Wireless Networks for Mobile Applications

Prof. Claudio Palazzi
cpalazzi@math.unipd.it

Università degli Studi di Padova

Multiple Access Control (MAC) Layer

- Media Access Control protocol: coordination and scheduling of transmissions among competing neighbors

- Access control to shared channel(s)
  - Natural broadcast of wireless transmission
  - Collision of signal: a time/space problem
  - Who transmits when? (and where)?
  - Avoid collisions (no Collision Detection)

- Scarce resources utilization
  - Channel capacity and battery power

- Goals: low latency, good channel utilization; best effort + real time support

MAC Layer's Role

- 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

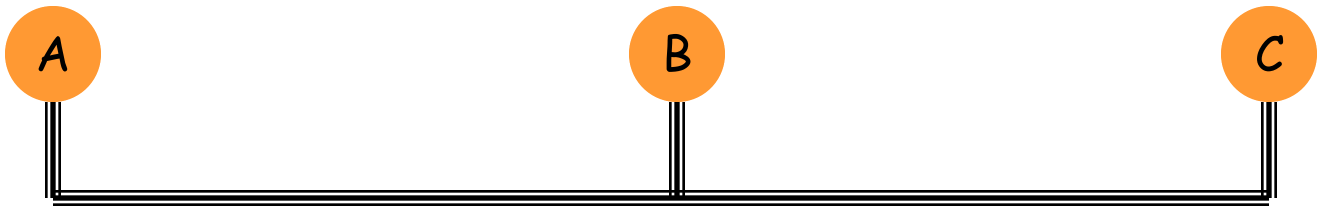
Wired Vs Wireless Media Access

Both are on shared media.

Then, what's really the problem ?

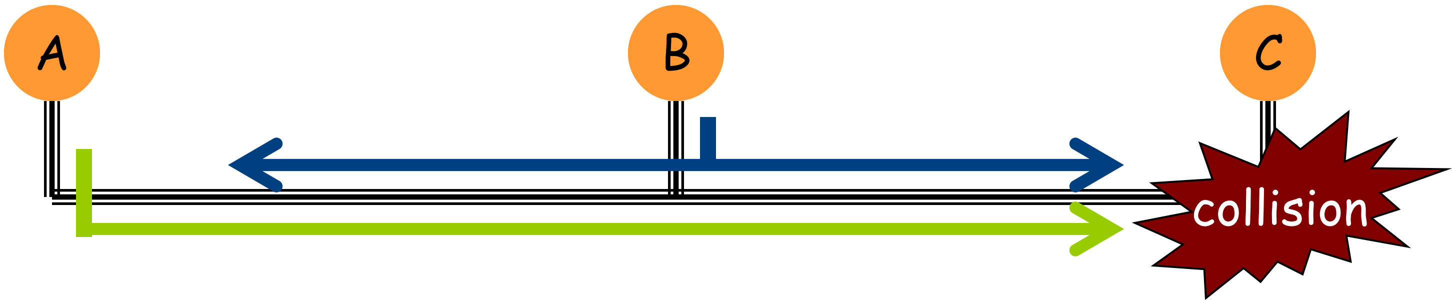
The Channel Access Problem

- Multiple nodes share a channel



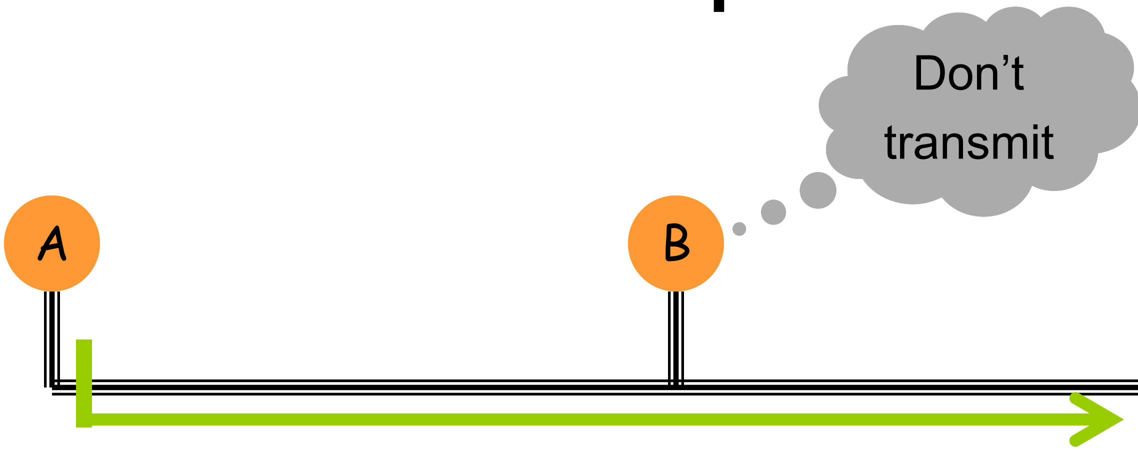
- Pairwise communication desired
  - Simultaneous communication not possible
- MAC Protocols
  - Suggests a scheme to schedule communication
    - Maximize number of communications
    - Ensure fairness among all transmitters

The Trivial Solution



- Transmit and pray
  - Plenty of collisions --> poor throughput at high load

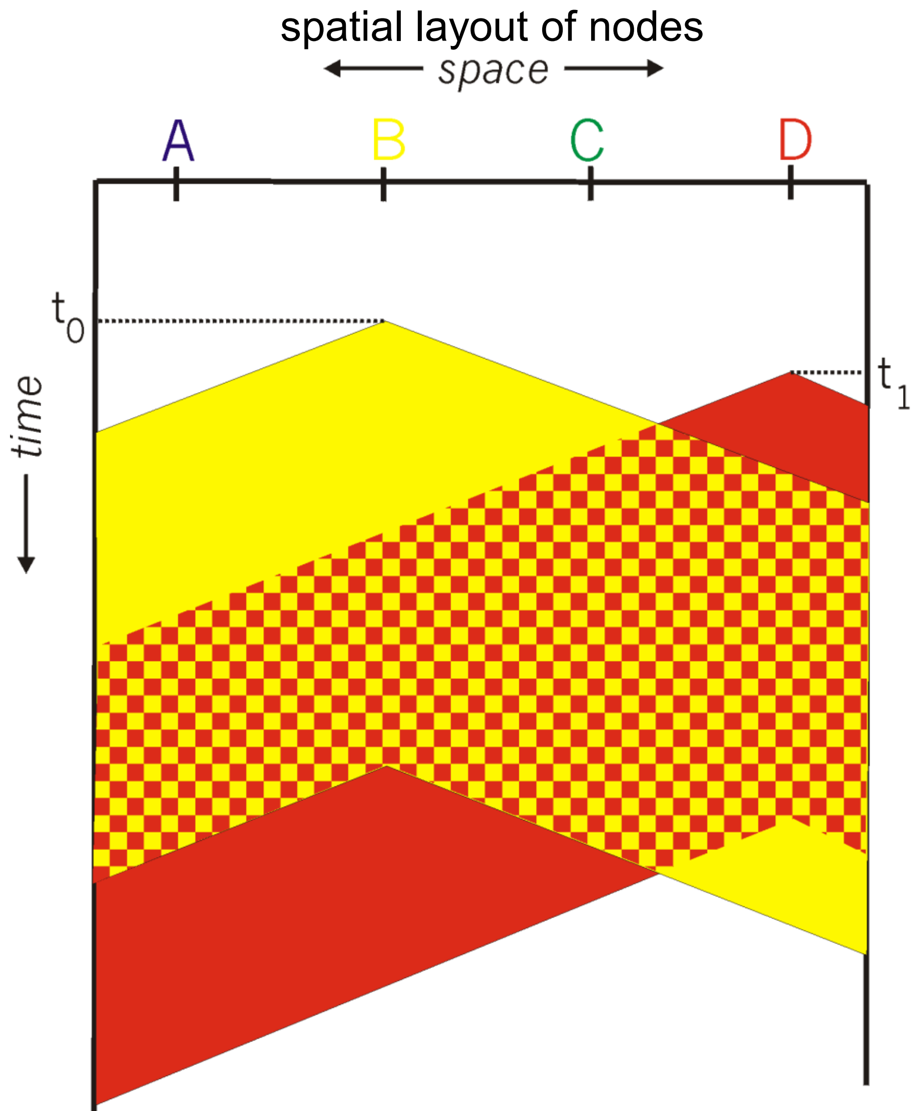
The Simple Fix



Can collisions still occur?

- Transmit and pray
  - Plenty of collisions --> poor throughput at high load
- Listen before you talk
  - Carrier sense multiple access (CSMA)
  - Defer transmission when signal on channel

CSMA collisions



Collisions can still occur:

Propagation delay non-zero between transmitters

When collision:

Entire packet transmission time wasted

note:

Role of distance & propagation delay in determining collision probability

MAC Layer's Aims

- Considering *B* = available bandwidth on the channel

- Desirable features:
  - *Efficiency* in bandwidth use (sum of rates = *B*)
    - If just one node, it should transmit at *B* rate
  - *Resilience*: Avoid collisions
  - *Fairness*: If *M* nodes want to transmit each should have *B/M* bandwidth available (in average)
  - *Robustness*: the protocol should be decentralized (no single point of failure)
  - *Simplicity*: the protocol should be easily implementable

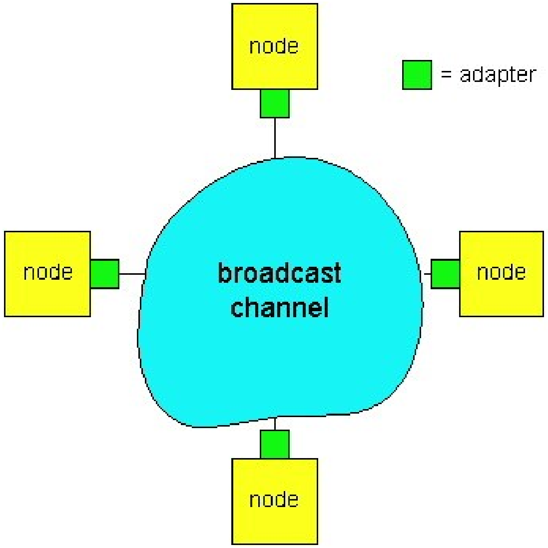
- PROJECT IDEA: consider different mac protocols and investigate whether some of these properties (e.g., Efficiency) are maintained in certain realistic scenarios

MAC Protocols

- FDMA/TDMA/CDMA
- ALOHA
- CSMA (Packet Radio Net)
- IEEE 802.11
- Bluetooth

MAC Layer

- MAC protocol: coordinates transmissions from different stations in order to minimize/avoid collisions
- (a) **Channel Partitioning** MAC protocols: TDMA, FDMA, CDMA
- (b) **Random Access** MAC protocols: CSMA, MACA
- (c) **"Taking turns"** MAC protocols: polling



MAC Layer Approaches

- Random Access (with contention)
  - Without *carrier sensing (*E.g., Aloha, Slotted Aloha)
  - With *carrier sensing* (E.g.,: CSMA, CSMA/CD, MACAW)

- Controlled Access
  - Centralized: there is an entity that is responsible to regulate the access to the channel (E.g., FDMA, TDMA, CDMA)
  - Distributed: the access to the channel is controlled by a distributed applications, with peer nodes (E.g., Token ring,)

- … obviously, hybrid solutions are possible

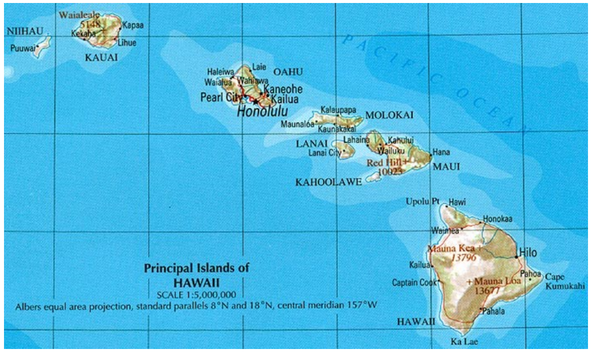
Random Access Protocols

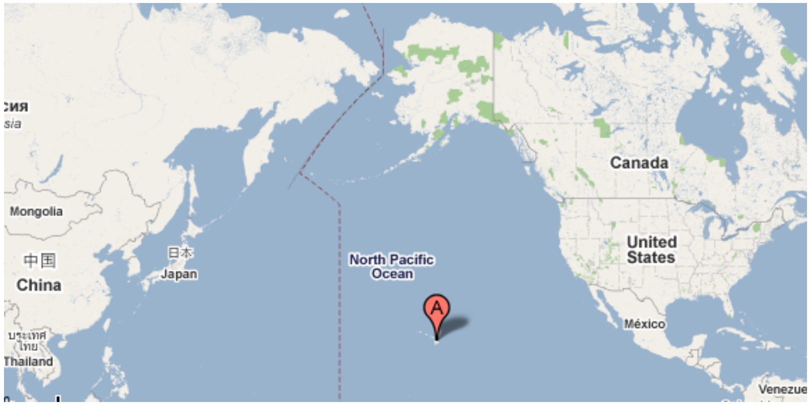
- A node transmits **at random** (i.e., no pre-coordination among nodes) at **full** channel data rate R
- If the transmissions of two or more nodes **collide**, they retransmit at random times
- The **random access MAC** protocol specifies how to detect collisions and how to recover from them (via delayed retransmissions, for example)
- Examples of random access MAC protocols:

- (b) SLOTTED ALOHA
- (a) ALOHA
- (c) CSMA and CSMA/CD

ALOHA

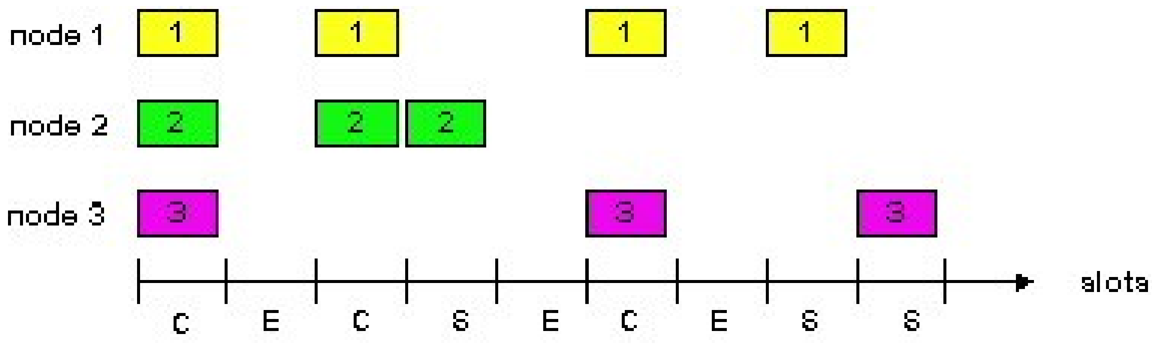
- Developed in the 70’s by University of Hawaii to have islands able to communicate among themselves and with the mainland.



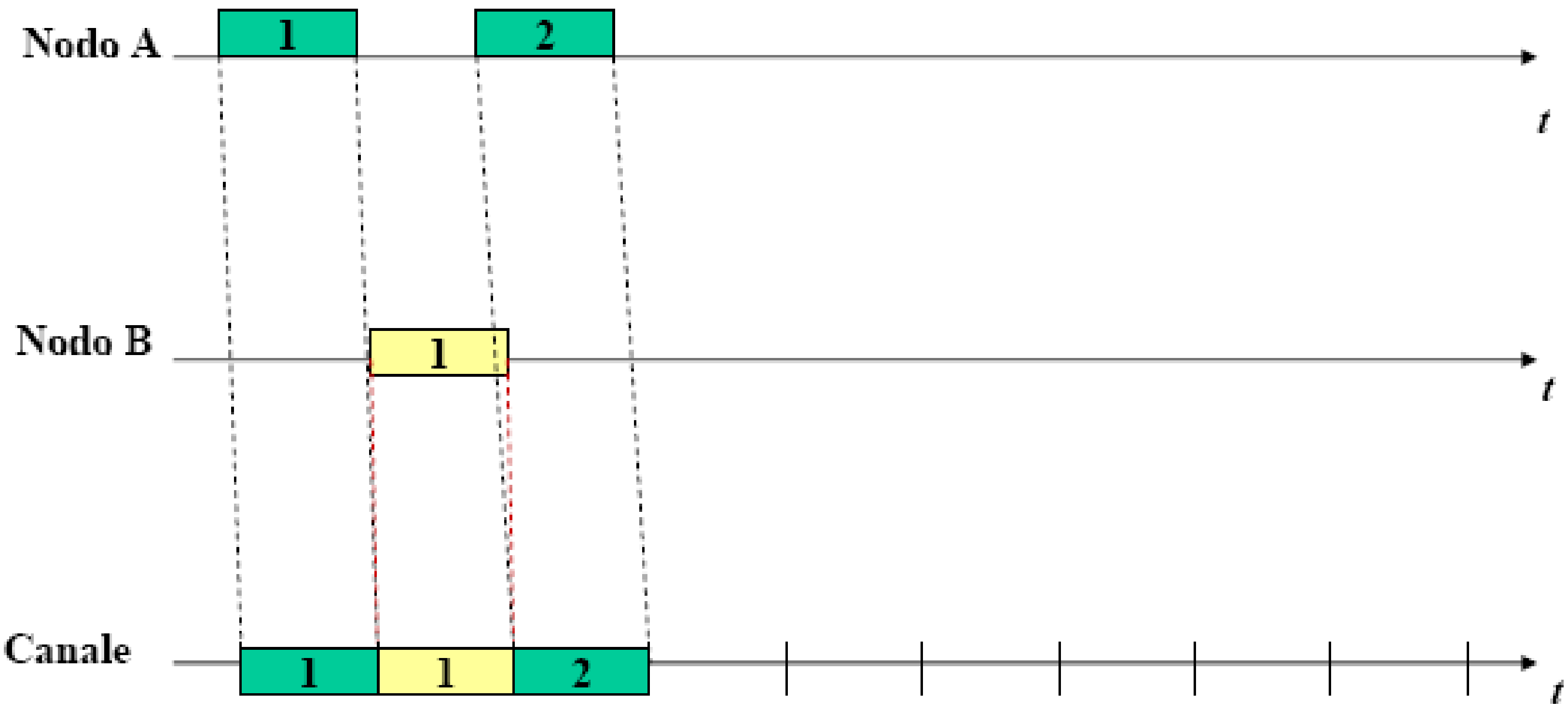


Slotted ALOHA

- Time is divided into equal size slots (= full packet size)
- a newly arriving station transmits a the beginning of the next slot
- if collision occurs (assume channel feedback, e.g. the receiver informs the source of a collision), the source retransmits the packet at each slot with probability P, until successful.
- Success (S), Collision (C), Empty (E) slots
- S-ALOHA is fully decentralized
- Throughput efficiency = 1/e

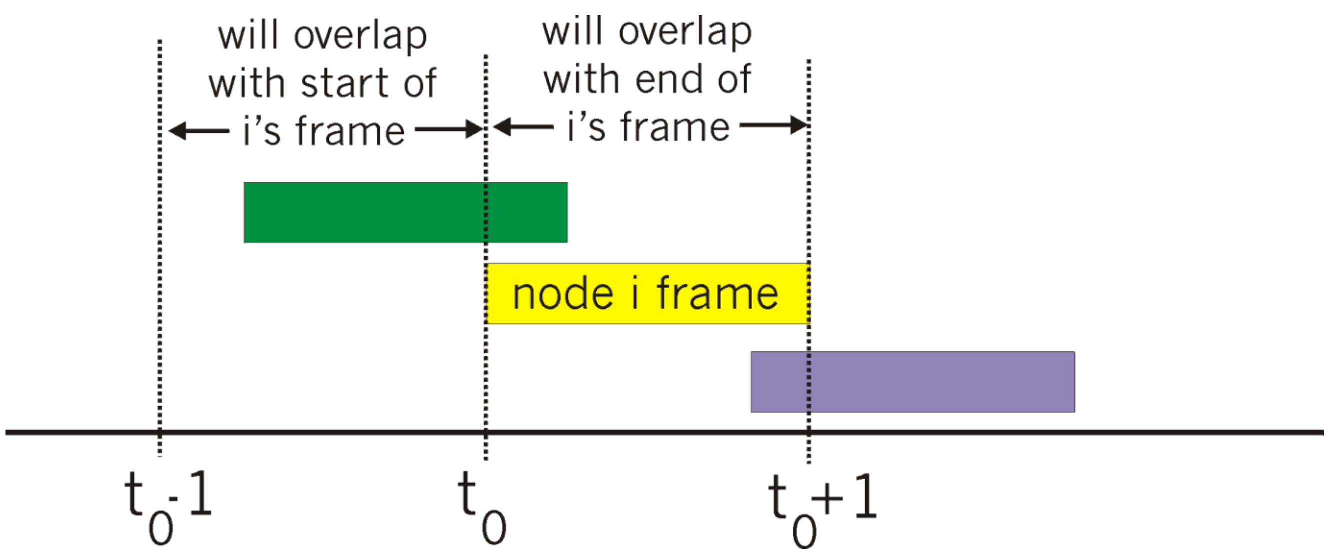


Slotted ALOHA: an Example

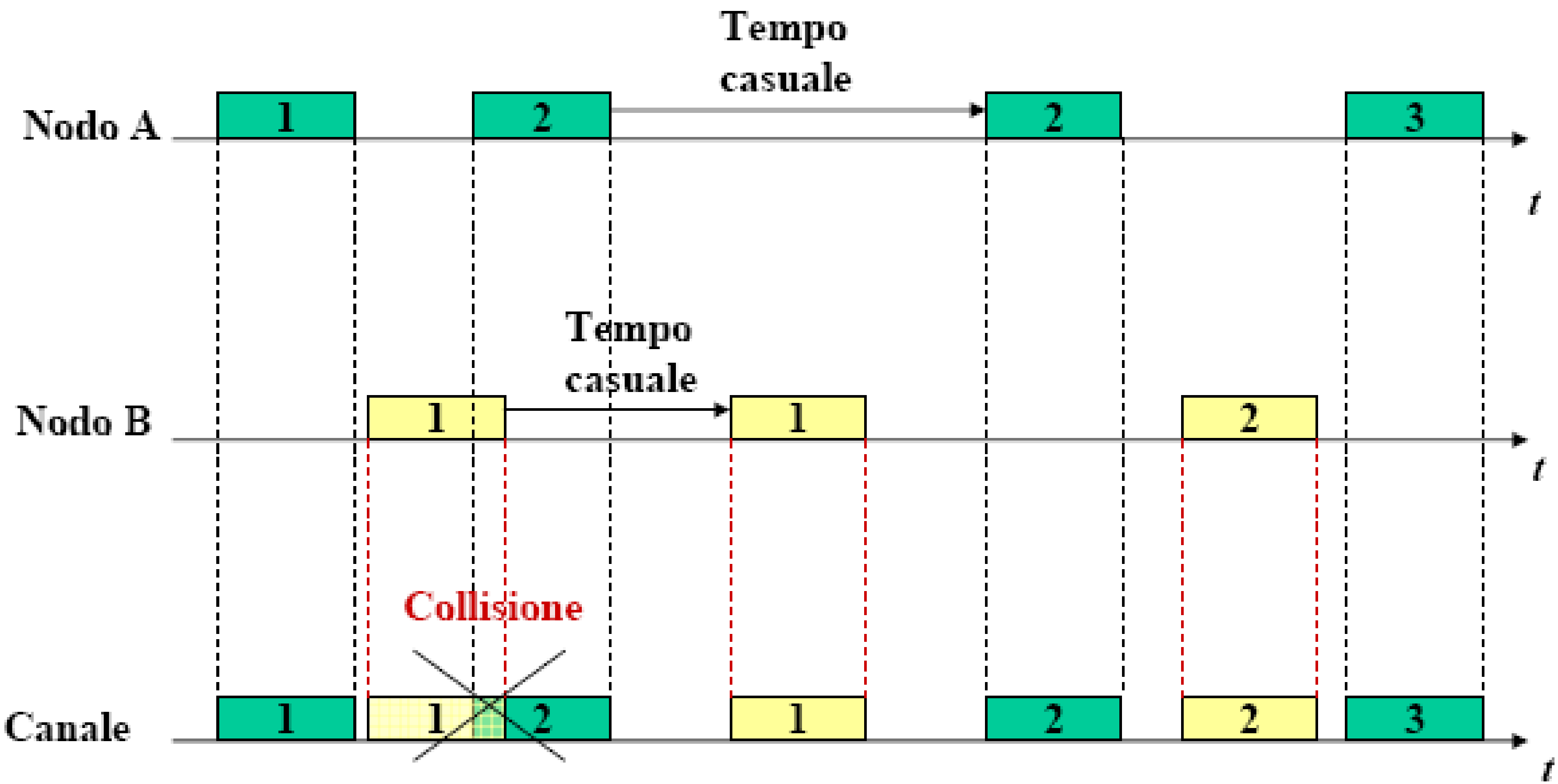


Pure (Unslotted) ALOHA

- Slotted ALOHA requires slot synchronization
- A simpler version, pure ALOHA, does not require slots
- A node transmits without awaiting for the beginning of a slot
- Collision probability increases (packet can collide with packets transmitted in a “vulnerable” window twice as large as in S-Aloha)
- Throughput is reduced by one half, ie S= 1/2e



Pure ALOHA: an Example



Why random waiting time?

ALOHA and Slotted ALOHA's Efficiency

Suppose N stations have packets to send

- each transmits in slot with probability p
- prob. successful transmission S is:

by single node: $S = p\,(1-p)^{(N-1)}$

by any of N nodes

S = Prob (only one transmits) = $N\,p\,(1-p)^{(N-1)}$

ALOHA

The value of p (p*) that maximises the efficiency of ALOHA is:

$$E(p) = Np(1 - p)^{2(N-1)}$$

$$E'(p) = N(1 - p)^{2N-2} - Np2(N-1)(1 - p)^{2N-3}$$

$$= N(1-p)^{2N-3} \quad ((1 - p)-p2(N- 1))$$

$$E'(p) = 0 \Rightarrow p^* = 1/\ 2(N-1)$$

Using this value, the max efficiency of ALOHA is;

$$\lim_{(N\to \text{infinity})} E(p^*) = \tfrac{1}{2} * 1/e = 1/2e$$

Slotted ALOHA

The value of p (p*) that maximises the efficiency of slotted ALOHA is:

$E(p) = Np(1 - p)^{N-1}$

$E'(p) = N(1 - p)^{N-1} - Np(N-1)(1 - p)^{N-2}$

$= N(1-p)^{N-2}((1 - p)-p(N- 1))$

$E'(p) = 0 \Rightarrow p^* = 1/N$

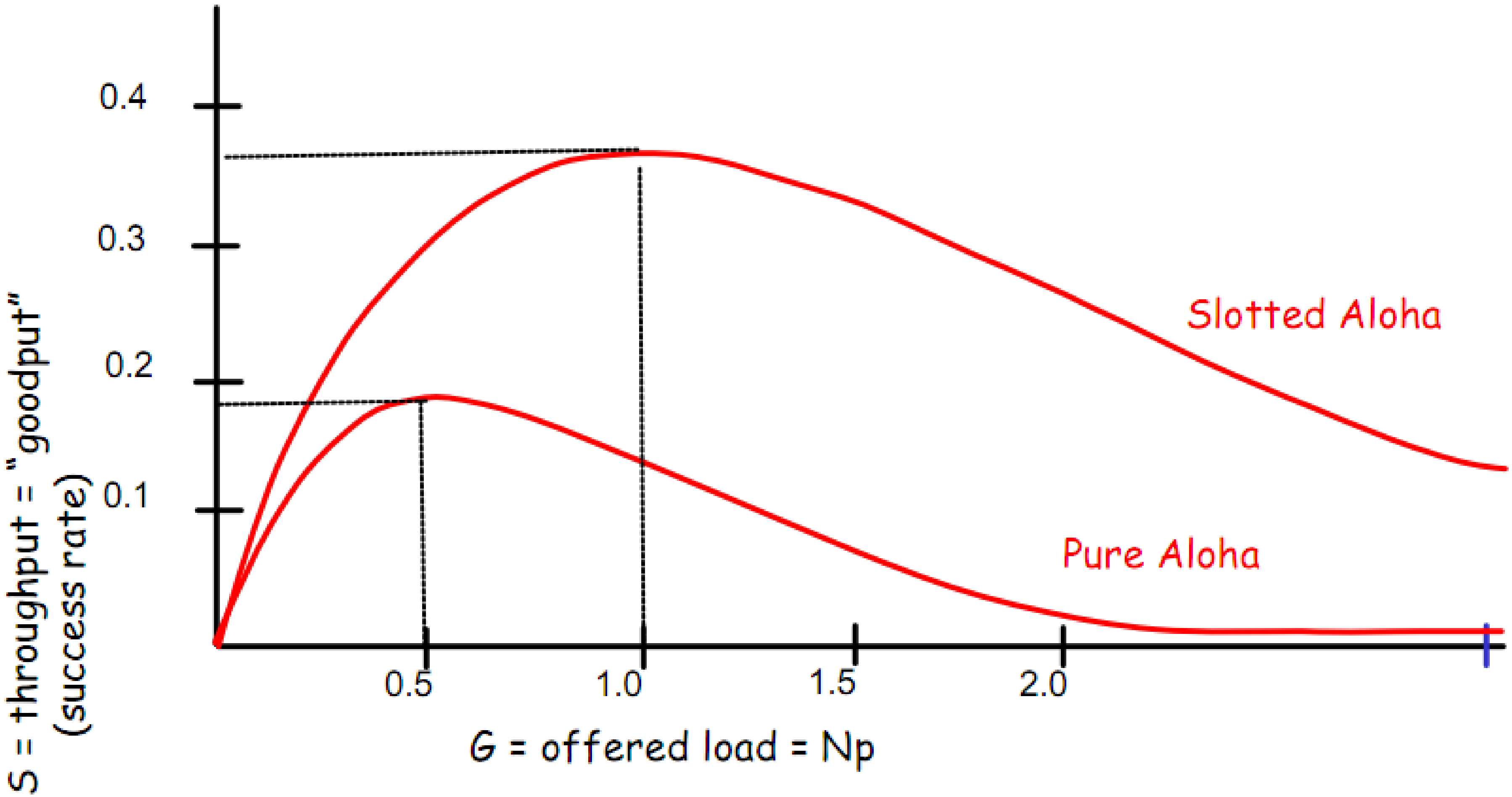
Using this value, the max efficiency of slotted ALOHA is;

$E(p^*)=N\,1/N(1-1/N)^{N-1} = (1-1/N)^{N-1} = (1-1/N)^{N}/(1-1/N)$

$\lim_{(N\to \text{infinity})} (1-1/N) = 1 \quad \lim_{(N\to \text{infinity})} (1-1/N)^{N} = 1/e$

Thus: $\lim_{(N\to \text{infinity})} E(p^*) = 1/e$

ALOHA vs Slotted ALOHA



ALOHA and Slotted ALOHA

- They are both NOT efficient max throughput is 0.184 (Aloha) or 0.368 (Slotted Aloha), when the actual channel availability is 1.

- They are both unfair: aggressive senders capture the channel

- They are both robust: no entity to control the system
  - clock/slot synchronization?

- They are simple
  - no coordination for Pure ALHOA
  - just synchronization for Slotted Aloha

Carrier Sense Multiple Access (CSMA)

• Low performances of Pure Aloha and Slotted Aloha are due to the lack of coordination among nodes

• Efficiency can be improved if each node behaves coherently with what other nodes do

• With Carrier Sense Protocols each node continuously listens to the channel to be aware of what other nodes are doing

CSMA Protocols

Different versions of CSMA:

– 1-persistent CSMA
– nonpersistent CSMA
– p-persistent CSMA

1-persistent CSMA

- Before transmitting, each node listens to the channel
  - If the channel is free, then it transmits the packet
  - If the channel is busy, then it waits for the channel to be free and then transmits the packet (IMMEDIATELY)
  - If there is a collision, the transmitting node waits for a random time and then tries again to transmit

- Propagation time has a significant impact on performances:
  - more propagation time means more collisions (and hence less efficiency)

- There could be collissions even with no propagation time:
  - if two nodes want to transmit while there is a third one that is currently occupying the channel
  - As soon as the channel becomes free, both waiting nodes will transmit immediately, at the same time!

Nonpersistent CSMA

- Before transmitting, each node listens to the channel
  - If the channel is free, then it transmits the packet
  - If the channel is busy, then it waits for a random time and then tries again the procedure

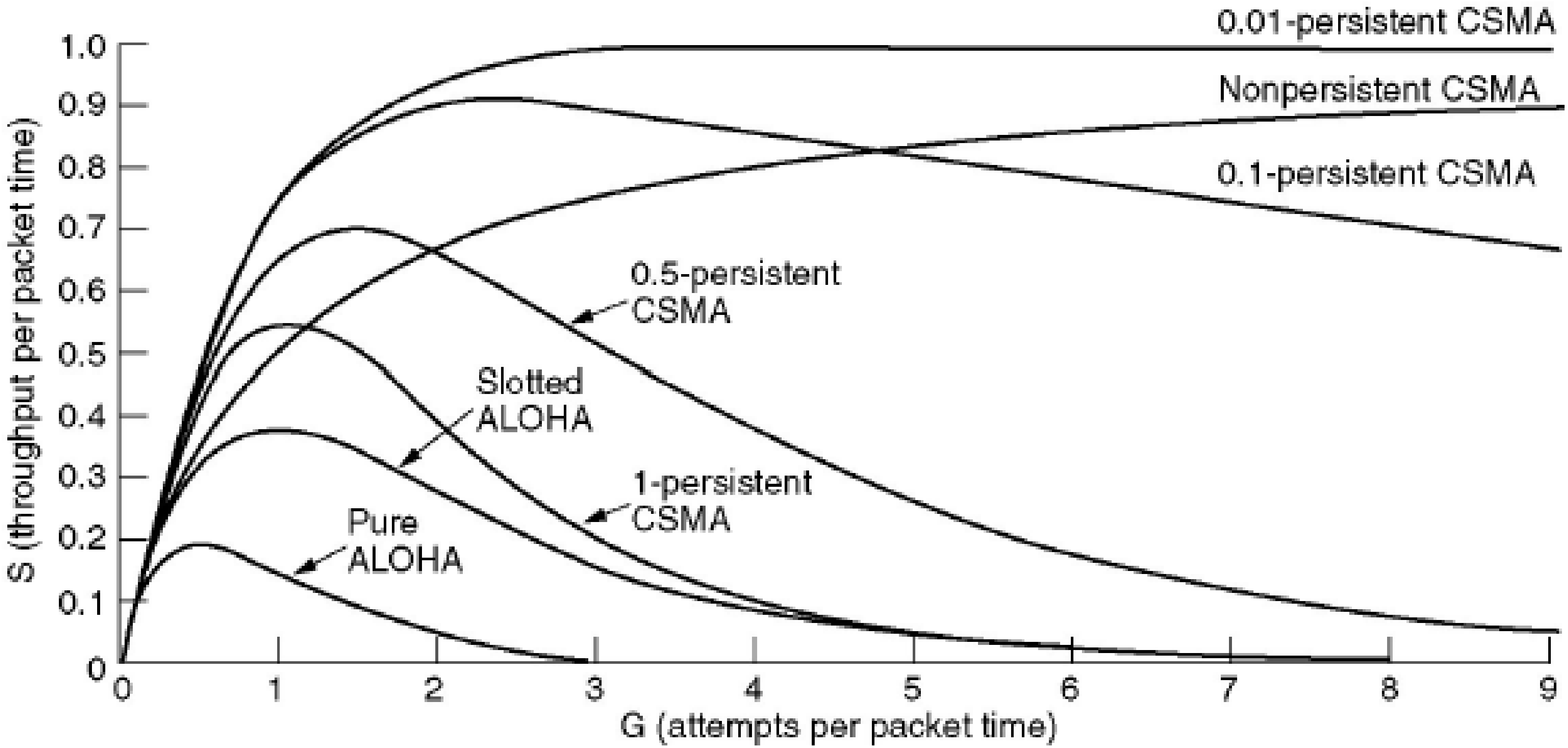
- This solution is less aggressive than 1-persistent CSMA

P-persistent CSMA

- Slot based system
- Before transmitting, each node listens to the channel
  - if the channel is free, than it transmits with probability *p* at the beginning of the next slots
  - otherwise (probability *1-p*) waits for a random time and then tries again the procedure

- The aggressiveness of this protocol depends on the parameter *p*

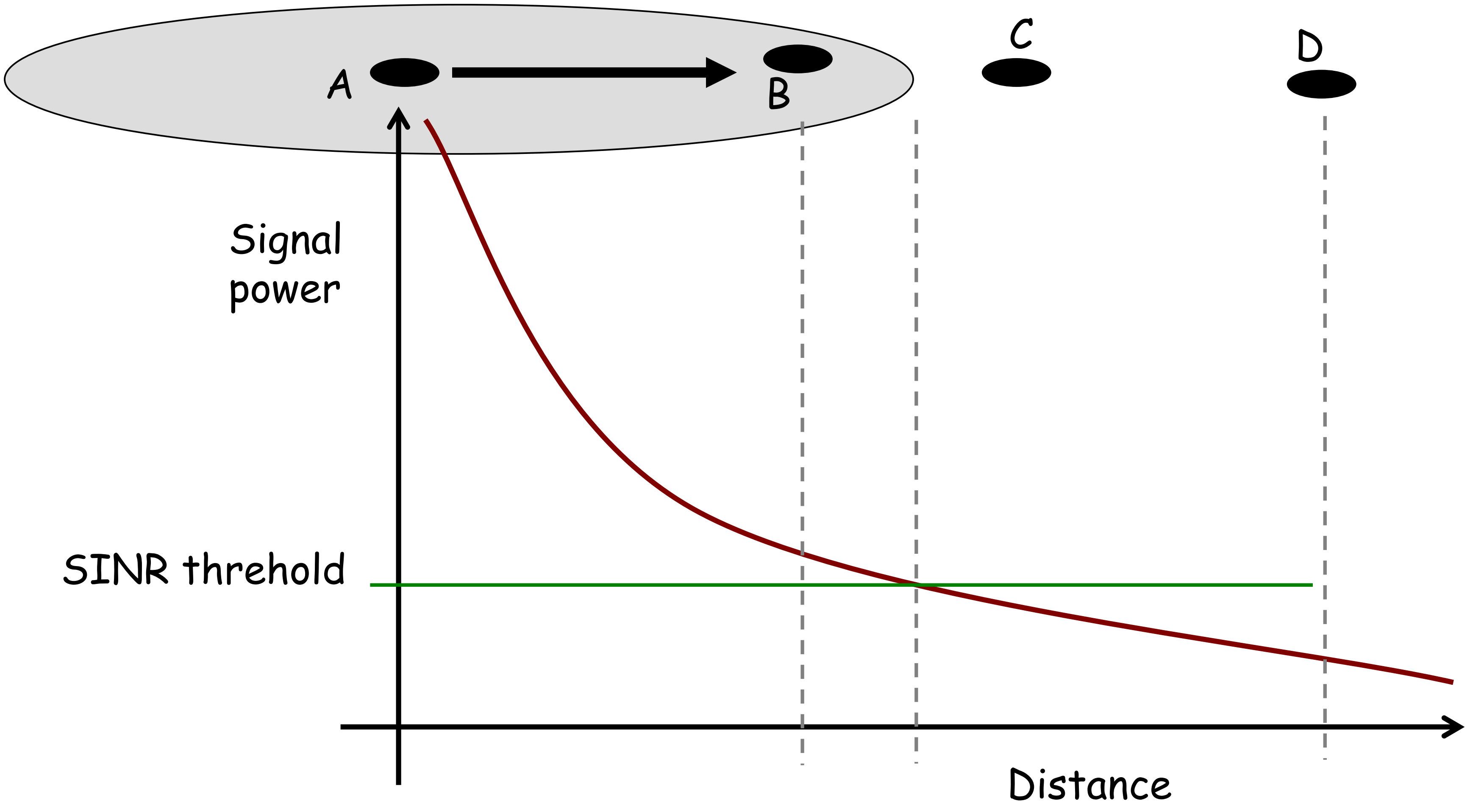
CSMA Protocols: Comparison



Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

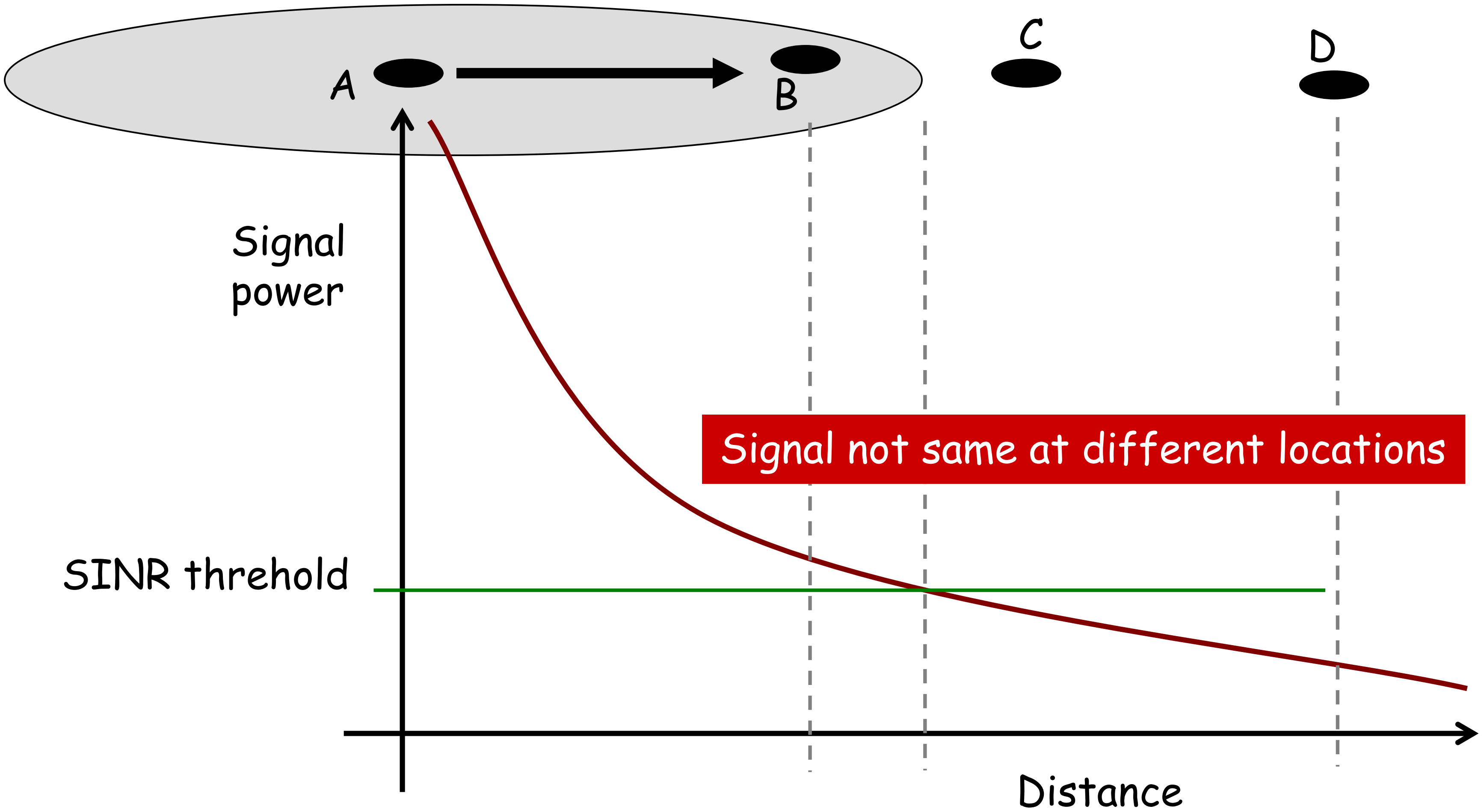
- CSMA/CD: carrier sensing and deferral like in CSMA. But, collisions are detected within a few bit times.
- Transmission is then aborted, reducing the channel wastage considerably.
- Typically, persistent transmission is implemented
- CSMA/CD can approach channel utilization =1 in LANs (low ratio of propagation over packet transmission time)
- Collision detection is easy in wired LANs (eg, E-net): can measure signal strength on the line, or code violations, or compare tx and receive signals
- Collision detection cannot be done in wireless LANs (the receiver is shut off while transmitting, to avoid damaging it with excess power)

Wireless Medium Access Control

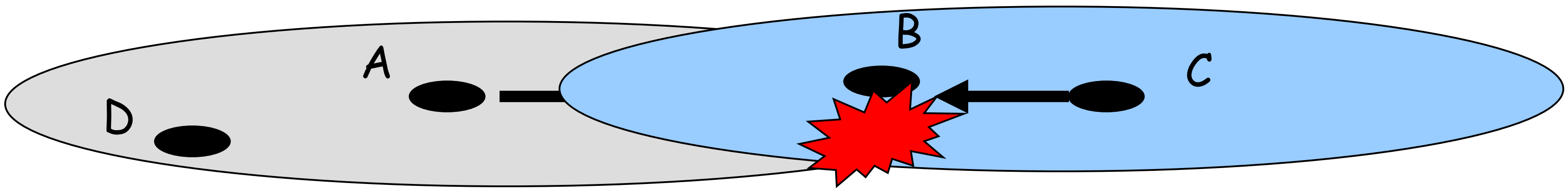


Wireless Media Disperse Energy

A cannot send and listen in parallel

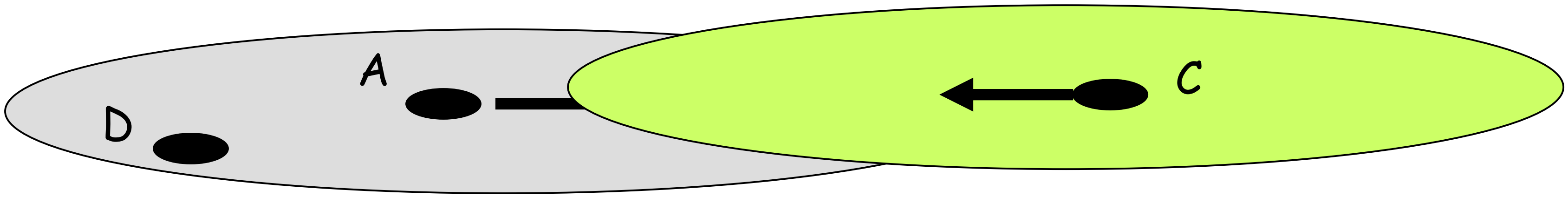


Collision Detection Difficult



- Signal reception based on SINR (signal-to-interference-plus-noise ratio)
  - Transmitter can only hear itself
  - Cannot determine signal quality at receiver

Calculating SINR

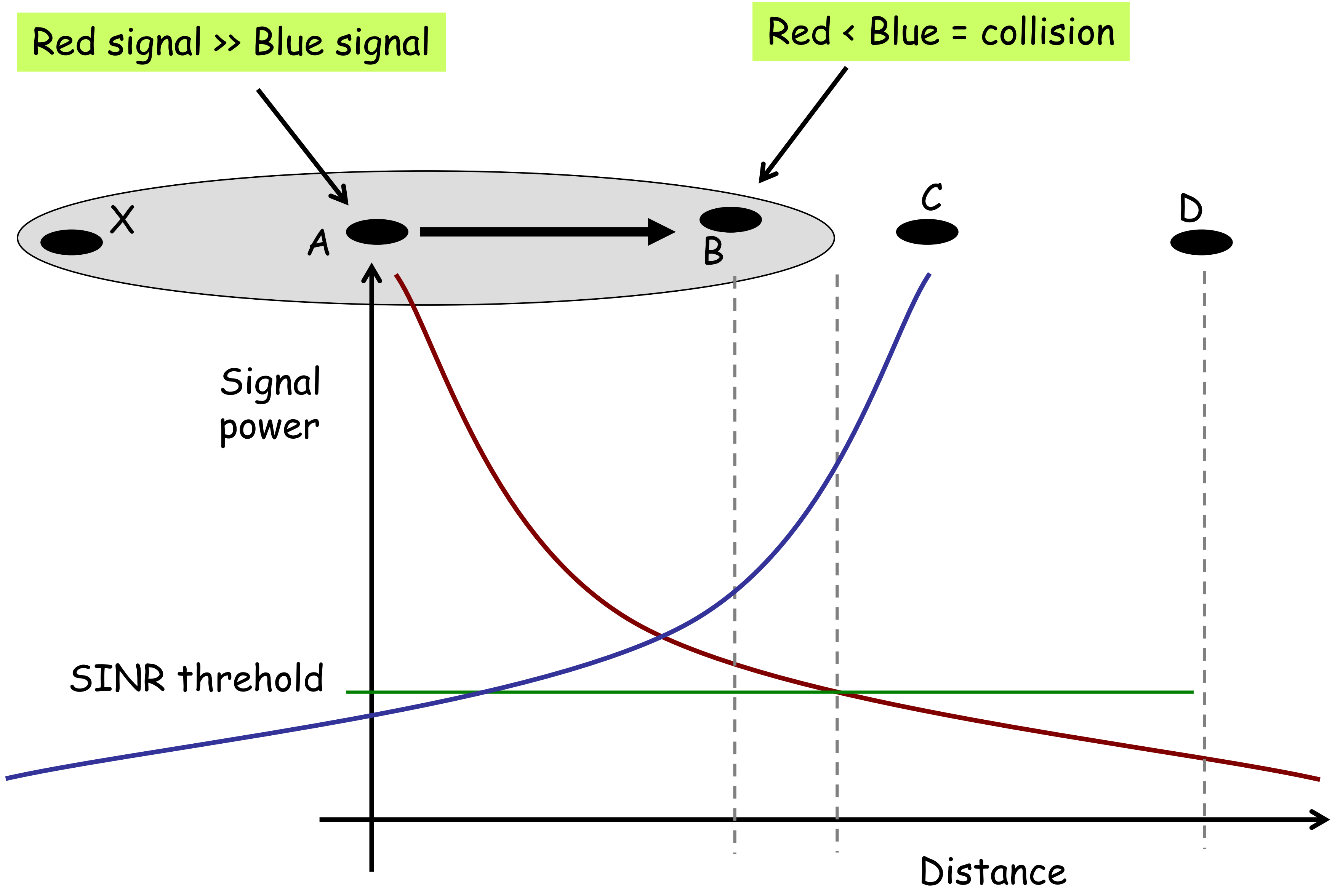


$$SINR = \frac{SignalOfInterest(SoI)}{Interference(I) + Noise(N)}$$

$$SoI_B^A = \frac{P_{transmit}^A}{d_{AB}^{\alpha}}$$

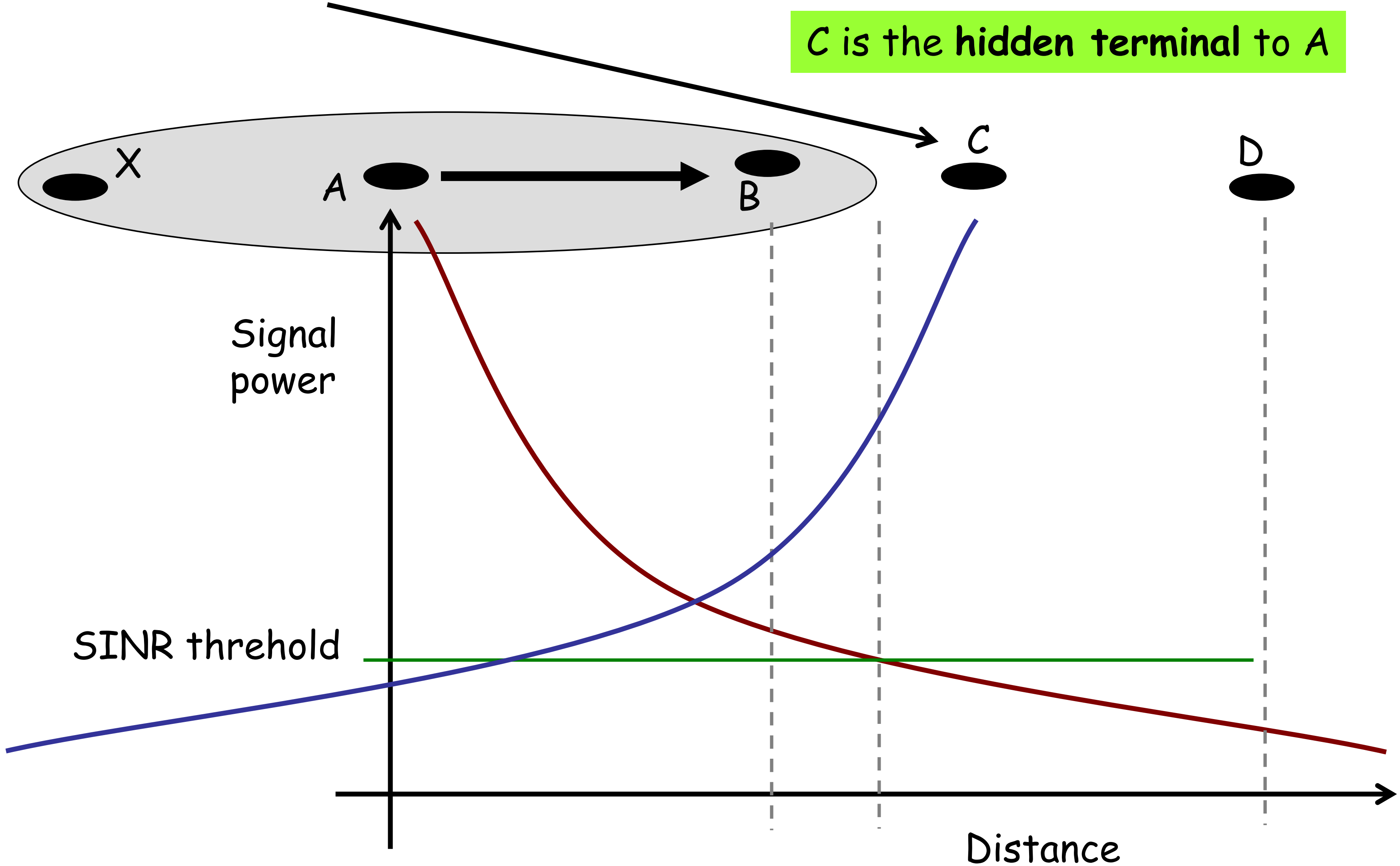
$$I_B^C = \frac{P_{transmit}^C}{d_{CB}^{\alpha}}$$

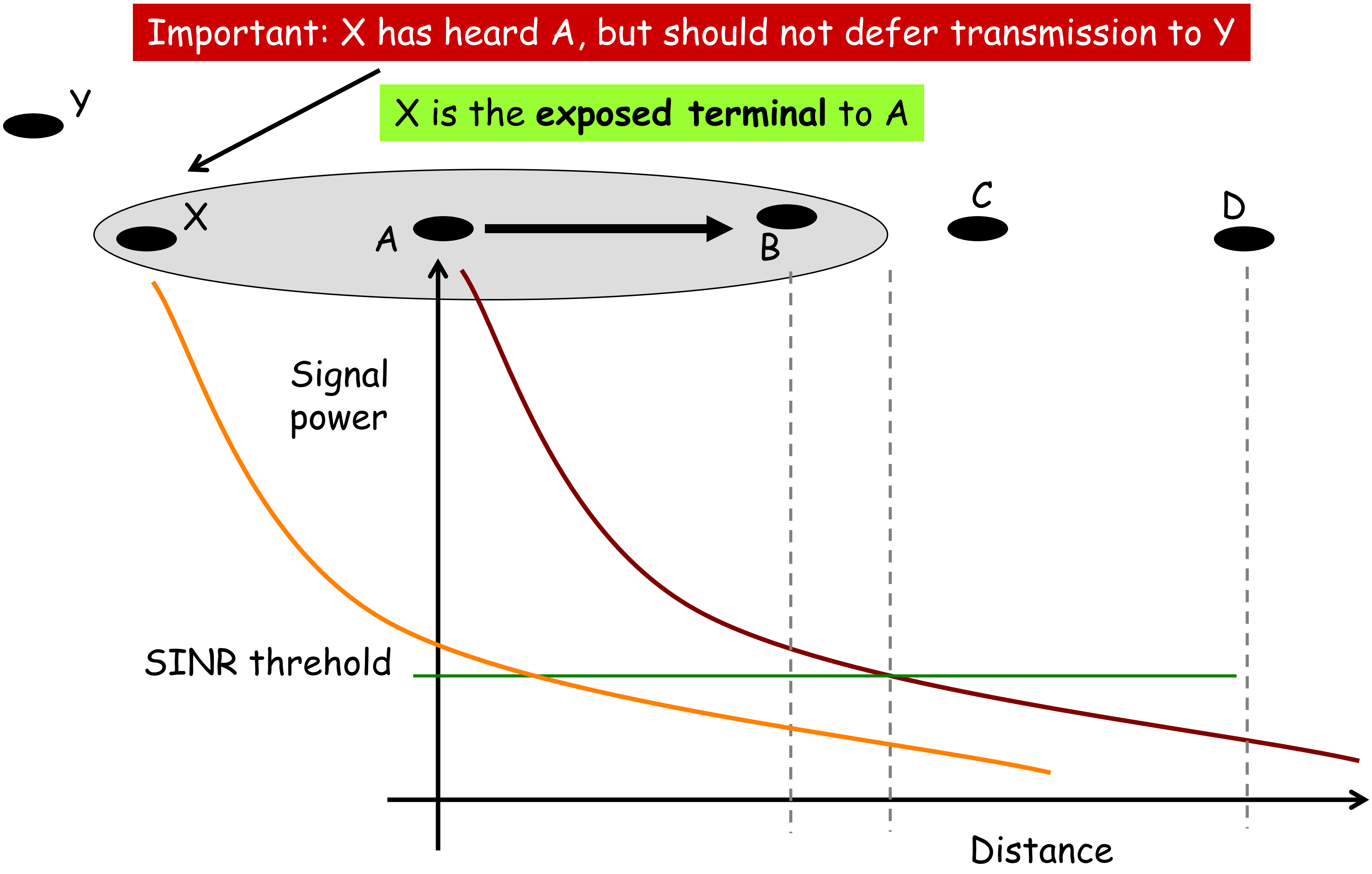
$$\rightarrow \quad SINR_B^A = \frac{\dfrac{P_{transmit}^A}{d_{AB}^{\alpha}}}{N + \dfrac{P_{transmit}^C}{d_{CB}^{\alpha}}}$$


Red signal >> Blue signal
Red < Blue = collision
X
A
B
C
D
Signal power
SINR threhold
Distance

Important: C has not heard A, but can interfere at receiver B

C is the **hidden terminal** to A

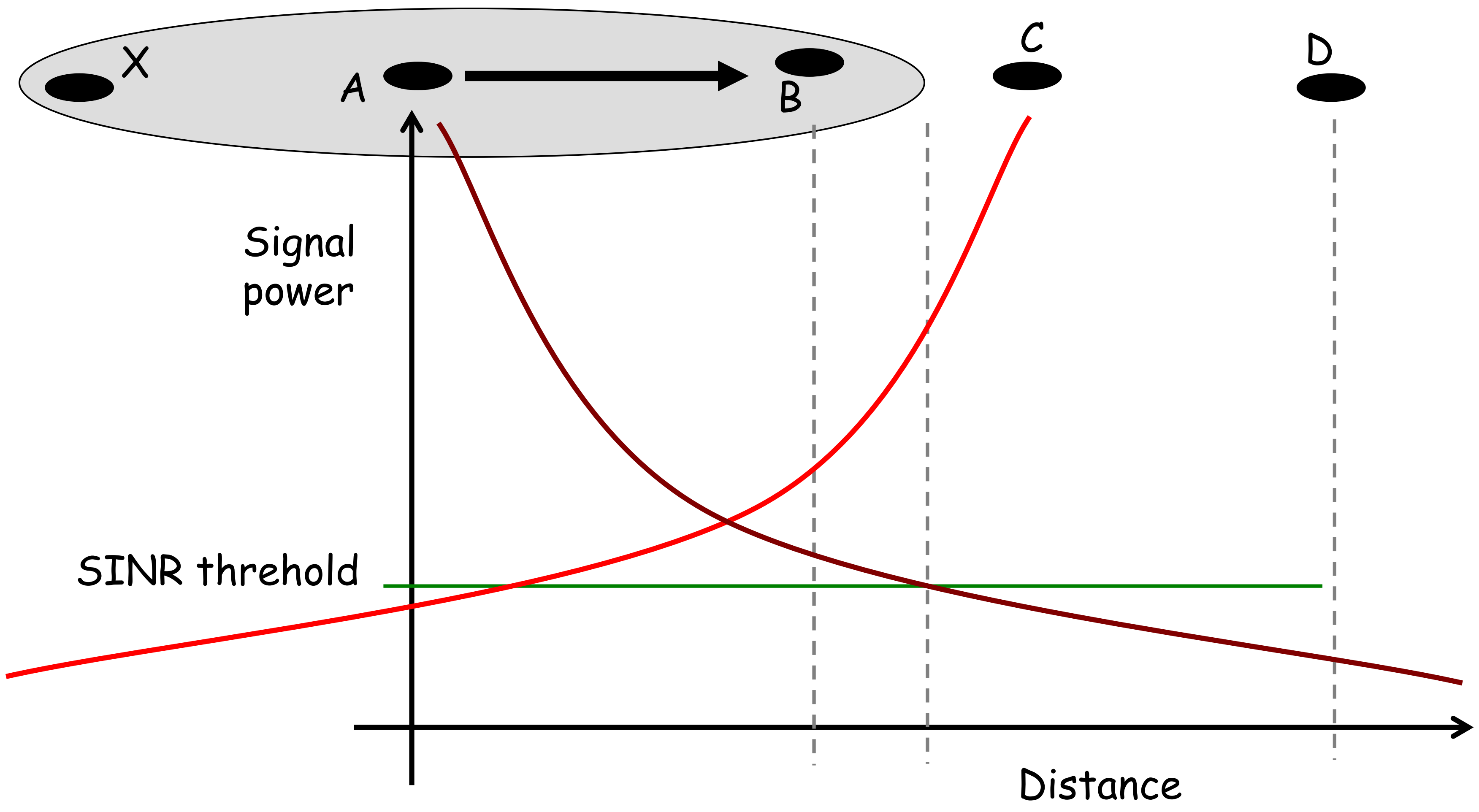




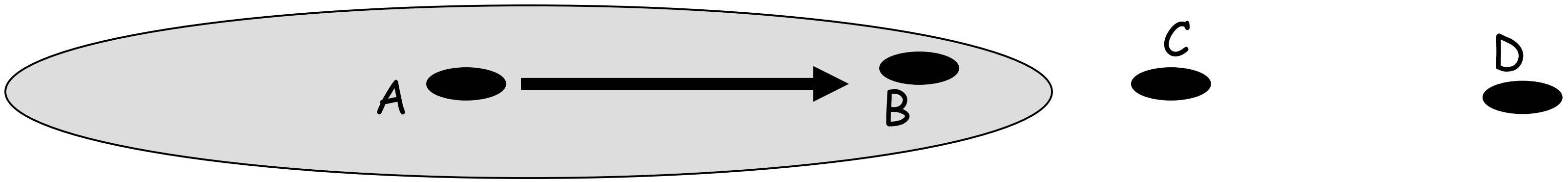
Important: X has heard A, but should not defer transmission to Y
X is the **exposed terminal** to A
Y
X
A
B
C
D
Signal power
SINR threhold
Distance

So, how do we cope with Hidden/Exposed Terminals?

How to prevent C from transmitting?



A Project Idea

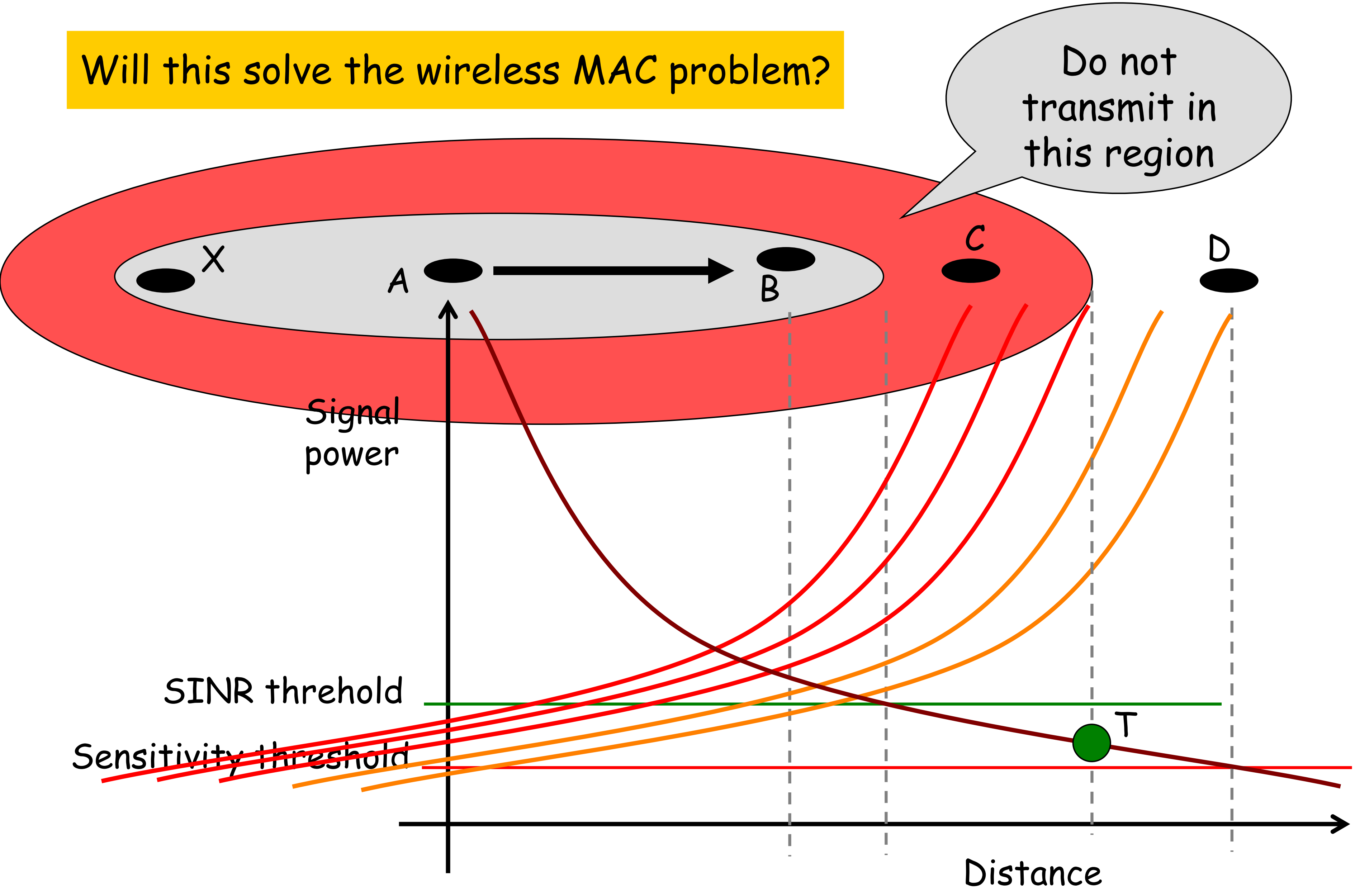


- A node decides to intelligently choose a
  Carrier sensing threshold (T)

- The node senses channel
  - If signal > T, then node does not transmit
  - If signal < T, then transmit

- Possible to guarantee no collisions?

Will this solve the wireless MAC problem?



To be continued…

(in next set of slides)