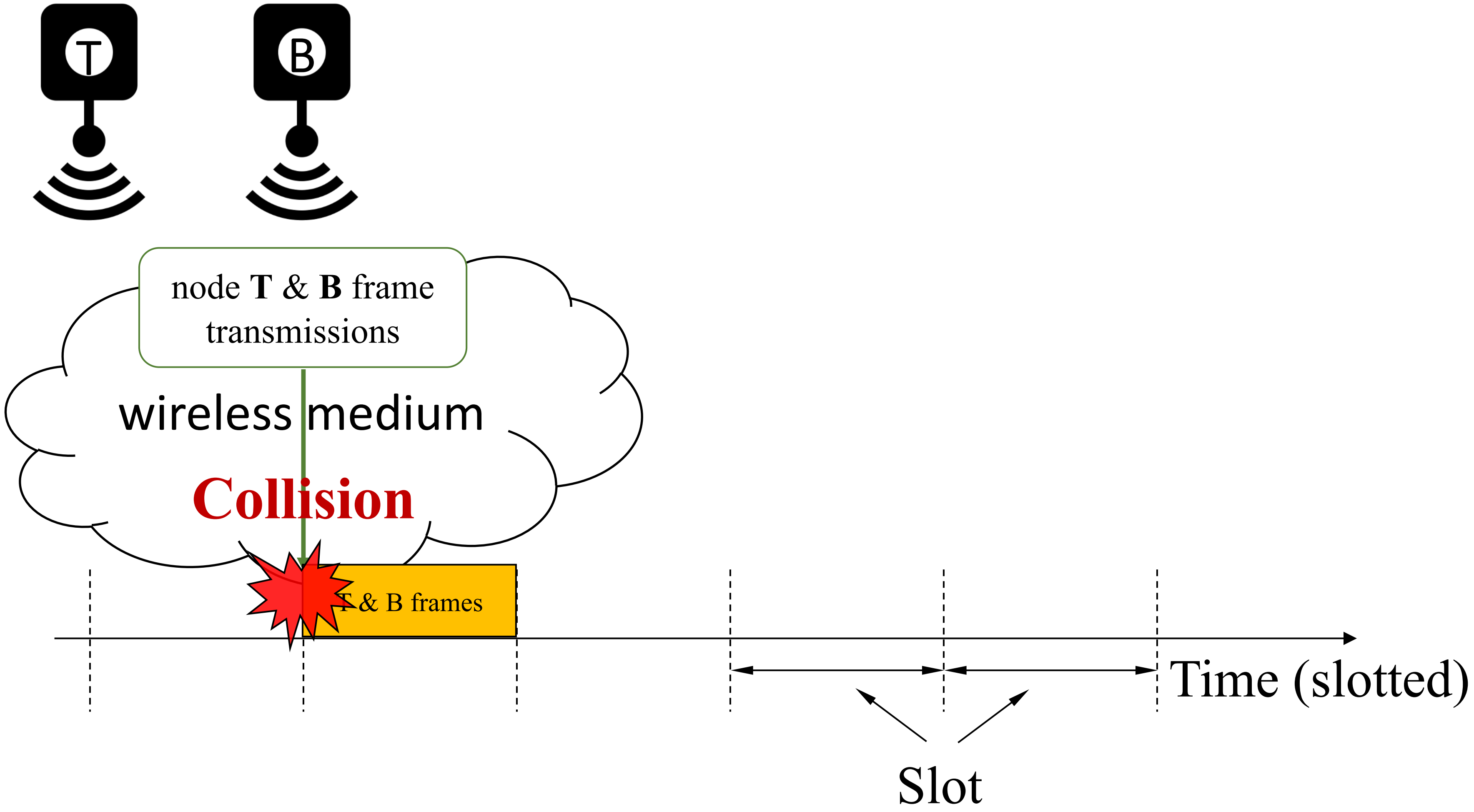
ALOHA MAC Protocols

Slotted ALOHA



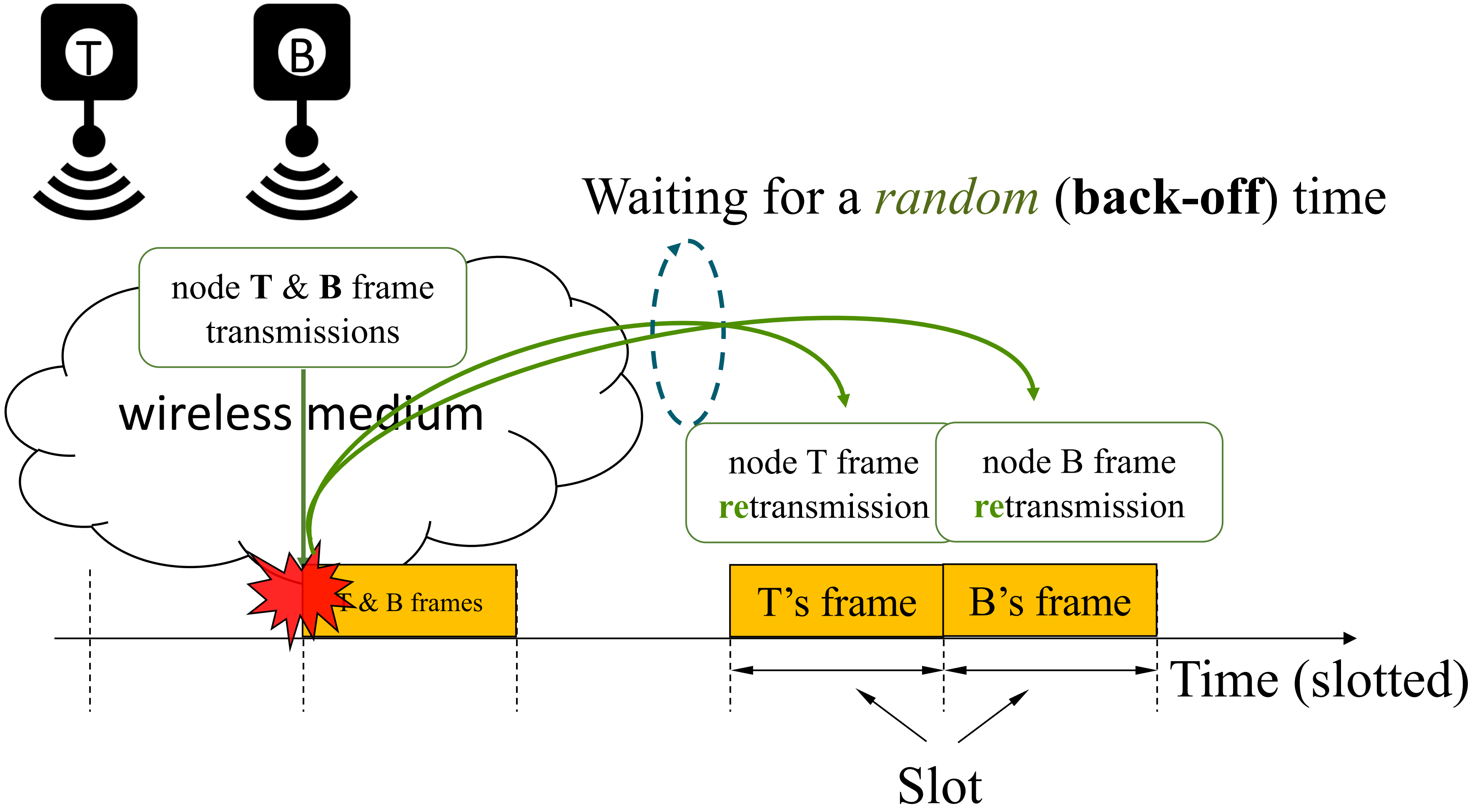
ALOHA MAC Protocols

Slotted ALOHA



ALOHA MAC Protocols

Slotted ALOHA



Whenever a node has a frame, it transmits only at the beginning of a slot.

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

ALOHA MAC Protocols

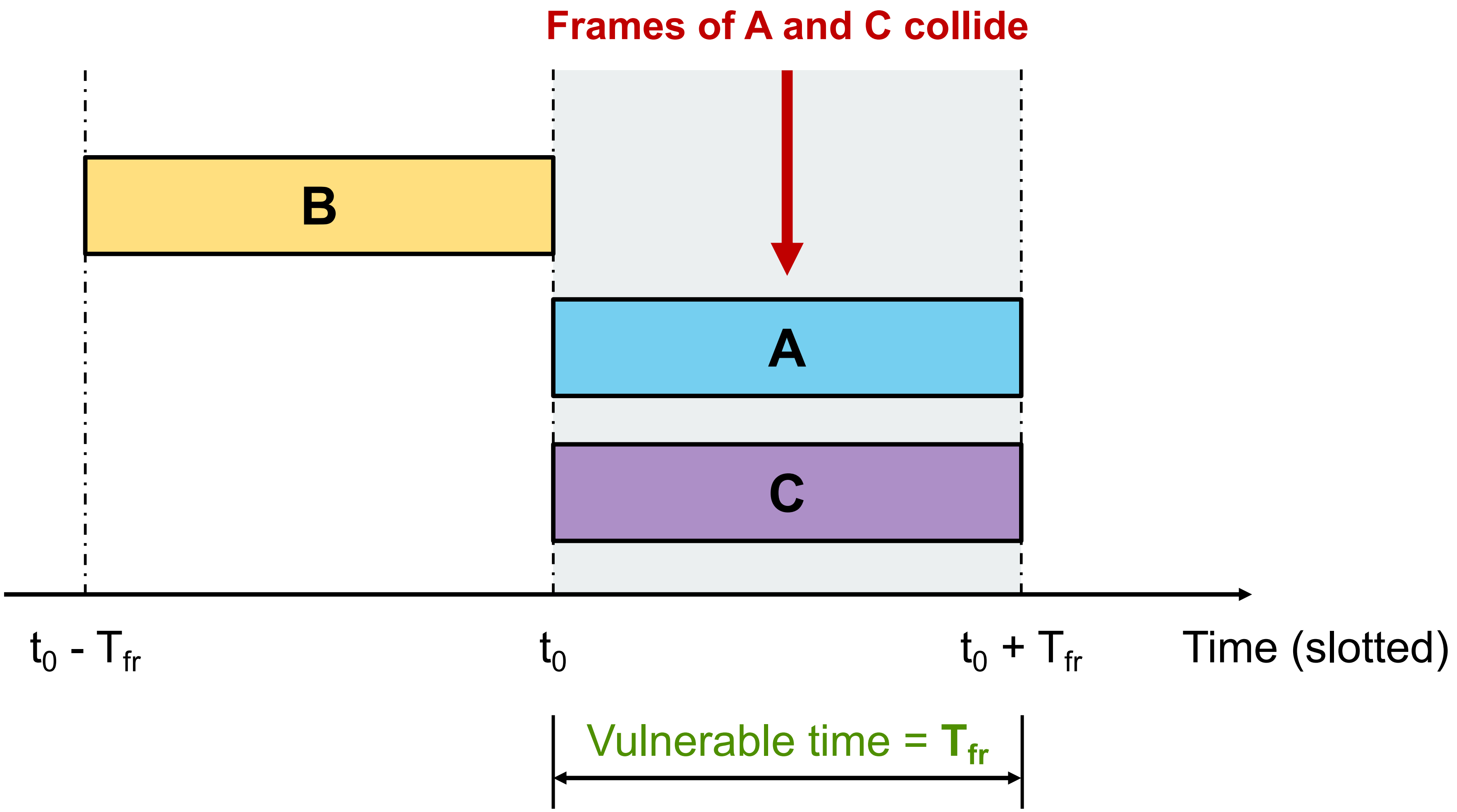
Slotted ALOHA: Summary

- The **continues time is divided in slots** of $\mathbf{T_{fr}}$ seconds**.**
- **Transmission** can take place **only at the beginning of a slot**.
  - if a node misses this opportunity, it must wait until the beginning of the next time slot.
- The **vulnerable time** is now reduced to **one-half**, equal to T_{fr}, that of Pure ALOHA.

- A **successful** frame transmission takes place only **when in each individual slot only a single frame is transmitted**.
- If **no frame is transmitted** in a **slot**, then **it will remain idle**.

ALOHA MAC Protocols

Slotted ALOHA: Vulnerable Time



The **vulnerable time** is reduced to **one-half**, equal to $\mathbf{T_{fr}}$, that of Pure ALOHA.

Random Access

Popular Protocols

- ALOHA
- Slotted ALOHA
- CSMA (Carrier Sense Multiple Access)
- CSMA/CD (CSMA with Collision Detection)
- CSMA/CA (CSMA with Collision Avoidance)
  - CSMA/CA with ACK
  - CSMA/CA with RTS/CTS

Random Access: CSMA MAC Protocol

Carrier Sense Multiple Access (CSMA)

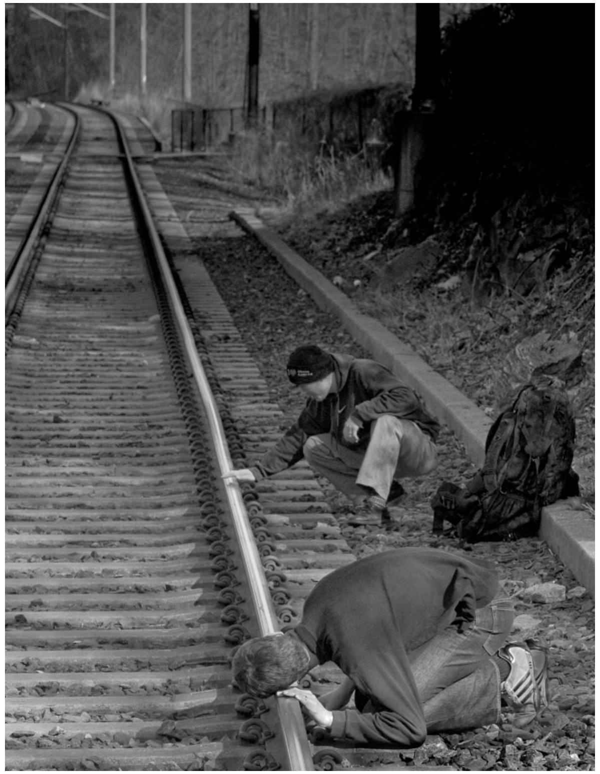
- The ALOHA (including Slotted ALOHA) protocols have poor utilization.
- The CSMA method was developed to minimize the probability of collision and, therefore, increase the network throughput performance.
- The probability of collision can be reduced if a node senses the medium before trying to use it.

- In CSMA protocols, a node will sense (i.e., check the state of the medium) the medium before transmitting a frame, and it will transmit a frame only if no other transmission is ongoing.
  - CSMA is based on the **principle** "*sense before transmit*" or "*listen before talk*".

Random Access: CSMA MAC Protocol

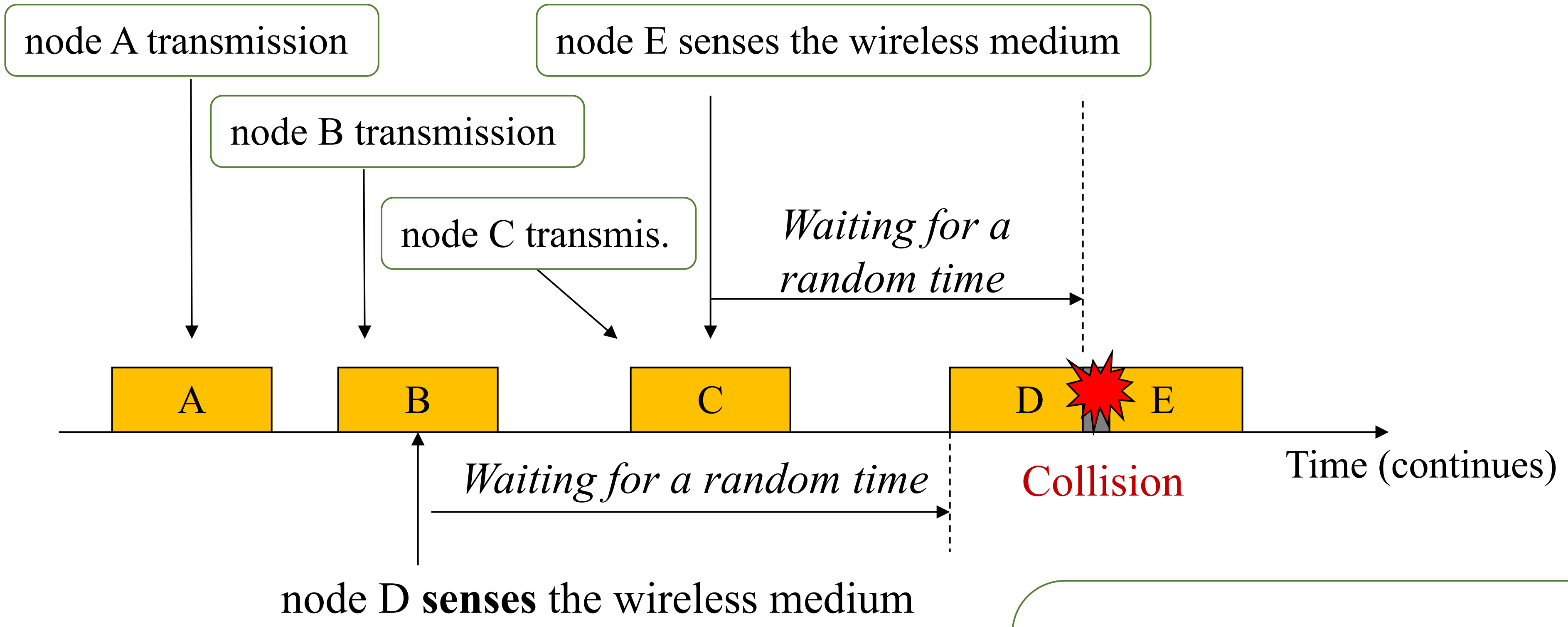
CSMA: Listening (sampling) the Medium

- Listen to the medium before transmitting a frame.
- Clear Channel Assessment (CCA):
  - Detected energy > threshold.
  - The detected signal corresponds to the PHY layer of the node with the same modulation and propagation characteristics.



Random Access: CSMA MAC Protocol

CSMA: Operation Example

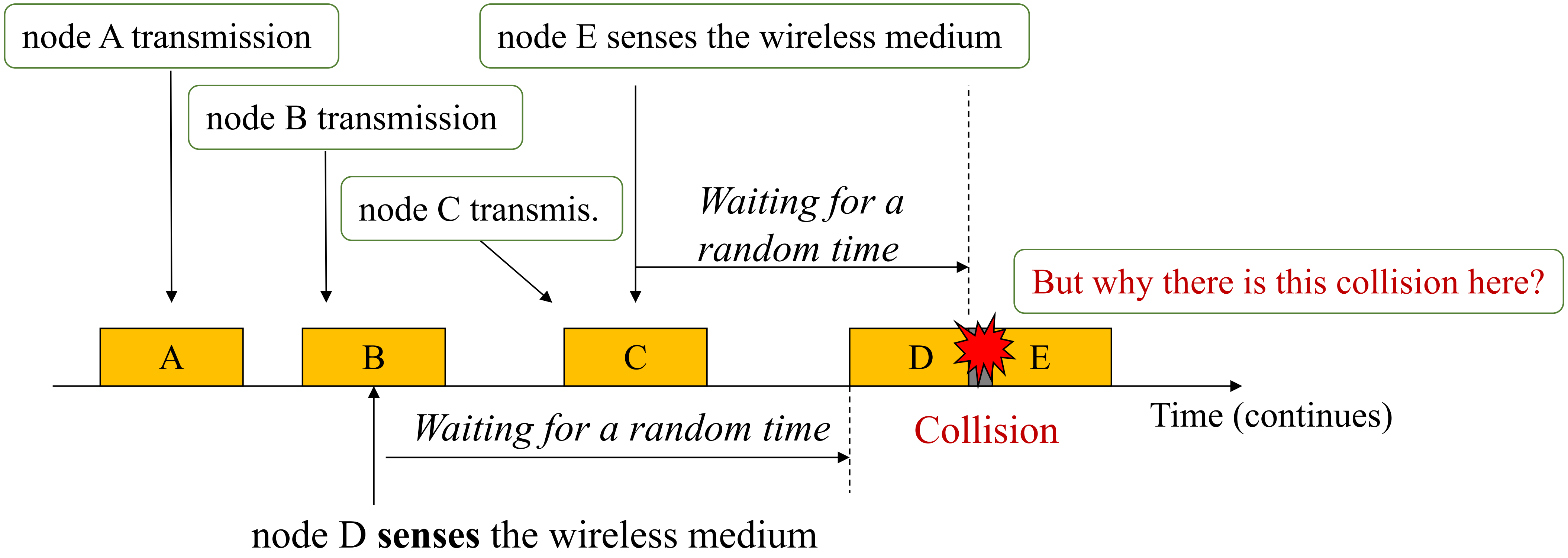


*Whenever a node has a frame, **it will listen** to the medium **before** transmitting.*

In Slotted CSMA, we would have collision only in the beginning of each SLOT, and not during.

Random Access: CSMA MAC Protocol

CSMA: Operation Example



CSMA can reduce the possibility of collision, but it cannot eliminate it!

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Random Access: CSMA MAC Protocol

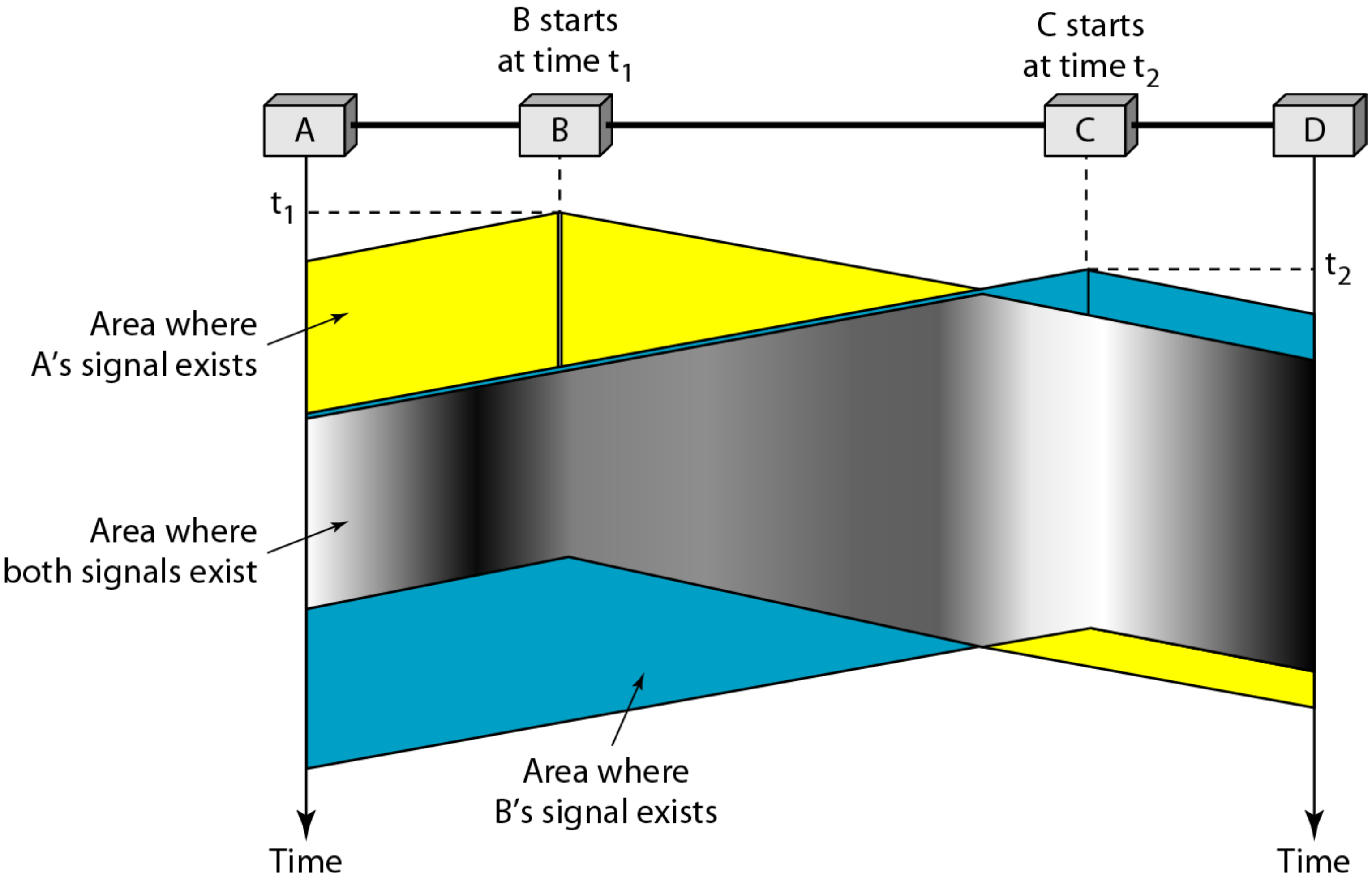
CSMA: Possibility of a Collision (1/3)

The **possibility of collision still exists because of propagation delay**. Indeed, when a node transmits a frame, it still takes time (although very short) for the first bit to reach every node and for every node to sense it.

In other words, ***a node may sense the medium and find it idle, only because the first bit sent by another node has not yet been received***.

Random Access: CSMA MAC Protocol

CSMA: Space/time model of the collision in CSMA



At time $\mathbf{t_1}$ node B senses the medium and finds it idle, so it transmits a frame. At time $\mathbf{t_2}$ ($\mathbf{t_2}$> $\mathbf{t_1}$) node C senses the medium and finds it idle because, at this time, the first bits from node B have not reached node C. Thus, node C also sends a frame. As a result, the two signals collide and consequently both frames are destroyed.

Random Access: CSMA MAC Protocol

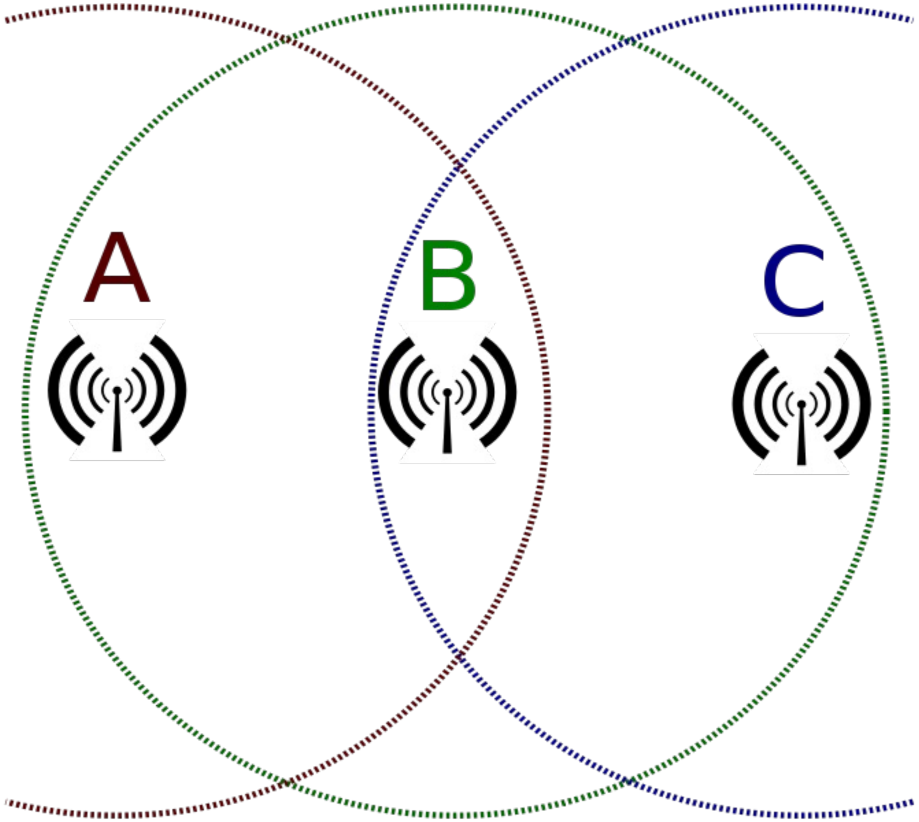
CSMA: Possibility of a Collision (2/3)

The **possibility of collision still exists because of simultaneous frame emission.**

Indeed, if two or more nodes sense the medium simultaneously, both will realize that the medium is idle, and therefore will initiate the transmission of their frames.

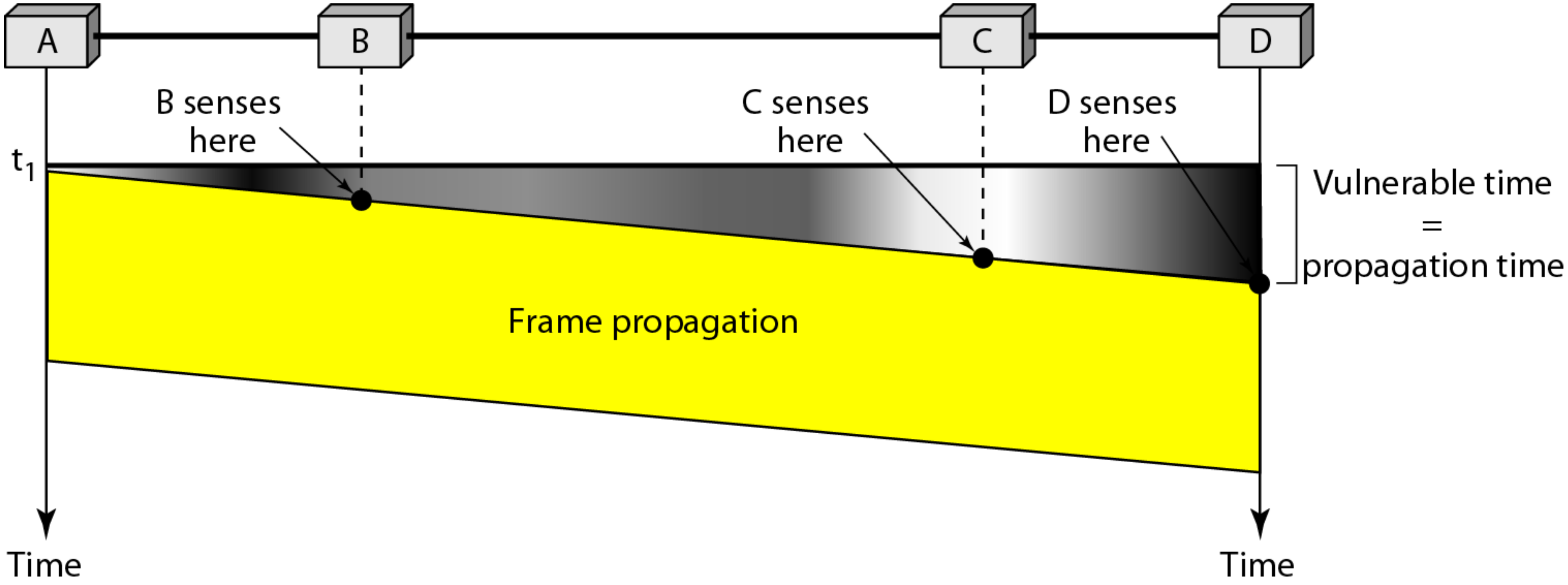
Random Access: CSMA MAC Protocol

CSMA: Possibility of a Collision (3/3) - Hidden Node Problem



Random Access: CSMA MAC Protocol

CSMA: Vulnerable Time



The **vulnerable time** for **CSMA is the propagation time T_p.**

- This is the time needed for a signal to propagate from one end of the medium to the other.
- The leftmost node A transmits a frame at time $\mathbf{t_1}$ which reaches the rightmost station D at time $\mathbf{t_1}$ + $\mathbf{T_p}$.
- Then, the grey area indicates the vulnerable area in time and space.

Random Access: CSMA MAC Protocol

CSMA: Persistence Methods

What should a node do if the channel is **busy**?
What should a node do if the channel is **idle**?

Three methods have been devised to answer these questions:

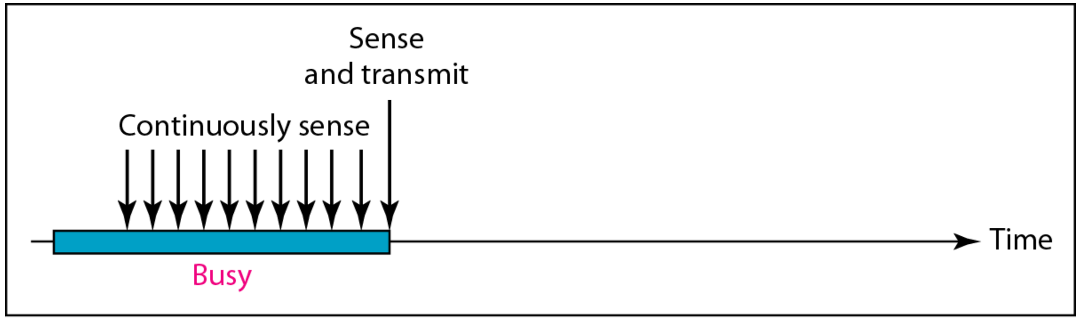
- the 1-persistent method.
- the Non-persistent method.
- the p-persistent method.

Random Access: CSMA MAC Protocol

CSMA: 1-persistent

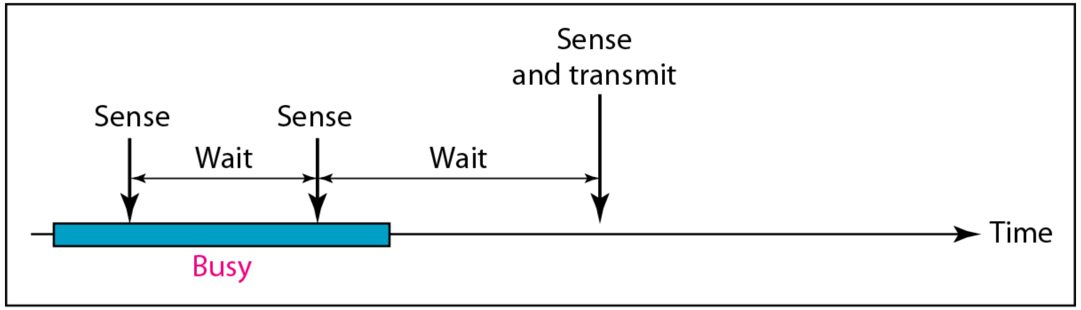
- 1-persistent (aggressive algorithm):
  - Step 1: If the medium is idle, transmit immediately (with probability 1).
  - Step 2: If the medium is busy (noisy), *continue to listen until medium becomes idle*, and then transmit immediately.

- If two nodes want to retransmit, there will always be a collision.
- After X retransmissions, *stop the transmission.*



a. 1-persistent

- Non-persistent (non-aggressive algorithm):
  - Step 1: If the medium is idle, transmit immediately.
  - Step 2: If the medium is busy, *wait a random time* and repeat Step 1.



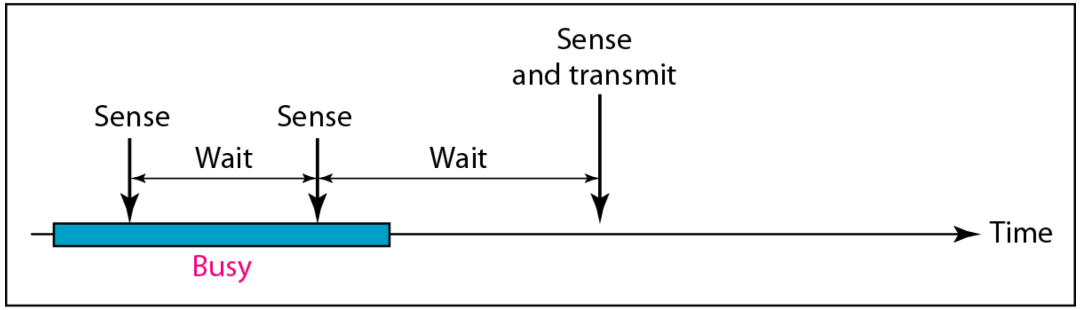
b. Nonpersistent

Random Access: CSMA MAC Protocol

CSMA: Non-persistent

- Non-persistent (non-aggressive algorithm):
  - Step 1: If the medium is idle, transmit immediately.
  - Step 2: If the medium is busy (noisy), *wait a random time* and repeat Step 1.

- Trade-off:
  - Random back-off reduces probability of collisions.
  - Waste idle time if the back-off time is too long.



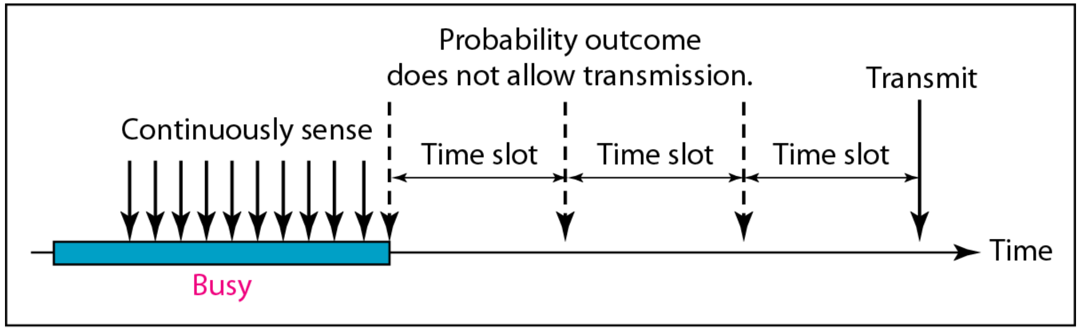
b. Nonpersistent

Random Access: CSMA MAC Protocol

CSMA: P-persistent

- P-persistent:
  - Step 1: If the medium is **idle**, transmit with *probability p*, and delay for worst case propagation delay for one frame with probability (1-p).
  - Step 2: If the medium is **busy**, continue to listen until medium becomes idle, then go to Step 1.
  - Step 3: If transmission is delayed by 1-time slot, continue with Step 1.

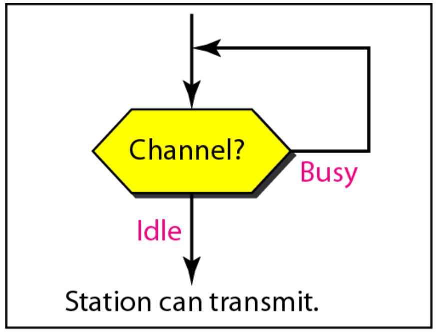
- Trade-off between non-persistent and 1-persistent CSMA



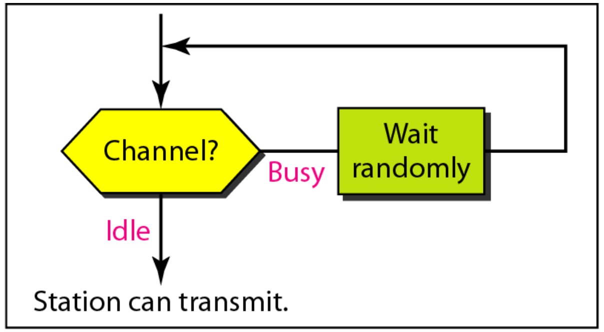
c. p-persistent

Random Access: CSMA MAC Protocol

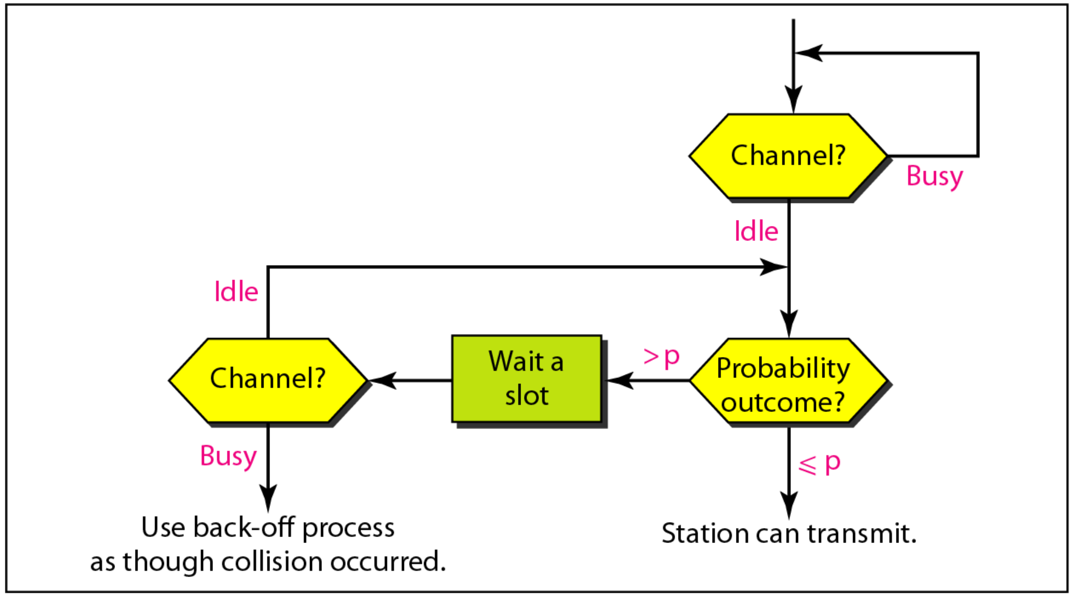
CSMA: Flowchart of the Three Persistence Methods



a. 1-persistent



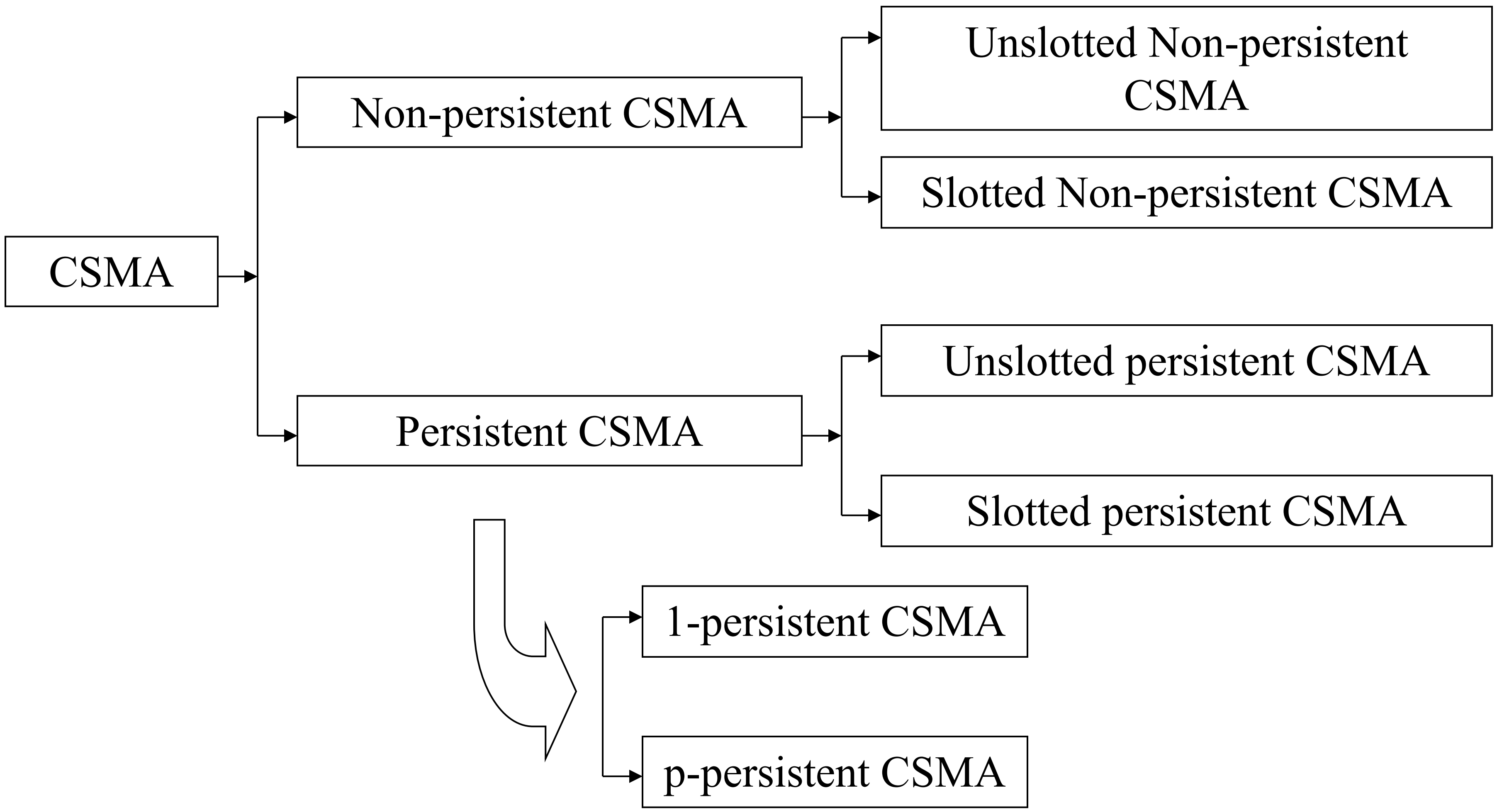
b. Nonpersistent



c. p-persistent

Random Access: CSMA MAC Protocol

CSMA: Summary of Persistence Methods



Random Access

Popular Protocols

- ALOHA
- Slotted ALOHA
- CSMA (Carrier Sense Multiple Access)
- CSMA/CD (CSMA with Collision Detection)
- CSMA/CA (CSMA with Collision Avoidance)
  - CSMA/CA with ACK
  - CSMA/CA with RTS/CTS

Random Access: CSMA/CD MAC Protocol

CSMA with Collision Detection

- The CSMA method does not specify the procedure following a collision.
- In *CSMA*, if two terminals begin transmitting a frame at the same time, each will transmit its complete packet (*although collision is taking place*).
  - Wasting medium for an entire packet time.
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) augments the algorithm to handle the collision.

Random Access: CSMA/CD

CSMA with Collision Detection

- CSMA/CD:
  - Step 1: If the medium is **idle**, **transmit**.
  - Step 2: If the medium is **busy**, continue to listen until the channel is idle **then transmit**.
  - Step 3: If a collision is detected during transmission, the node stops its (ongoing) transmission.
  - Step 4: Then, it will wait for a random amount of time, and it will repeat the algorithm.

Random Access: CSMA/CD

CSMA with Collision Detection

- CSMA/CD:
  - Step 1: If the medium is **idle**, **transmit**.
  - Step 2: If the medium is **busy**, continue to listen until the channel is idle **then transmit**.
  - Step 3: If a collision is detected during transmission, the node stops its (ongoing) transmission.
  - Step 4: Then, it will wait for a random amount of time, and it will repeat the algorithm.
- Suppose that two nodes begin to transmit at the “same” time. *How long until the collision is detected*?

Random Access: CSMA/CD

CSMA with Collision Detection

- CSMA/CD:
  - Step 1: If the medium is idle, **transmit**.
  - Step 2: If the medium is busy, continue to listen until the channel is idle **then transmit**.
  - Step 3: If a collision is detected during transmission, the node stops its (ongoing) transmission.
  - Step 4: Then, it will wait for a random amount of time, and it will repeat the algorithm.
- Suppose that two nodes begin to transmit at the “same” time. *How long until the collision is detected*?
  - The Propagation Delay (T_p).

Random Access: CSMA/CD

The worst-case scenario to detect the collision

- What is the worst-case scenario to detect the collision, when two devises ***do not*** transmit at the same time?

Random Access: CSMA/CD

The worst-case scenario to detect the collision

- What is the worst-case scenario to detect the collision, when two devises do not transmit at the same time?

  - Let T_p be the propagation delay.
  - At t=0, node 1 begins transmission.
  - Suppose that at $t=T_p-\varepsilon$ node 2 begins to transmit.
  - At $t=T_p$, node 2 detects the collision.
  - At $t=2T_p-\varepsilon$, node 1 detects the collision.

Random Access: CSMA/CD

The worst-case scenario to detect the collision

- What is the worst-case scenario to detect the collision, when two devises do not transmit at the same time?
  - Twice the propagation delay (T_p), worst case scenario.

  - Let T_p be the propagation delay.
  - At t=0, node 1 begins transmission.
  - Suppose that at $t=T_p - \varepsilon$ node 2 begins to transmit.
  - At $t=T_p$, node 2 detects the collision.
  - At $t=2T_p - \varepsilon$, node 1 detects the collision.

Random Access: CSMA/CD

The worst-case scenario to detect the collision

- What is the worst-case scenario to detect the collision, when two devises do not transmit at the same time?
  - Twice the propagation delay (T_p), worst case scenario.

  - Let T_p be the propagation delay.
  - At t=0, node 1 begins transmission.
  - Suppose that at $t=T_p-\varepsilon$ node 2 begins to transmit.
  - At $t=T_p$, node 2 detects the collision.
  - At $t=2T_p-\varepsilon$, node 1 detects the collision.

- Keeping propagation delay (T_p) small can improve efficiency.
- After a collision is detected, often a jamming signal is applied*.
- This slightly increases the contention interval.

* The jam signal or jamming signal is a signal that carries a 32-bit binary pattern sent by a data station to inform the other stations of the collision and that they must not transmit.

Random Access: CSMA/CD

Collision Detection Example

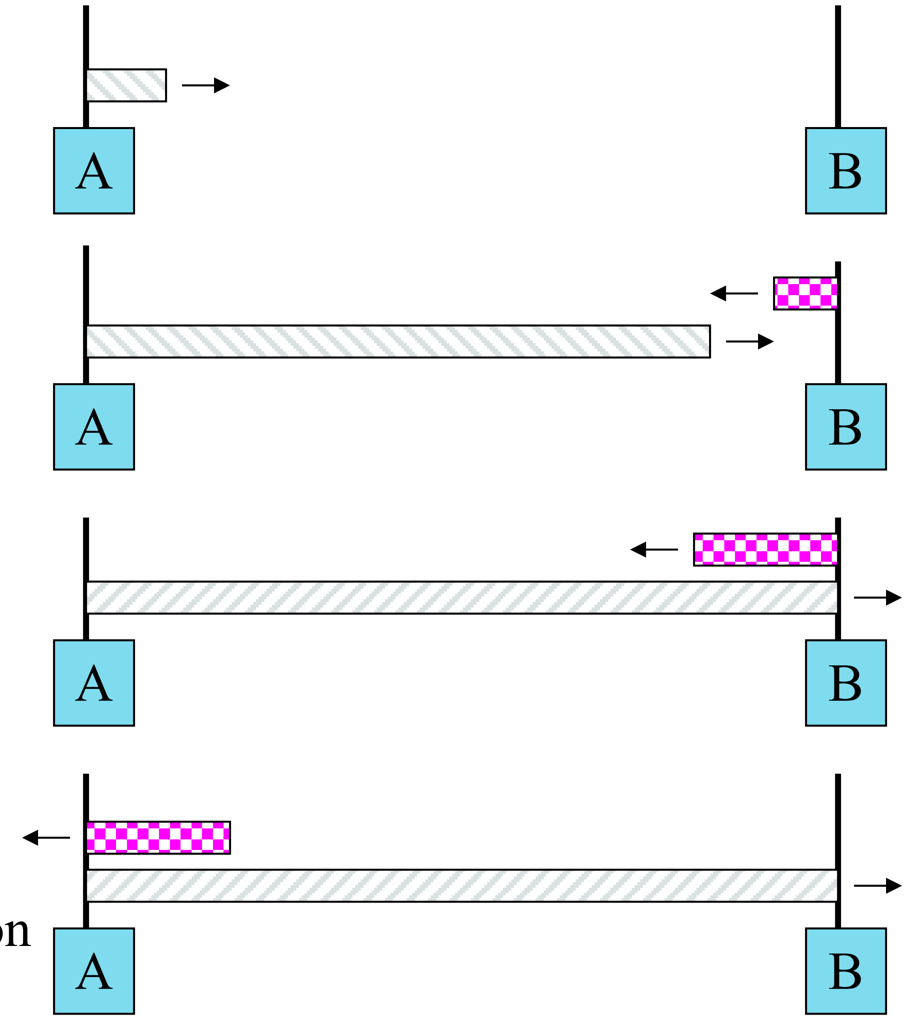
t_0 — A begins transmission

$t_0+T_p-\varepsilon$ — B begins transmission

t_0+T_p — B detects collision

$t_0+2T_p-\varepsilon$ — A detects collision just before end of transmission

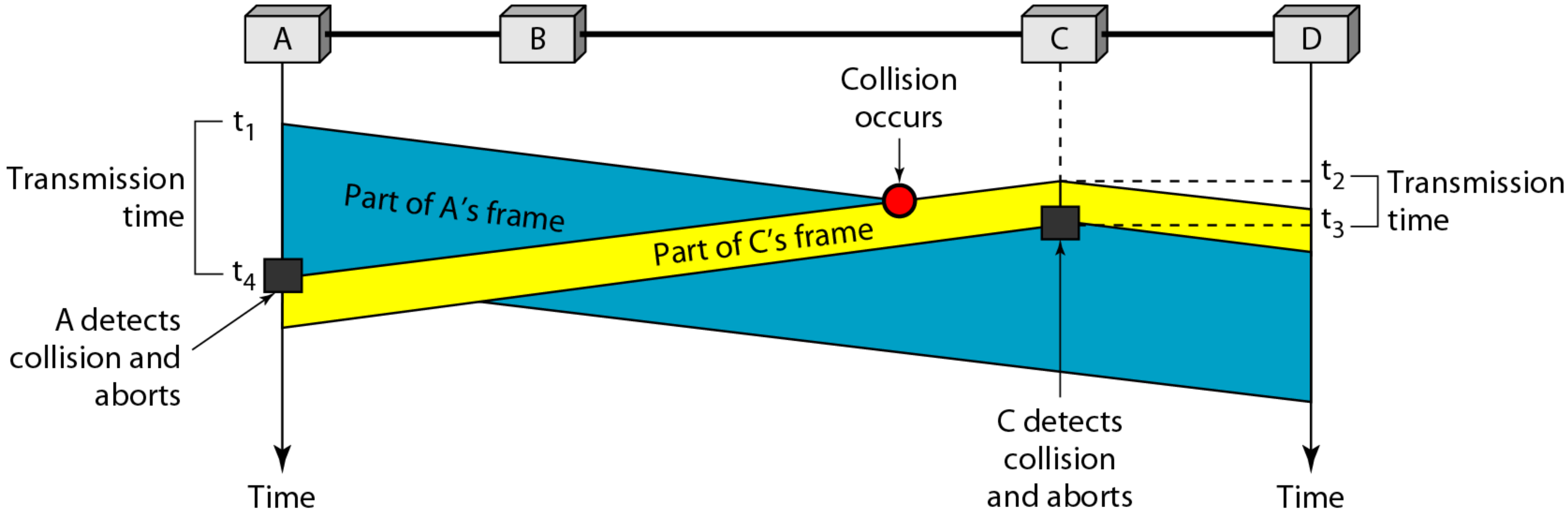
Time



(T_p is the propagation time)

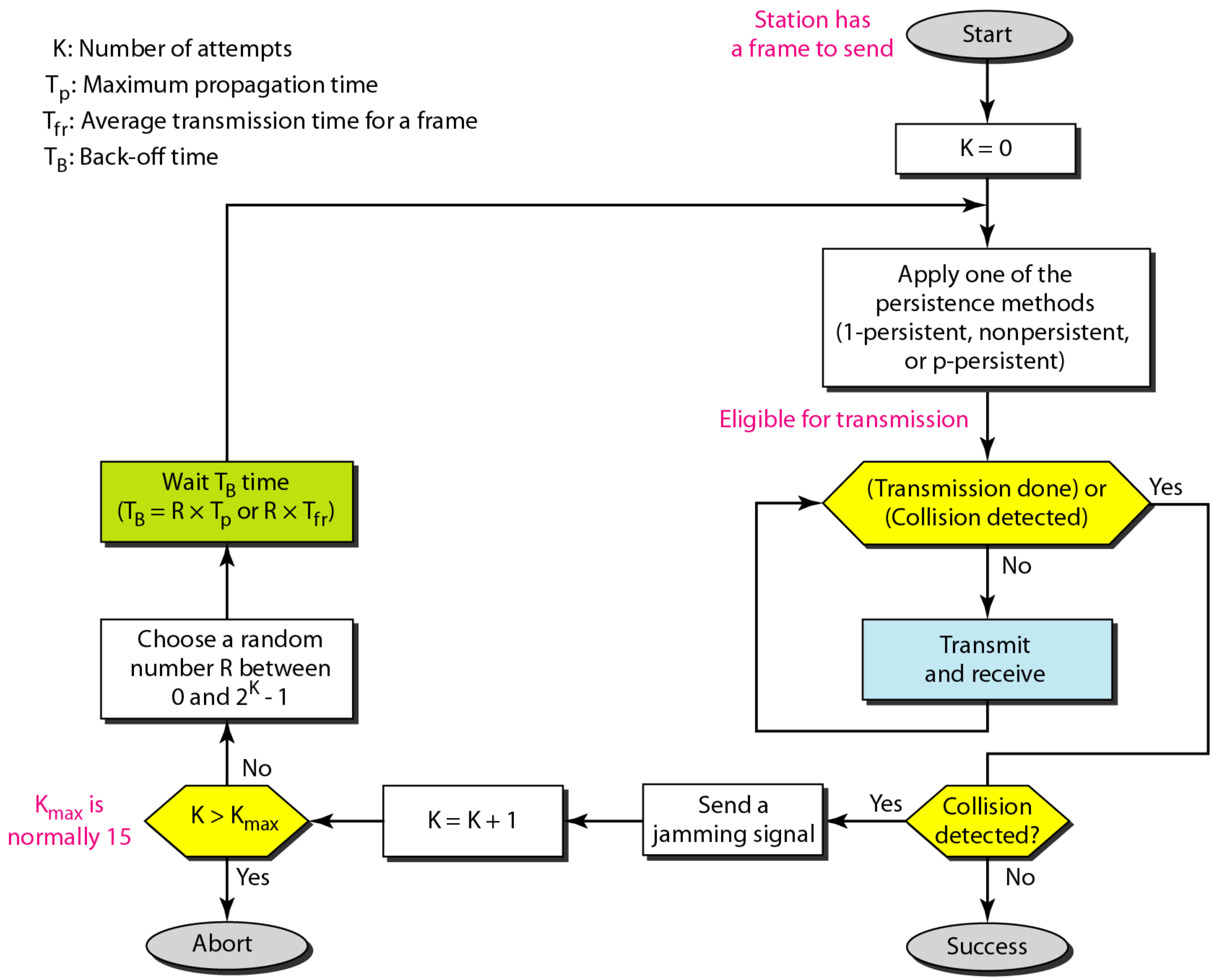
Random Access: CSMA/CD

Collision Detection and Abortion Example



Random Access: CSMA/CD

FlowChart Operation



IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Random Access: CSMA/CD

The worst-case scenario to detect the collision

- A network using CSMA/CD MAC protocol has a bandwidth of 10 Mbps. If the maximum propagation time T_p, including the delays in the devices and ignoring the time required to transmit a jamming signal, is 25.6 μs, what should be the minimum size of a frame in 10 Mbps Ethernet network?

Random Access: CSMA/CD

The worst-case scenario to detect the collision

- A network using CSMA/CD MAC protocol has a bandwidth of 10 Mbps. If the maximum propagation time T_p, including the delays in the devices and ignoring the time required to transmit a jamming signal, is 25.6 μs, what should be **the minimum size of a frame** in 10 Mbps Ethernet network?

Solution

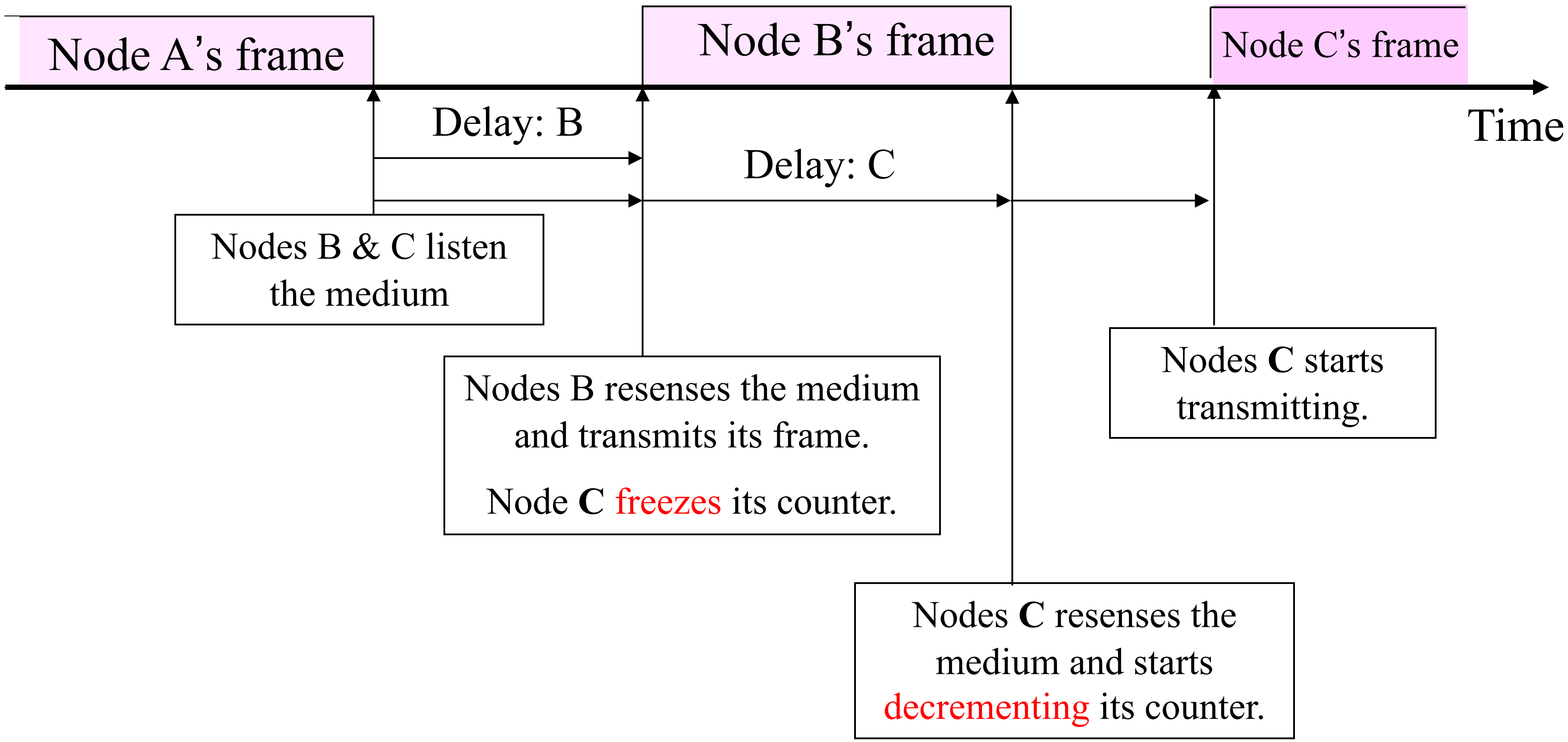
- In CSMA/CD, the size of a frame must be large enough so that collision can be detected by sender while sending the frame. So, the frame transmission time (**T_{fr}**) **must be at least two times the maximum propagation time** (**T_p**).

- The frame transmission time is $T_{fr} = 2 \times T_p = 51.2$ μs. This means, in the worst case, a device needs to transmit for a period of 51.2 μs to potentially detect the collision. The minimum size of the frame would be 10 Mbps × 51.2 μs = 512 bits or 64 bytes ($L = T_{fr} \times R$). This is actually the minimum size of the frame for 10 Mbps Ethernet network.

- ALOHA
- Slotted ALOHA
- CSMA (Carrier Sense Multiple Access)
- CSMA/CD (CSMA with Collision Detection)
- CSMA/CA (CSMA with Collision Avoidance)
  - CSMA/CA with ACK
  - CSMA/CA with RTS/CTS

Random Access: CSMA/CA

Operation Example



Random Access: CSMA/CA

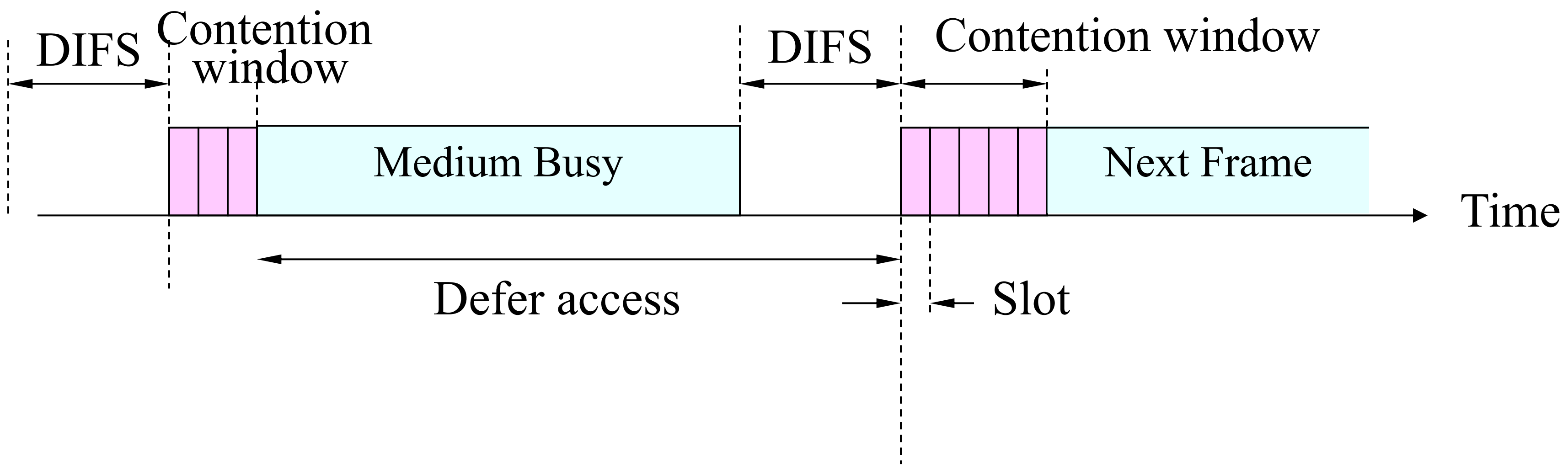
CSMA/CA (CSMA with Collision Avoidance)

- In CSMA/CA:
  - Step 1: All terminals listen to the same medium as CSMA/CD.
  - Step 2: If medium is busy, it waits until the end of current transmission.
  - Step 3: It again waits for an additional predetermined time DCF* Interframe Space (**DIFS**).
  - Step 4: Then picks up a random number of slots (the initial value of back-off counter) within a **contention window** to wait before transmitting its frame (P-persistent).
  - Step 5: If there are transmissions by other terminals during this period, the terminal freezes its counter.
  - Step 6: It resumes count down after other terminals finish transmission + DIFS. The terminal can start its transmission when the counter reaches to zero.

* DCF = Distributed Coordination Function

Random Access: CSMA/CA

Detailed Operation Example



DIFS – DCF Interframe Space

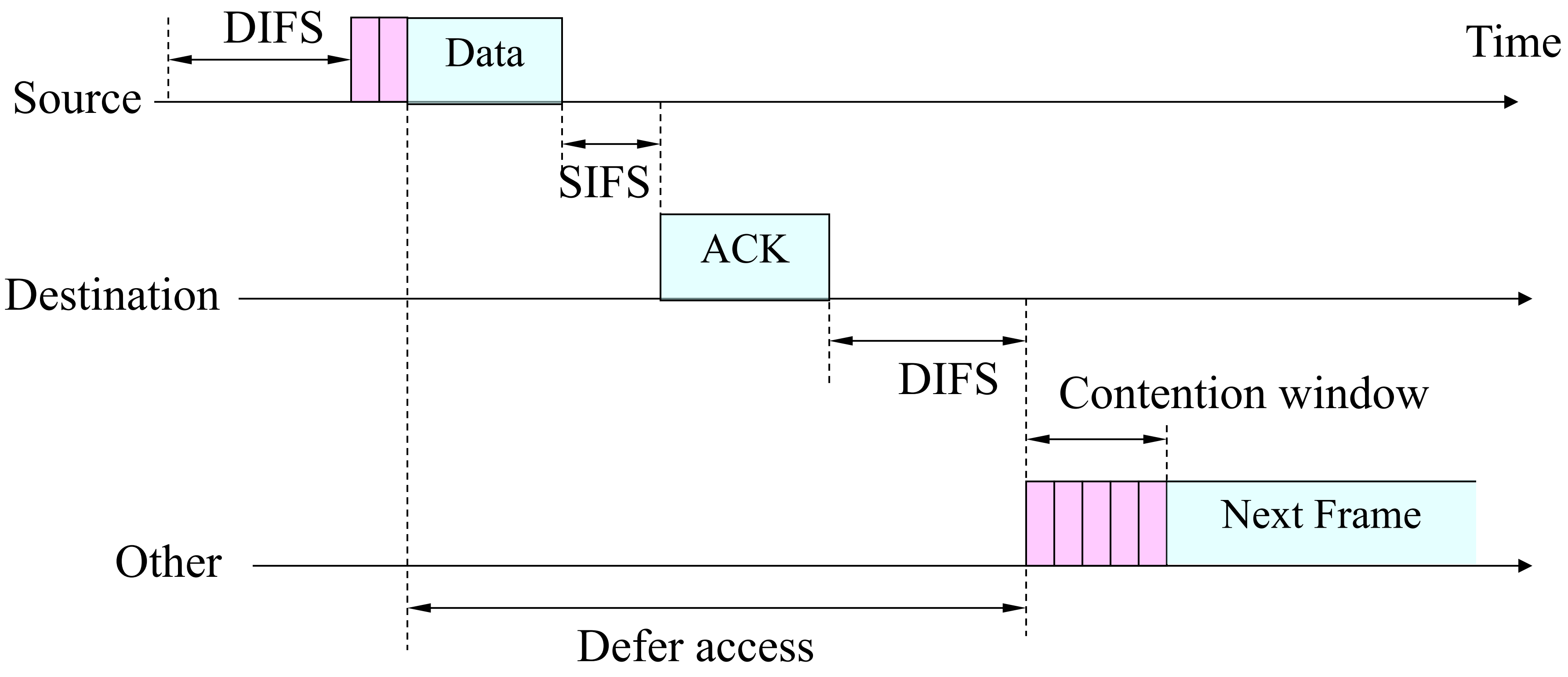
Random Access: CSMA/CA with ACK

CSMA/CA (CSMA with Collision Avoidance) with ACK

- In CSMA/CA with ACK:
  - Immediate Acknowledgements from receiver upon reception of data frame without any need for sensing the medium.
  - ACK frame transmitted after time interval Short Interframe Space (SIFS), where SIFS < DIFS.
  - Receiver transmits ACK without sensing the medium.
  - If ACK is lost, a retransmission will follow up.

Random Access: CSMA/CA with ACK

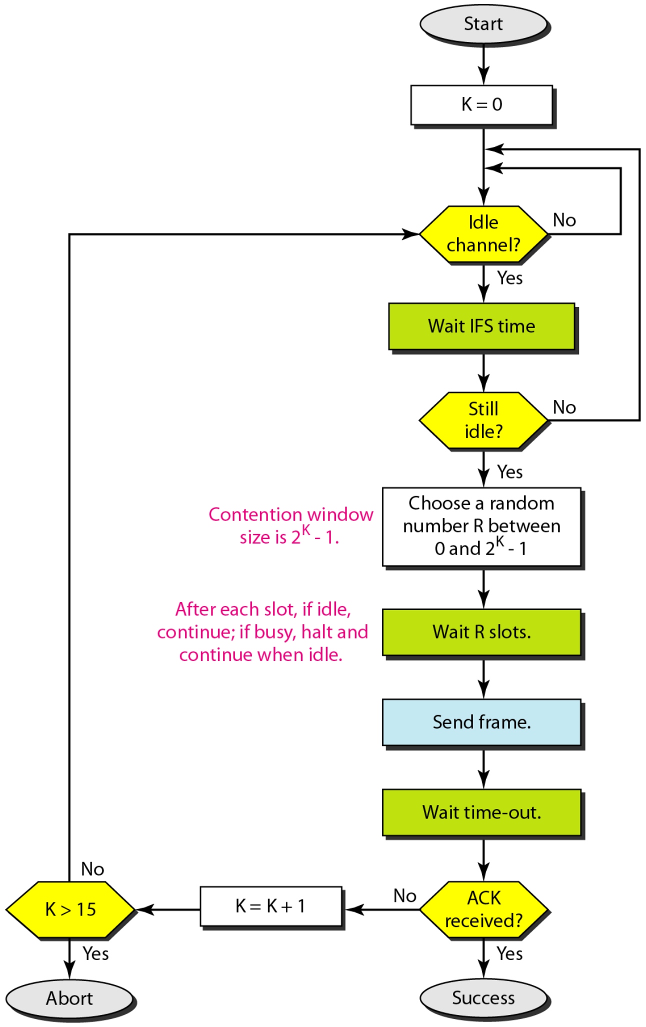
Operation Example



SIFS – Short Interframe Space

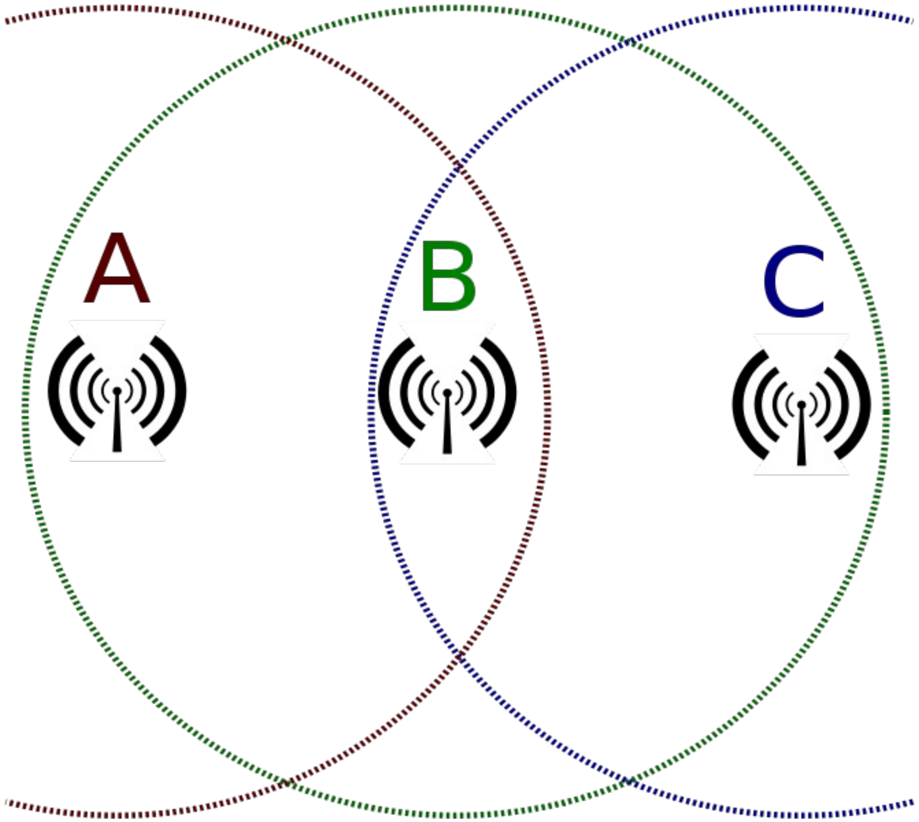
Random Access: CSMA/CA with ACK

Flowchart Operation Example



Random Access: CSMA/CA with ACK

Hidden Node Problem



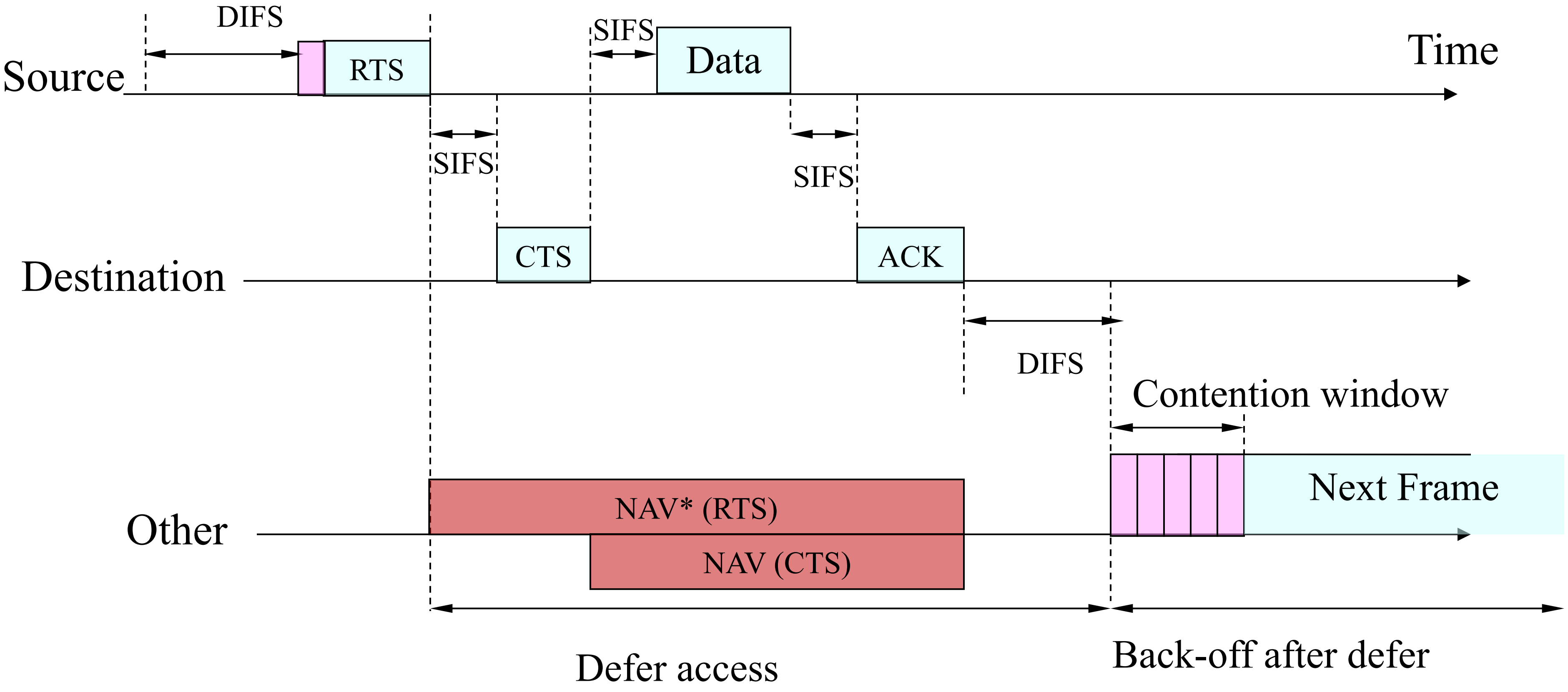
Random Access: CSMA/CA with ACK & with RTS/CTS

CSMA/CA (CSMA with Collision Avoidance) with ACK & with RTS/CTS

- In CSMA/CA with ACK and with RTS/CTS:
  - Transmitter sends an Request To Send (RTS) after medium has been idle for time interval more than DIFS.
  - Receiver responds with Clear To Send (CTS) after medium has been idle for SIFS.
  - Then Data is exchanged.
  - RTS/CTS is used for reserving channel for data transmission so that the collision can only occur in control message.

Random Access: CSMA/CA with ACK & with RTS/CTS

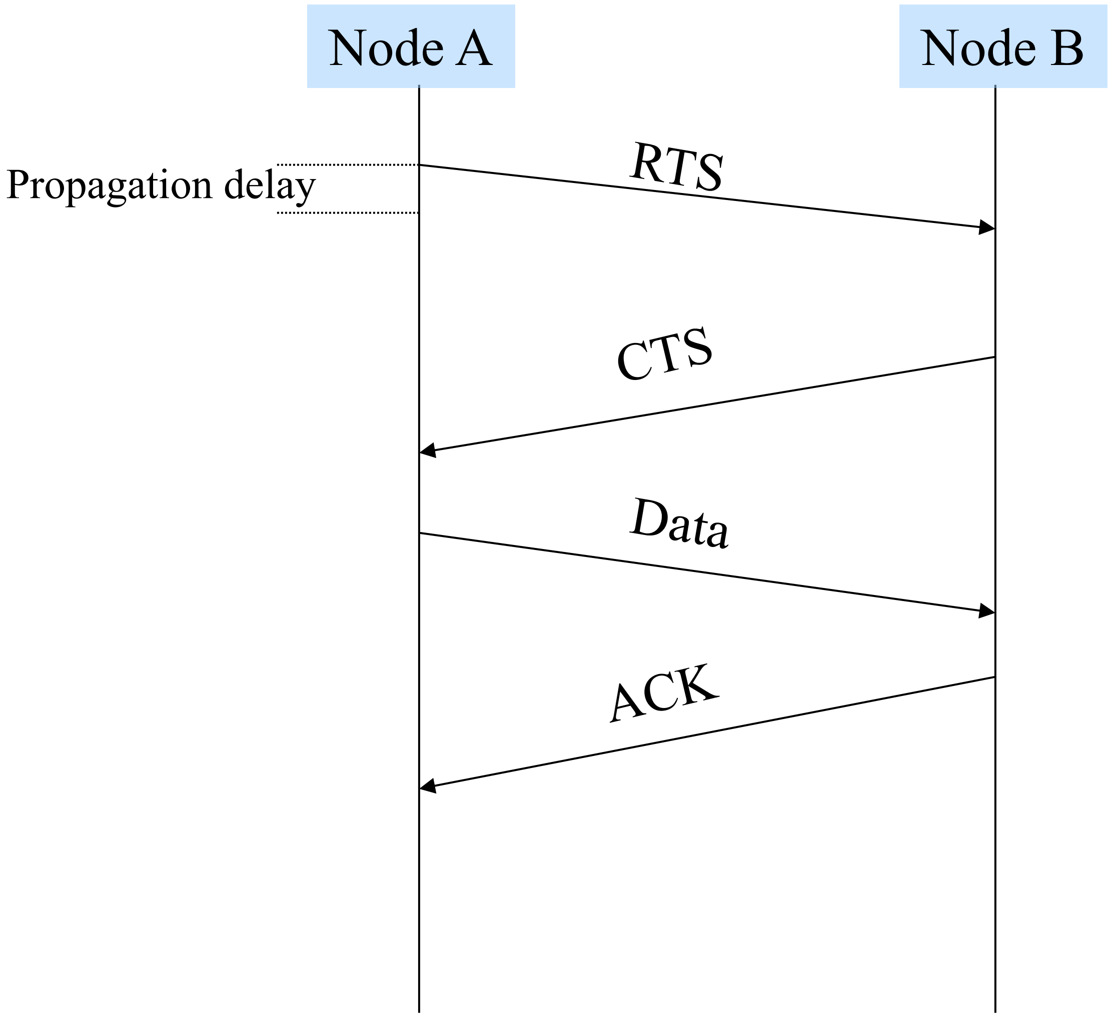
Operation Example

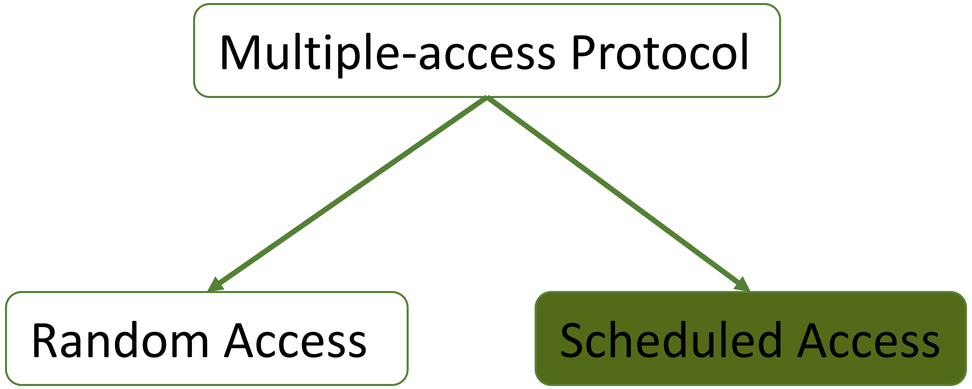


* NAV = Network Allocation Vector

Random Access: CSMA/CA with ACK & with RTS/CTS

Operation Timeline

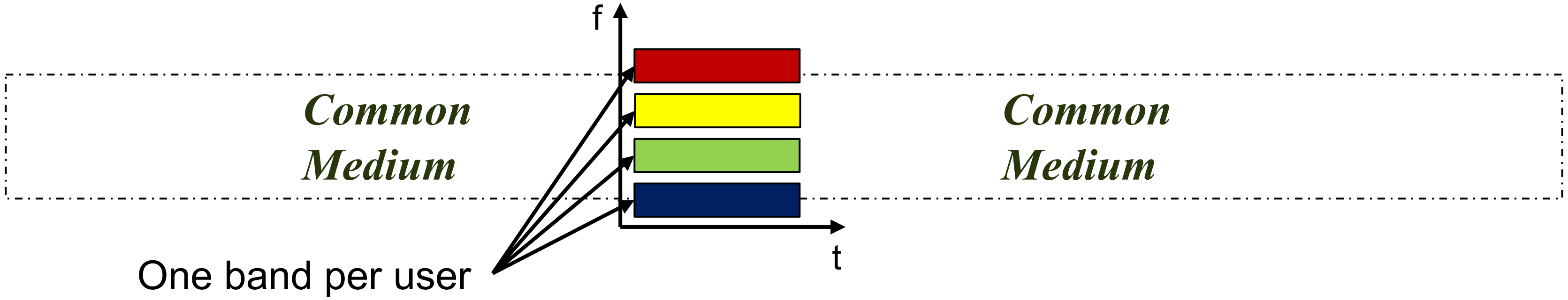



Multiple-access Protocol
Random Access
Scheduled Access

Frequency-Division Multiple Access (FDMA)

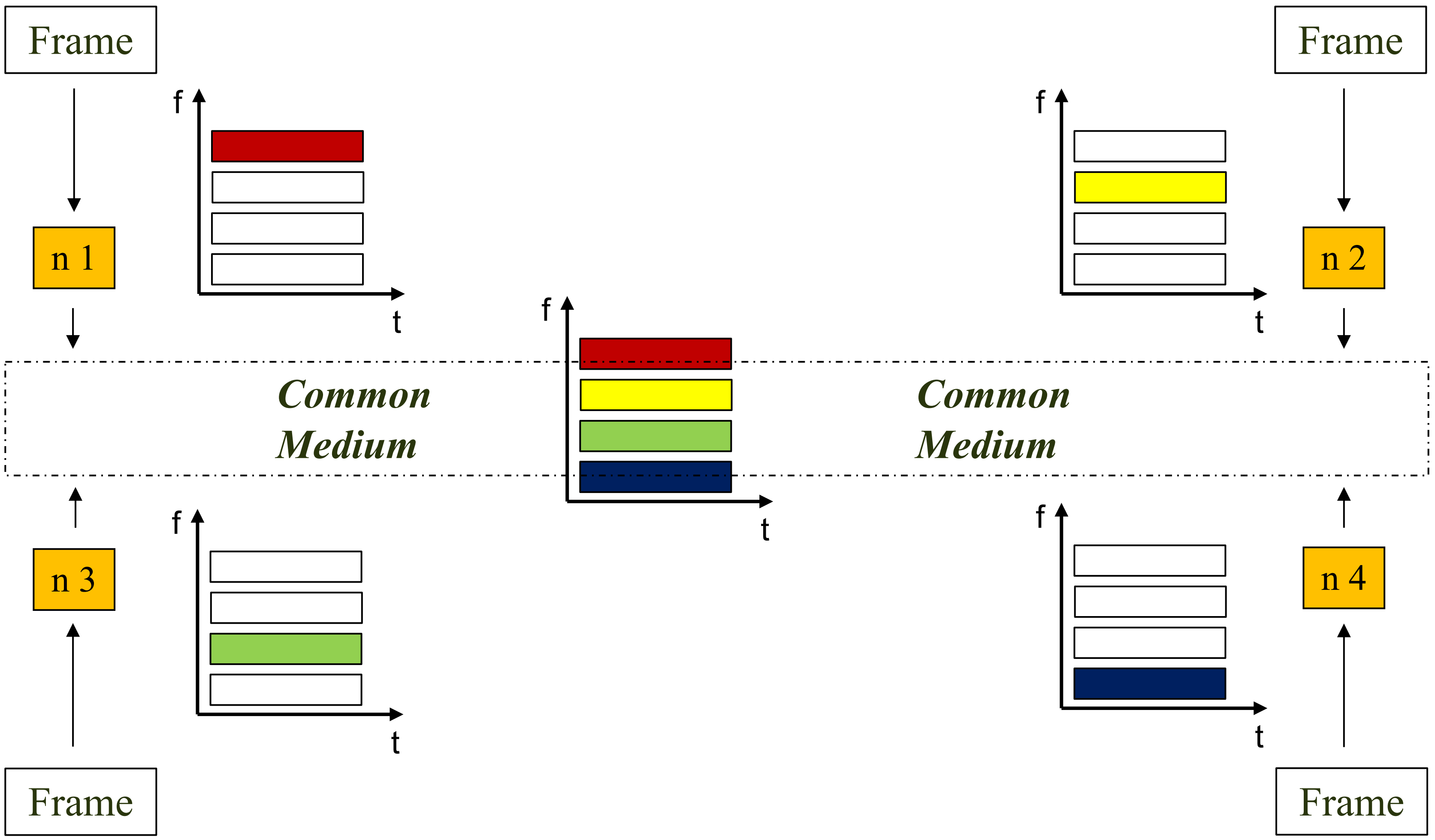
Overview

Under FDMA method, the available channel or bandwidth is divided into multiple individual bands that are separated by guard bands, each for use by a single user.



Frequency-Division Multiple Access (FDMA)

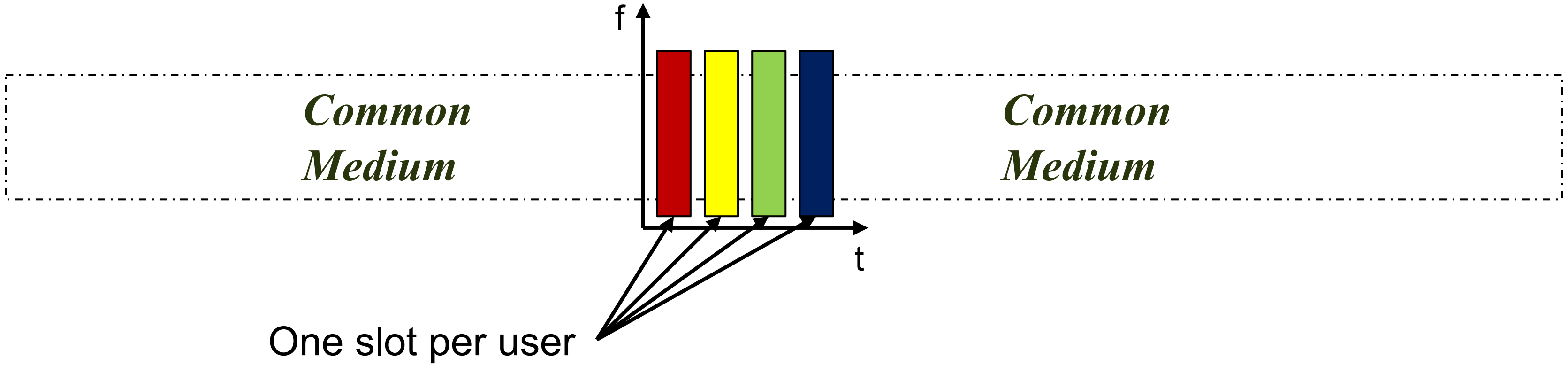
Overview



Time-Division Multiple Access (TDMA)

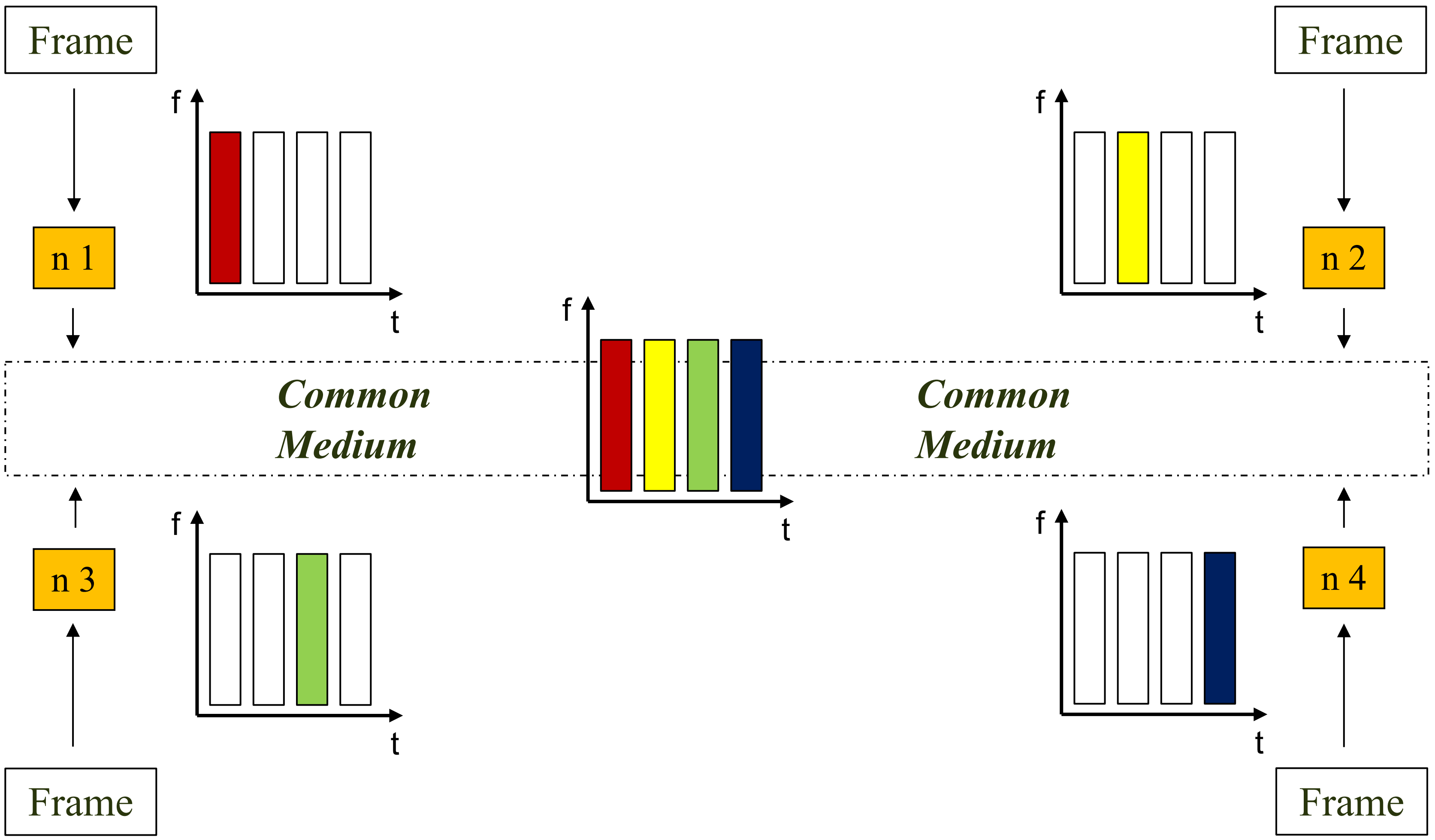
Overview

Under TDMA method, a channel is divided into time slots. Each slot is dedicated to different nodes to transmit their frames.



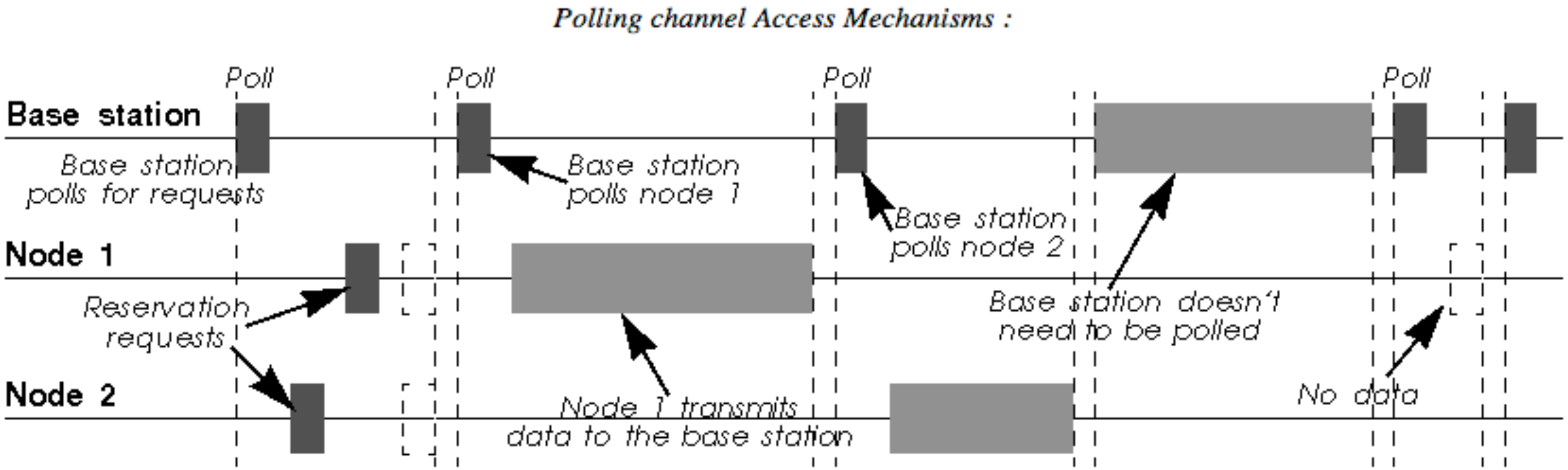
Time-Division Multiple Access (TDMA)

Overview



Polling MAC
Overview

Polling MAC is a combination of TDMA and CSMA. It comes with a Base station control mechanism, with variable packets size, and a poll mechanism.



Source: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.mac.html

Summary

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Summary

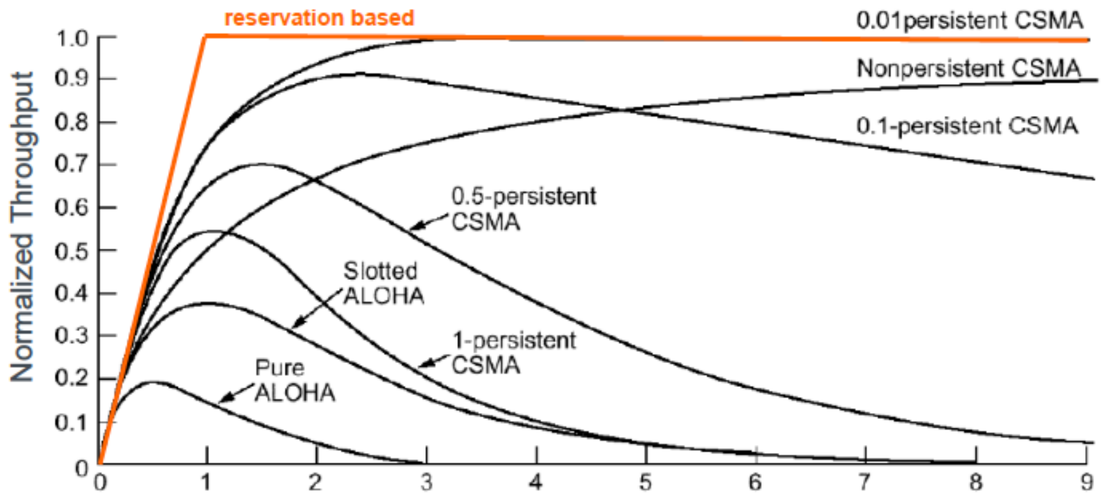
Contention-free vs. Contention-based MAC protocols

- Contention-free MAC protocols (e.g., TDMA):
  - Knowledge of topology and strict synchronization
  - Requires large overheads and/or (potentially) expensive hardware
- Contention-based MAC protocols (e.g., CSMA):
  - Throughput degradation when the traffic load increases
  - Prevents them to achieve the same efficiency as ideal reservation-based protocols

Summary

Reservation vs. Contention based MAC protocols

- Throughput versus offered load:



Pure ALOHA	$s = ge^{-2g}$
slotted ALOHA	$s = ge^{-g}$
unslotted 1 - persistant CSMA	$s = \frac{g\left[1 + g + ag\left(1 + g + \frac{ag}{2}\right)\right]e^{-g(1+2a)}}{g(1+2a) - \left(1 - e^{-ag}\right) + (1 + ag)e^{-g(1+a)}}$
slotted 1 - persistant CSMA	$s = \frac{g\left[1 + a - e^{-ag}\right]e^{-g(1+a)}}{(1+a)\left(1 - e^{-ag}\right) + ae^{-g(1+a)}}$
unslotted nonpersistant CSMA	$s = \frac{ge^{-ag}}{g(1+2a) + e^{-ag}}$
slotted nonpersistant CSMA	$s = \frac{age^{-ag}}{1 - e^{-ag} + a}$

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.74.8411&rep=rep1&type=pdf

Q&A

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Q&A

- What is the role of the Medium Access Control protocol?

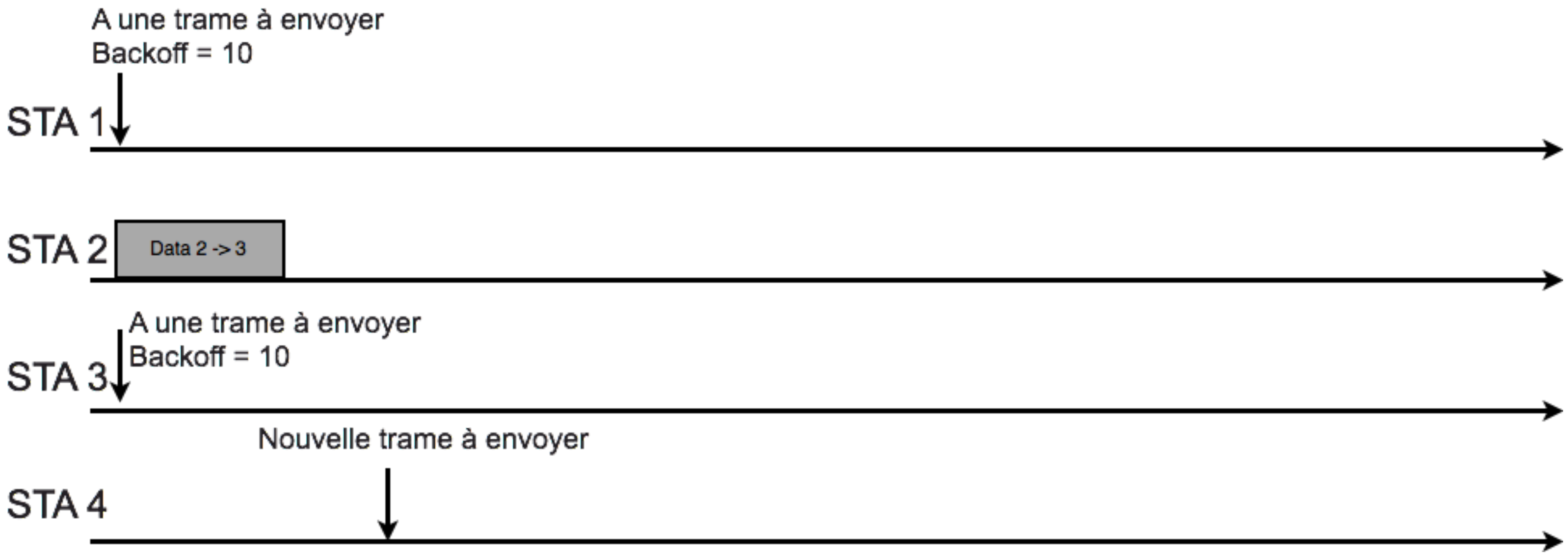
- Which are the main techniques to access the wireless medium?
- Comment the difficulties of their implementation and on their performances.

- How to ensure that a data packet was received successfully at the destination?

- In Wi-Fi, what is the purpose of employing RTS and CTS handshake?

Q&A

- In the following scenario (i.e., Wi-Fi), design the following up exchanged packets.



IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Medium Access Control (MAC) - Fundamentals

Georgios Z. **PAPADOPOULOS, PhD, HDR**
e-mail: georgios.papadopoulos@imt-atlantique.fr
web: www.georgiospapadopoulos.com
twitter: @gzpapadopoulos
youtube: www.youtube.com/c/gzpapadopoulos