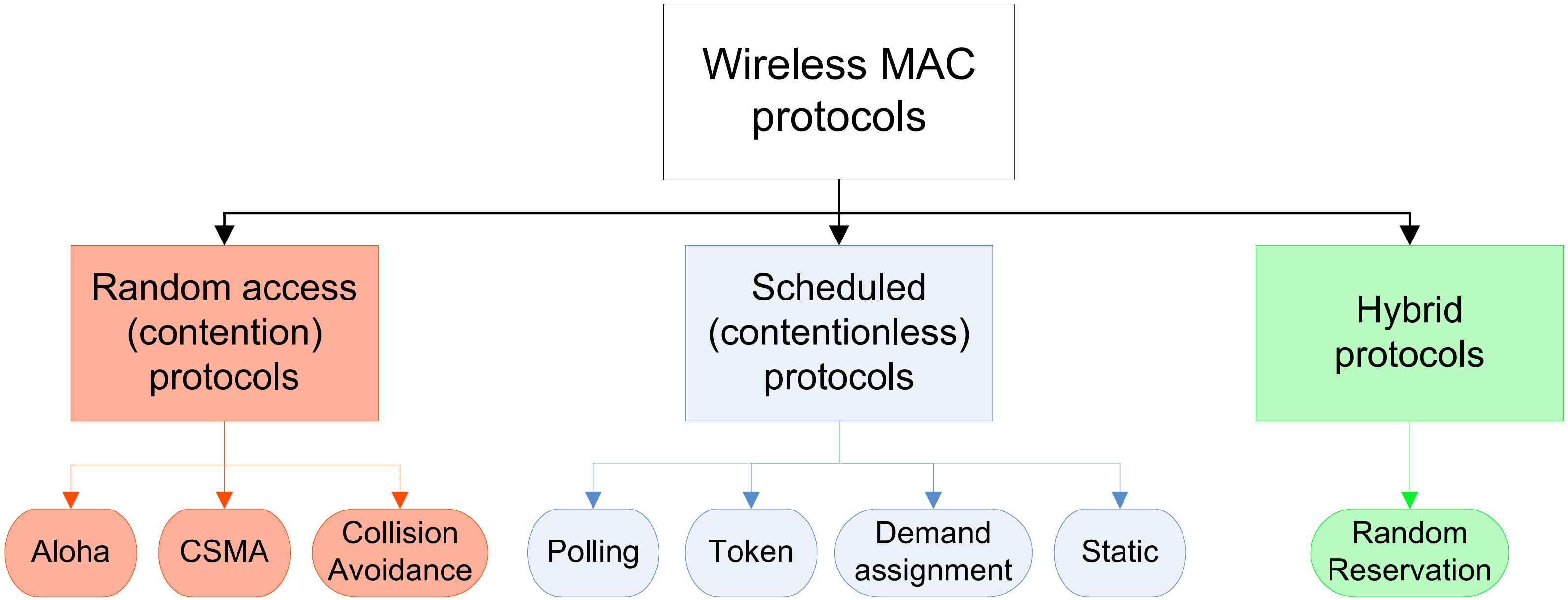
Wireless
Medium Access Control
Protocols

Telecomunicazioni
Undergraduate course in Electrical Engineering
University of Rome La Sapienza
Rome, Italy
2007-2008

Classification of wireless MAC protocols



- The above classification is based on how DATA traffic is transferred
- Most scheduled protocols, in fact, foresee a random access phase in which control packets are subject to collision

Random Access Protocols (1/2)

- In random access protocols each packet is subject to collision, since no resource reservation is adopted
- The main advantage of this family of protocols is simplicity:
  - Each terminal can transmit with no (or limited) information regarding other terminals
  - Random access protocols provide low delays, since packets are transmitted (almost) immediately
- The main drawback is the low scalability with traffic load:
  - When the offered traffic increases, the probability of collision increases as well, and the number of lost packets increases
  - This reduces the throughput (roughly: the amount of data successfully transferred) and increases the delay, since lost packets must be eventually retransmitted
- In order to reduce the negative effect of collisions, Collision Avoidance mechanisms are often adopted

Random Access Protocols (2/2)

- Collision Avoidance mechanisms can be divided in:

In-Band Collision Avoidance

- The Collision Avoidance procedure uses the same channel used for data transmission
- Typically based on a sequence of control packets exchanged between transmitter and receiver (hand-shaking)
- Examples:
  - MACA (Medium Access with Collision Avoidance)
  - 802.11 DFWMAC (Distributed Foundation Wireless MAC)

Out-of-Band Collision Avoidance

- The Collision Avoidance procedure uses a dedicated channel
- Typically based the assertion of sinusoidal tones (since the channel is dedicated, there is no need for organizing control information into packets)
- Example:
  - BTMA (Busy Tone Multiple Access)
  - DBTMA (Dual Busy Tone Multiple Access)

Scheduled Access Protocols

- Scheduled access protocols adopt mechanisms that avoid more than one terminal to transmit at a given time
- Data packets are never subject to collision, since at any time all terminals in the network are made aware of which terminal in the network is allowed to transmit
- These protocols are particularly suited for centralized network architectures, where a controller (Base Station, Access Point) manages the access, but are suitable as well for distributed network architectures in which the resource control and management is centralized (centralized network organization). Schemes which can be adopted include:
  - Polling: the controller "calls" one terminal at the time (see **Bluetooth**)
  - Demand Assignment: the controller grants the channel to terminals following a request, typically submitted in a random access phase
  - Static: A resource (e.g. time slot, carrier) is statically assigned to a terminal when it joins the network
- In distributed architectures, scheduled protocols can be adopted either by selecting a terminal which acts as a controller (see above) or by adopting a distributed scheduling strategy (token)

Random Access Protocols

- Three main classes of Random Access Protocols will be analyzed:
  - Aloha and Slotted Aloha
  - Carrier Sensing Multiple Access
  - Carrier Sensing Multiple Access with Collision Avoidance

ALOHA

- The simplest random access protocol is ALOHA
- Developed in 1970 at University of Hawaii
- ALOHA does not require any action by terminals before they transmit a packet
- A checksum is added at the end of each packet
- The receiving terminal uses the checksum to evaluate if the packet was received correctly or was corrupted by collision
- In case of collision the packet is discarded
- Retransmission of discarded packets is accomplished based on an Automatic Repeat on ReQuest (ARQ) protocol, that re-schedules packets after a random delay

Evaluation of Aloha throughput (1/4)

- The evaluation of the throughput S (i.e. the number of successful packet transmissions in a time unit) in Aloha can be easily performed under the following hypotheses:
  - ***Poisson arrivals***: packets arrive for transmission in each of the m nodes according to independent Poisson processes. The arrival rate in each node is λ / m, so that the overall arrival rate is λ
  - ***Collision or perfect reception***: whenever two or more packets are transmitted at the same time, all packets are lost and must be retransmitted. If only one packet is transmitted, reception is correct
  - ***Immediate feedback***: a node is always informed of the result of previous transmissions (no packets transmitted, 1 packet transmitted, collision)
  - ***Infinite set of nodes***: The system has an infinite set of nodes ($m=\infty$) and each new packet arrives in a new node: this hypothesis is set in order to account for the case where new packets are generated in a node that is busy in retransmitting a packet, and would thus discard to serve the new generated packet.
  - ***Poisson retransmission***: we assume that also retransmissions happen following a Poisson process in each node, and arrival rate in each retransmitting node is x

Evaluation of Aloha throughput (2/4)

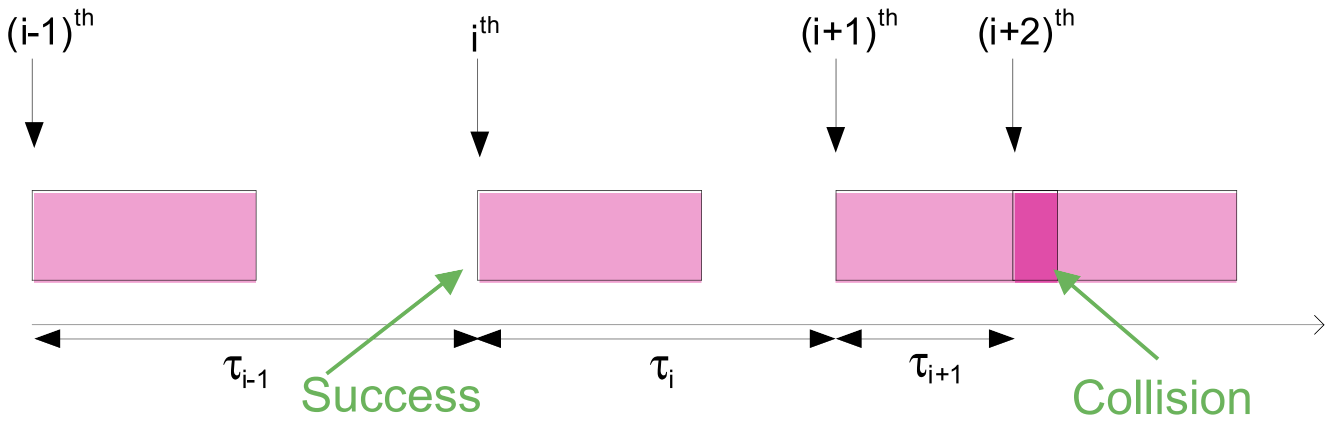
- Under the previous assumptions, it is easy to derive that the overall packet arrival rate in a time unit, if *n* nodes have a packet to be retransmitted, is:

$$G(n) = \lambda + nx$$

Cumulative arrival rate → $G(n)$

Number of terminals waiting for retransmission → n

- Let us assume that each packet has duration T. Packet transmission is successful with probability P_{succ} defined below
- Let us consider two subsequent transmission attempts by two different nodes, the i^{th} and the $(i+1)^{th}$. τ_i is the interval between the two attempts
- The i^{th} attempt is successful if both τ_i and τ_{i-1} are >T:



Evaluation of Aloha throughput (3/4)

- We obtain thus:

$$P_{succ} = Prob(\tau_i > T)Prob(\tau_{i-1} > T)$$

- Since the arrival process is a Poisson process with overall arrival rate G(n), one can write:

$$Prob(\tau_k \leq T) = 1 - e^{-G(n)T} \qquad \text{for any } k$$

- And thus one has:

$$Prob(\tau_i > T) = Prob(\tau_{i+1} > T) = e^{-G(n)T}$$

$$\Downarrow$$

$$P_{succ} = e^{-G(n)T} e^{-G(n)T} = e^{-2G(n)T}$$

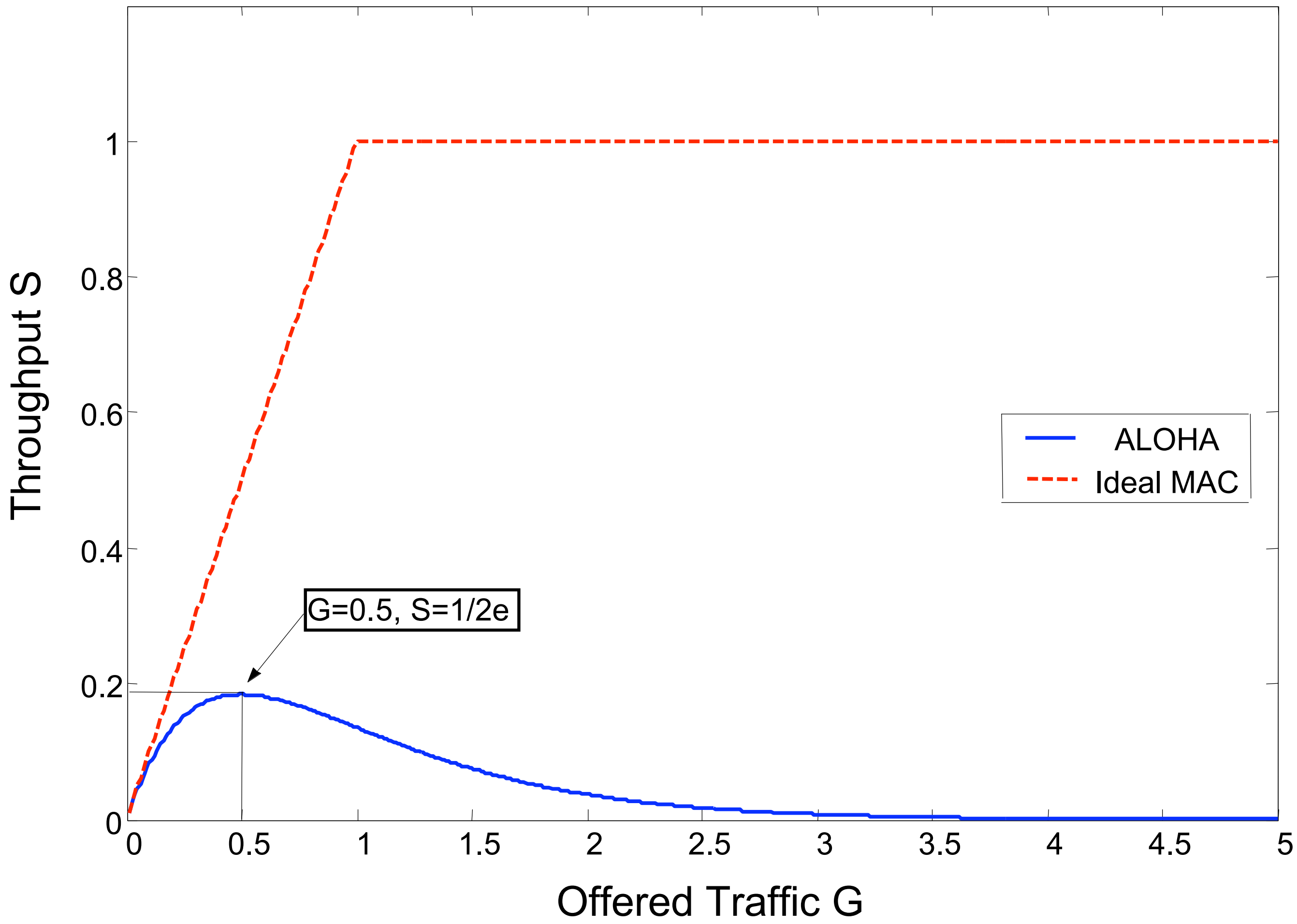
- Since throughput *S* is the percentage of packets that is successfully transmitted, one has :

$$S = G(n)TP_{succ} = G(n)Te^{-2G(n)T}$$

- And, if T is set to 1:

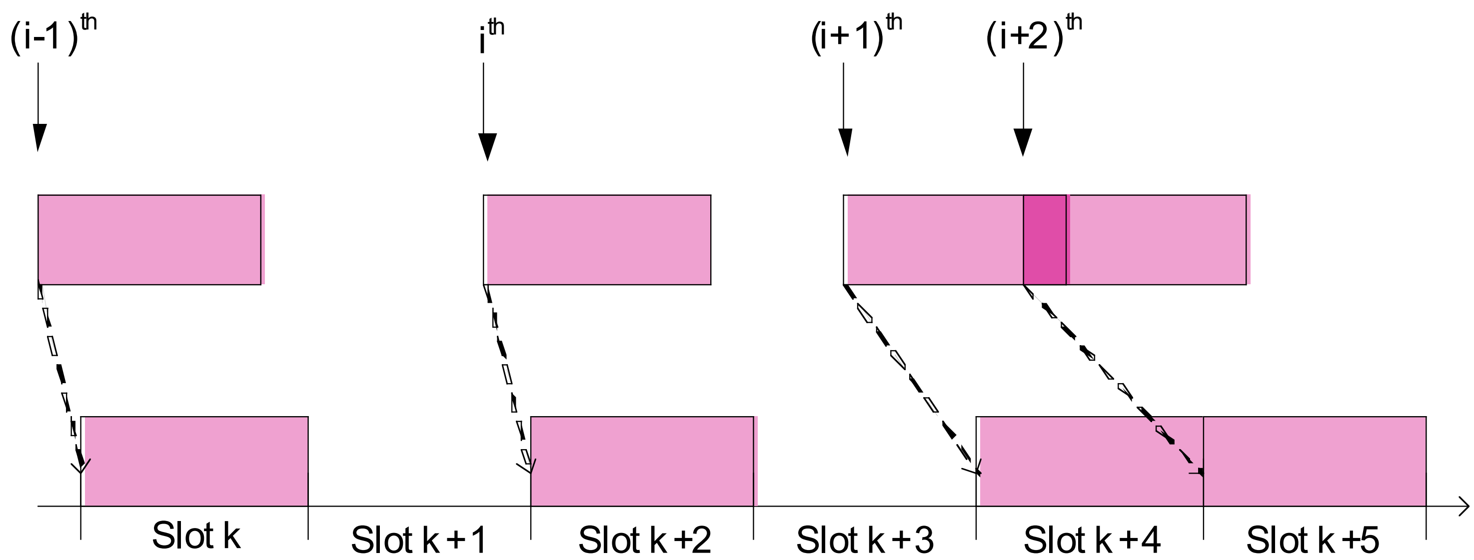
$$S = G(n)e^{-2G(n)}$$

Evaluation of Aloha throughput (4/4)



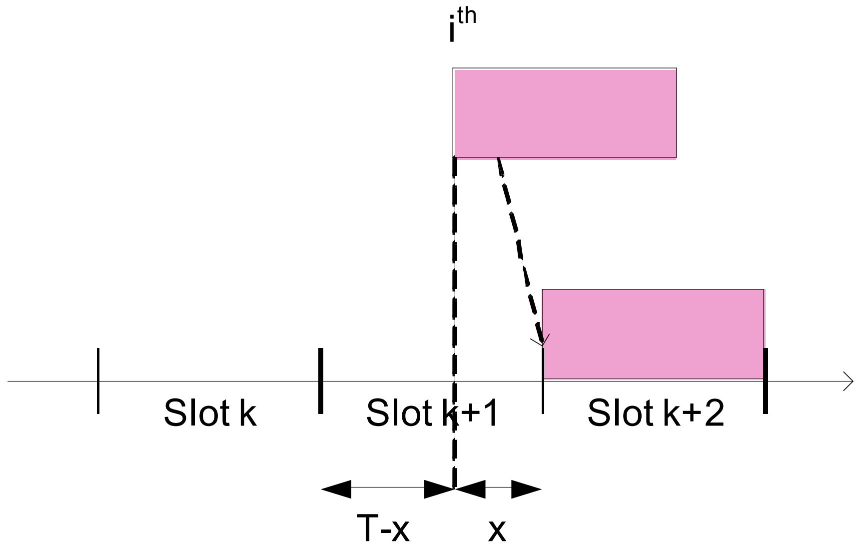
Slotted ALOHA (1/3)

- It was shown that ALOHA is suitable for networks characterized by a low offered traffic, i.e. with a low overall emission rate *G*
- The performance of the protocol can be improved by adding a slotted time axis, leading to the so-called Slotted ALOHA
- In slotted ALOHA, packets are not transmitted at any time, but only at the beginning of each time slot:



Slotted ALOHA (2/3)

- The probability of successful transmission can be evaluated as follows.



- The i^th transmission is successful if $\tau_{i-1} > T\text{-}x$ and $\tau_i > x$, leading to:

$$P_{succ} = Prob(\tau_{i-1} > T\text{-}x)\, Prob(\tau_i > x) = e^{-G(T-x)}\, e^{-Gx} = e^{-GT}$$

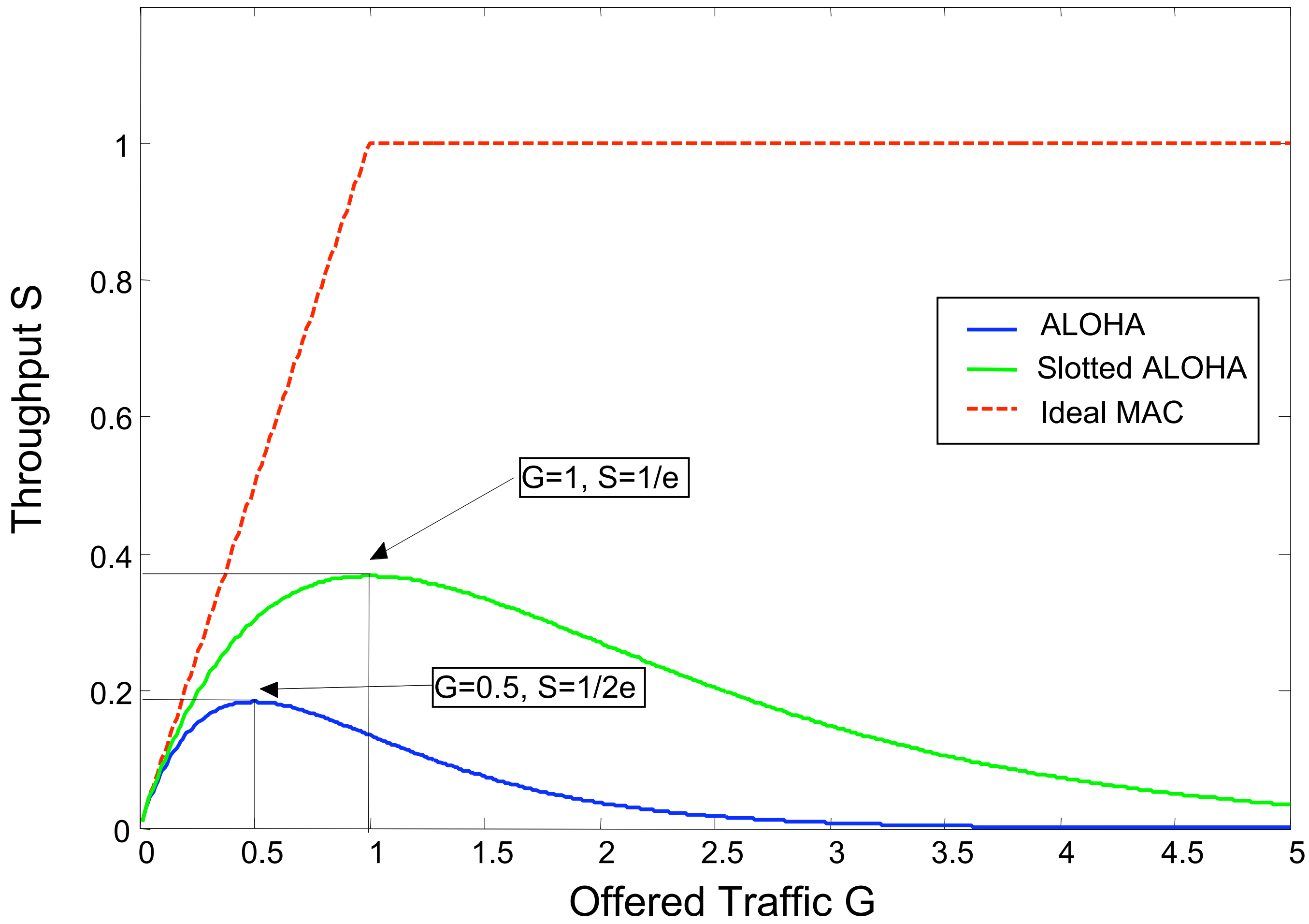
- As in the case of ALOHA, we can evaluate the throughput *S*:

$$S = GTP_{succ} = GTe^{-GT}$$

- And, for T=1:

$$S = Ge^{-G}$$

Slotted ALOHA (3/3)



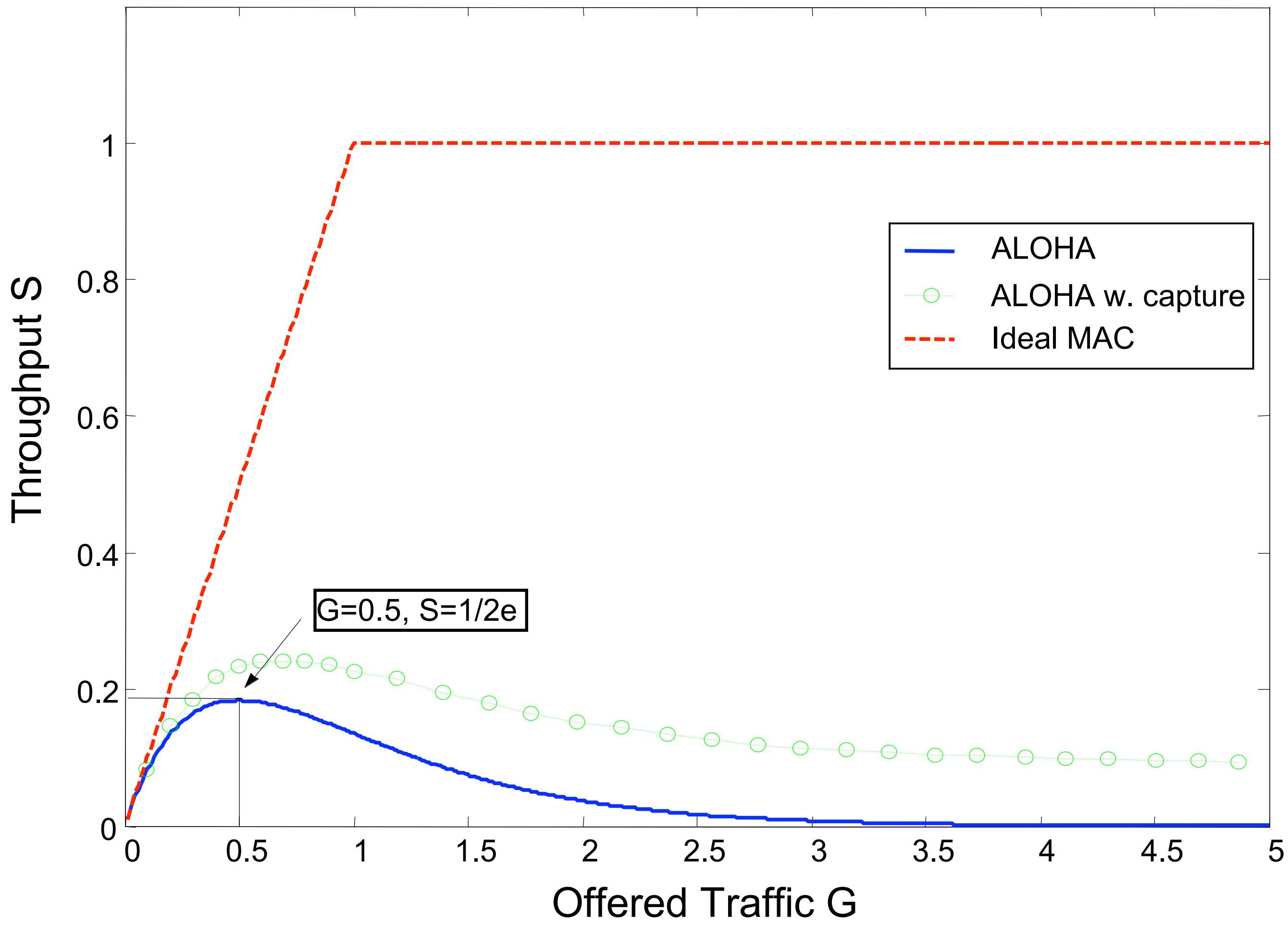
ALOHA in real world

- The analysis of throughput of ALOHA carried out in the previous slides relies on a set of simplistic hypotheses
- Not all hypotheses hold when ALOHA is applied to real networks: as a consequence, the actual behavior of the protocol can be different from what we know from the theory
- In particular, the ALOHA throughput was evaluated under the worst case hypothesis that **every** time a collision happens, all packets involved in the collision are lost
- The actual effect of a collision event will depend on the percentage of packets that overlap and on the average received powers at the receiver of interest
- In many cases, one or more packets involved in a collision are received correctly, thus increasing the throughput: such an event is the so-called capture

ALOHA- The capture effect

- Let us consider a simple scenario in which N packets, directed to N different receivers, collide in air
- The effect of collision is to introduce interference noise during the reception procedure
- Each receiver R_i (i=1,...,N) will experience a useful received power P_{Ri} (for the packet of interest) and an interference power I_{Ri} given by the N-1 interfering packets
- When the Signal to Interference Ratio (SIR) P/I is large enough, the receiver is still able to correctly receive the packet of interest (capture effect)
- The lower the value for P/I required for correct reception (SIR threshold) the higher the number of packets that are received in case of collision
- The capture effect may lead to a throughput significantly higher than the theoretical result

ALOHA throughput with capture

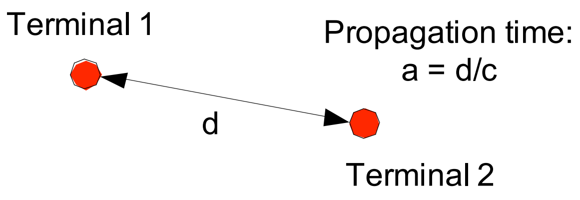


Carrier Sensing Multiple Access

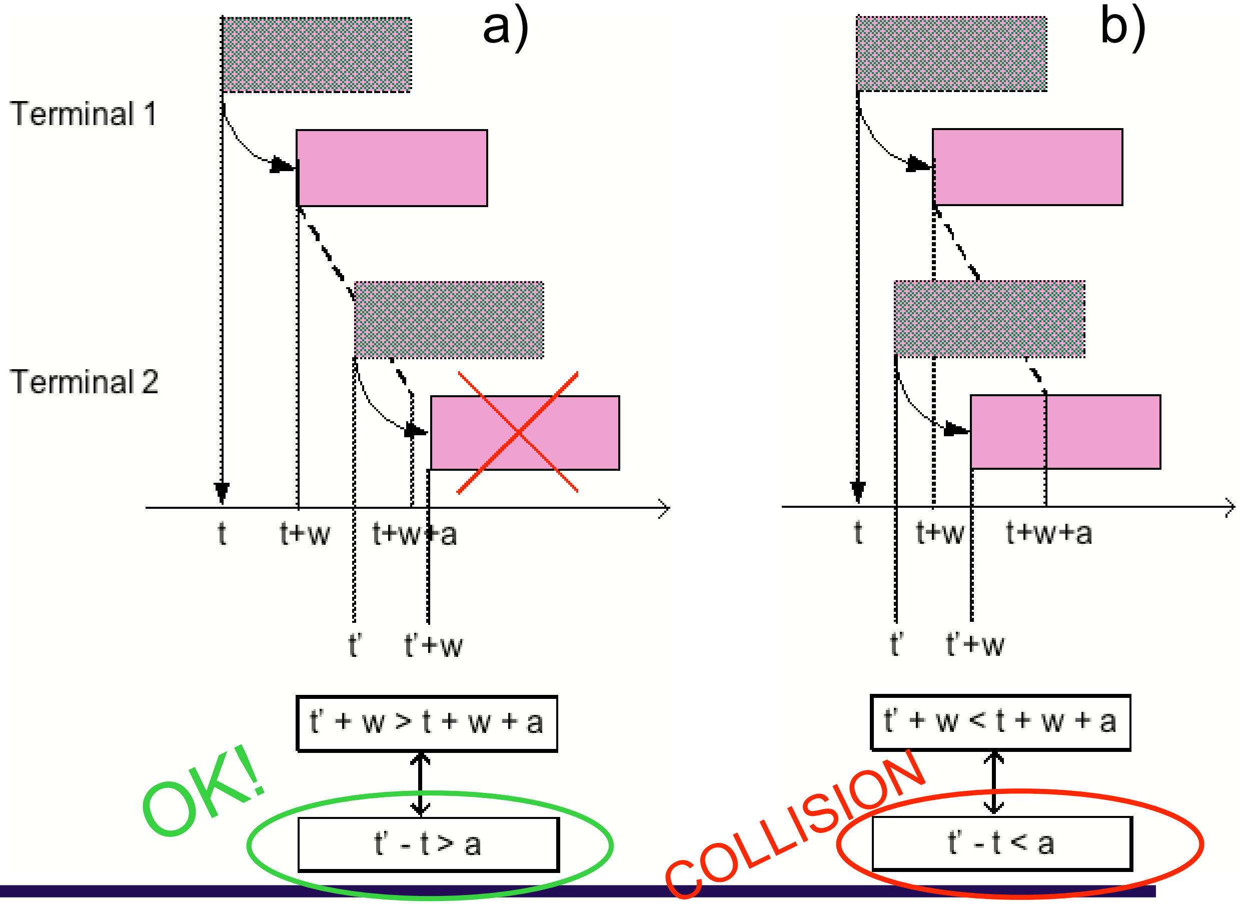
- In networks with high traffic load ALOHA is not effective due to collisions
- Performance can be increased by introducing Carrier Sensing, leading to *Carrier Sensing Multiple Access* (*CSMA*)
- When a terminal A has packets to transmit, it **senses** the channel before starting transmission
- If another terminal B is already transmitting, terminal A will detect its transmission
- In this case A will postpone its own transmission
- When A senses the channel as **idle** for a predefined amount of time, it assumes the channel as available and starts transmission.

Throughput of CSMA (1/3)

- Although terminals sense the channel for a time w before transmitting, collision can still occur because of the propagation time:



- Case a): the packet emitted by Terminal 1 propagates to Terminal 2 during its channel sensing phase: Terminal 2 defers transmission
- Case b): the packet emitted by Terminal 1 propagates to Terminal 2 after the channel sensing phase is concluded: transmissions collide



Throughput of CSMA (2/3)

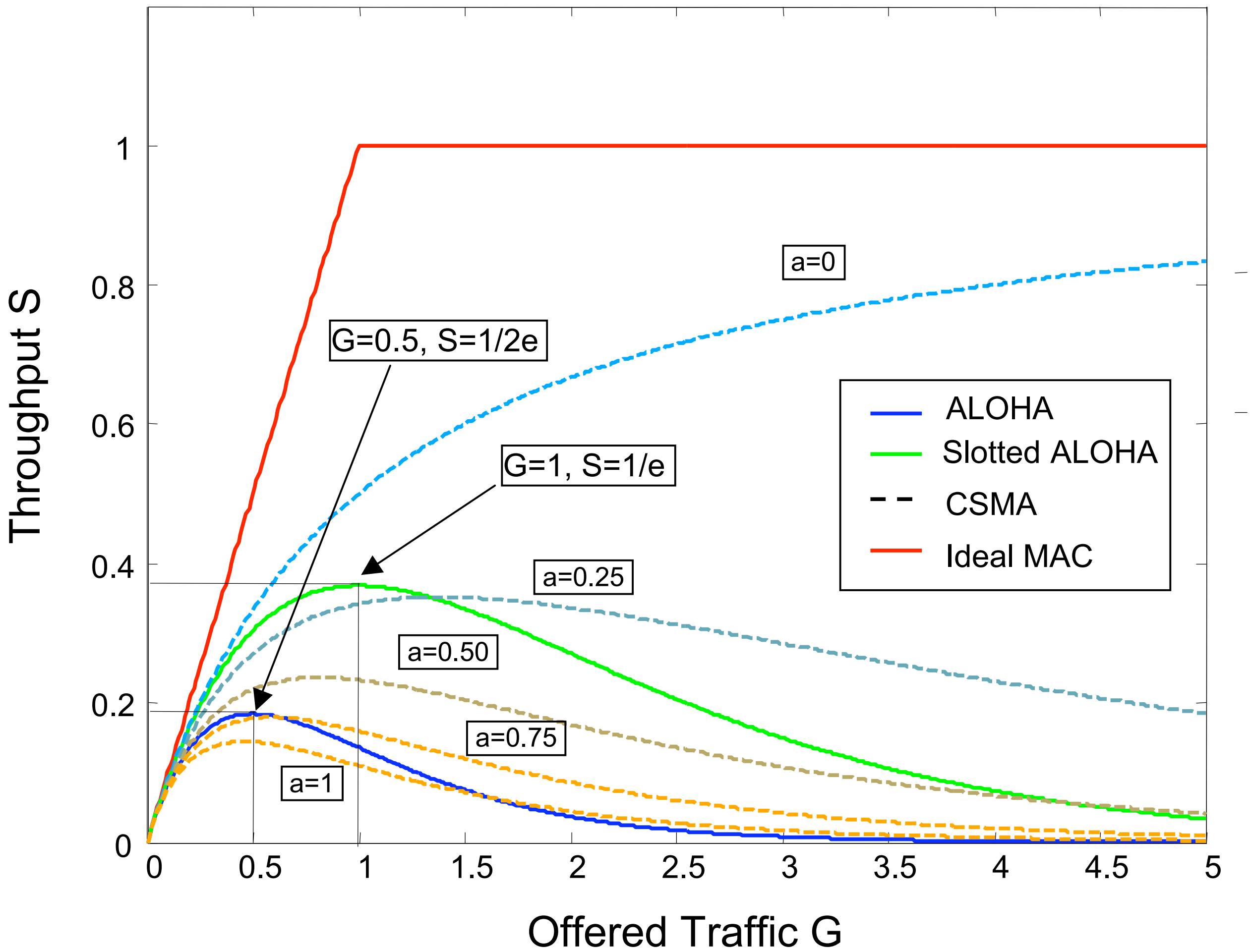
- We take the same assumptions introduced for calculating the ALOHA throughput:
  - *Poisson arrivals*
  - *Collision or perfect reception*
  - *Immediate feedback*
  - *Infinite set of nodes*
  - *Poisson retransmission*
- Furthermore, we have an additional hypothesis:
  - *Random (Poisson) rescheduling*: a packet transmission that is deferred due to busy channel is not scheduled **immediately** after the end of the busy channel period, but after a random time chosen following a Poisson process (this approach is defined **nonpersistent CSMA**)
- Under the above hypotheses, it can be shown* that the throughput is given by the relation:

$$S = \frac{Ge^{-aG}}{G(1+2a)+e^{-aG}}$$

- Note that since the propagation delay is different for every pair of terminals, throughput is evaluated with parameter **a** being set to the largest possible delay in the network (normalized by packet duration), leading to a lower bound for system performance

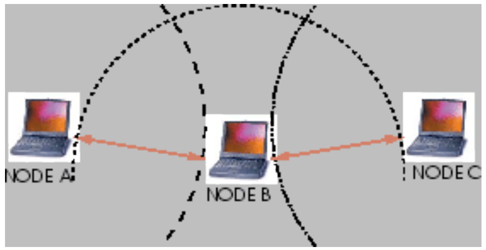
* Kleinrock, L. and F.A. Tobagi, "Packet Switching in Radio Channels: Part I–Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics," *IEEE Transaction on Communications*., Volume: 23, Issue: 12 December 1975), 1400–1416.

Throughput of CSMA (3/3)



CSMA Issues (1/4)

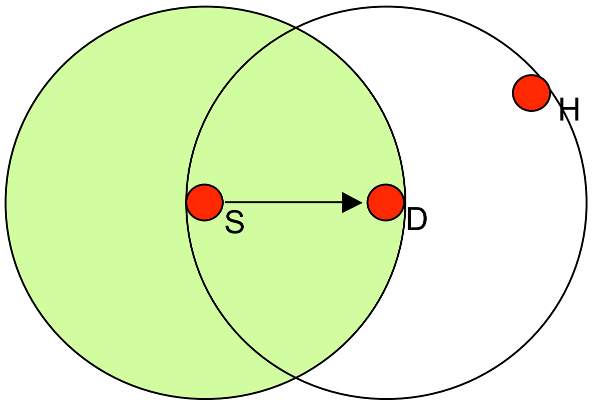
- The performance of CSMA heavily depends on the network scenario
- Wireless networks are in fact characterized by:
  1. Varying network topology
  2. Partial connectivity
     - This can lead to errors in protocols that work perfectly fine in wired networks



- In the case of CSMA, the wireless medium causes two phenomena that significantly reduce the protocol performance:
  - Hidden terminal
  - Exposed terminal

CSMA Issues (2/4)

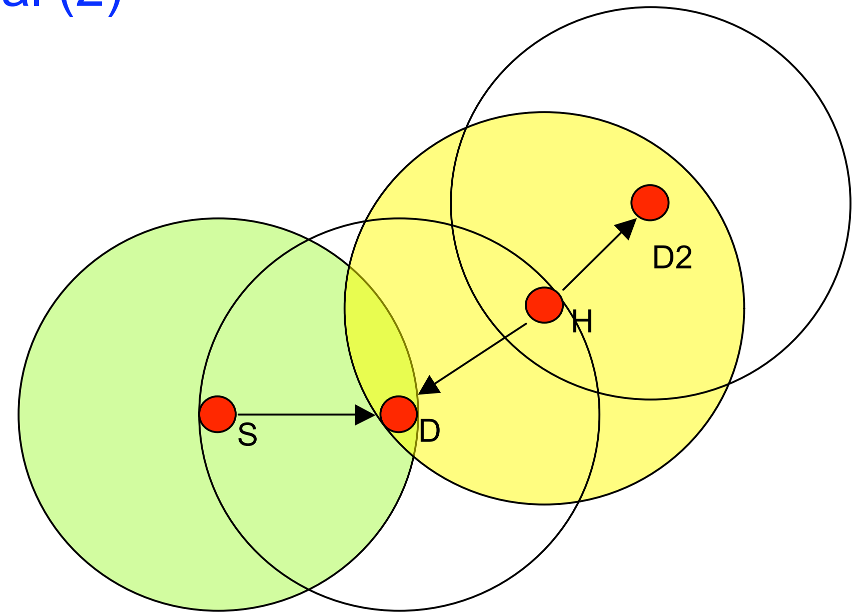
- Hidden terminal (1)



- Node S is sending a packet to D, which is acting only as receiver
- Node H, willing to transmit, starts the Carrier Sensing procedure, sensing the channel for the time period w defined in the protocol
- After a time w, H, which cannot detect the transmission by node S (due to limited radio coverage), assumes the medium is available

CSMA Issues (3/4)

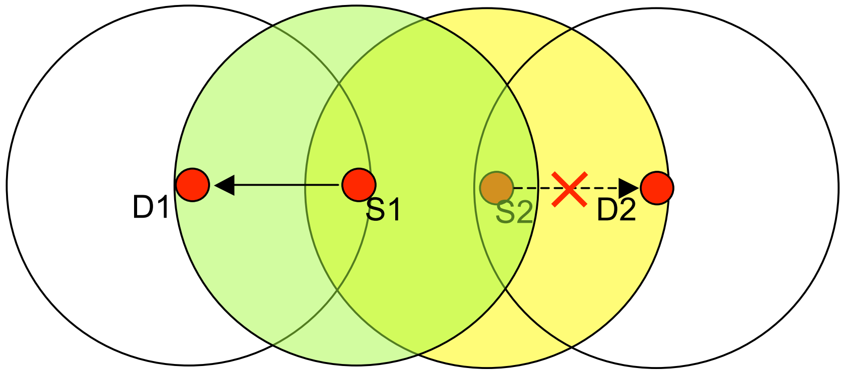
- Hidden terminal (2)



- H starts its transmission, causing a collision in D, and potentially the loss of both packets
- N.B.: Since wireless medium is inherently broadcast, this issue arises even if H is not willing to transmit to D, but to another terminal D2 in its range!

CSMA Issues (4/4)

- Exposed terminal



- In $t = 0$ terminal S1 starts a packet transmission to D1
- In $t = t_0$, S2 is willing to transmit a packet to D2
- S2 starts the Carrier Sensing procedure
- S2 detects a transmission already active, and assumes the channel is **busy**, postponing thus the transmission to D2
- Since D2 is not reached by S1, however, the transmission S2 -> D2 could be activated without causing any collision

Collision Avoidance

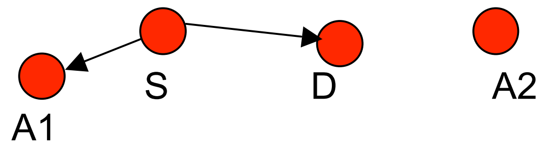
- Collision Avoidance (CA) mechanisms have been proposed in order to solve the hidden terminal problem.
- CA-based protocols can be divided in:
  - In-band CA protocols: the Collision Avoidance is performed on the same channel used for data traffic
    - Example: Medium Access with Collision Avoidance (MACA)
  - Out-of-Band CA protocols: the Collision Avoidance is performed on the dedicated channel, separated (usually in frequency) from the data channel
    - Example: Busy Tone Multiple Access (BTMA)

In-band CA: Medium Access with Collision Avoidance (MACA)

- MACA does not use Carrier Sensing, in the sense that terminals start transmitting a packet without spending any time sensing the channel
- In MACA when a terminal has a data packet to send, it does not transmit directly the data packet, but instead starts a Collision Avoidance procedure with the intended destination, based on three steps:
  1. Transmission of a Request-To-Send (RTS) packet from source to destination
  2. Transmission of a Clear-To-Send (CTS) packet from destination to source, in response to the CTS
  3. Transmission of the DATA packet from source to destination, after reception of the CTS
- The procedure is called handshaking

MACA: Request-To-Send

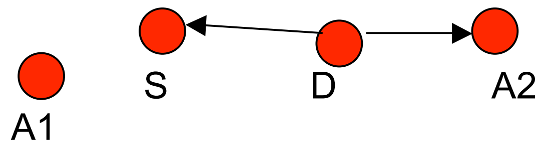
- The RTS is emitted by the source **S**, and is received by the destination **D** and by all other terminals within transmission range of **S** (terminal **A1** in figure)
- The RTS includes:
  - The ID of the source **S**
  - The ID of the destination **D**
  - The expected duration of the DATA packet to be transmitted



- The RTS has two goals:
  a. communicating to all terminals within range of **S** that a transmission is going to start
  b. trigger the destination **D** to emit a CTS message in reply to the RTS
- After the reception of the RTS, **A1** will expect to hear the CTS transmitted by **D** in reply to the RTS
- If A1 does not hear the CTS within a given time, it can start transmitting in any moment, since it is out of the range of **D**

MACA: Clear-To-Send

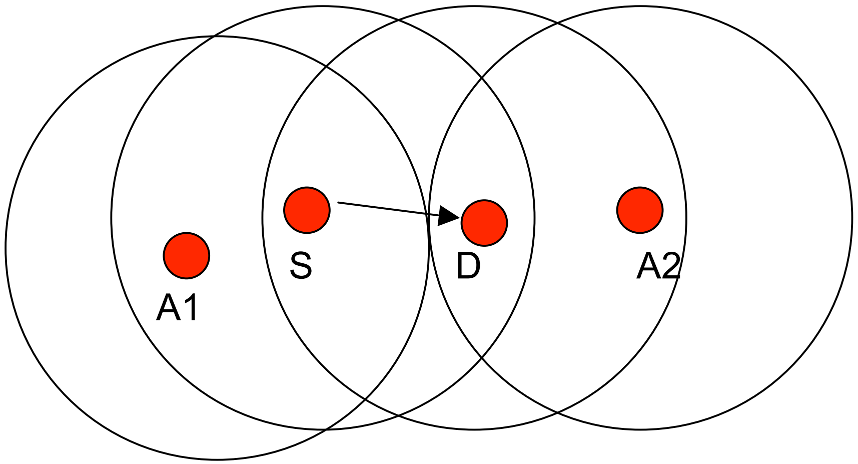
- The CTS is emitted by the destination **D**, and is received by the source **S** and by all other terminals within transmission range of **D** (terminal **A2** in figure)



- The CTS includes:
  - The IDs of **S** and **D**
  - The expected duration of the DATA packet to be transmitted
- The CTS has two goals:
  a. communicating to all terminals within range of **D** that a reception is going to start
  b. trigger the source **S** to emit the DATA packet
- Terminal **A2** will hear the CTS and will know that a transmission is going to start, even if it did not hear the CTS transmitted by **S**
- If **A2** has packets to send, it will thus postpone the transmission until the transmission S->D is over
- Since CS is not used, **A2** understands how long it will have to wait by reading the content of the CTS

MACA: Advantages

- The adoption of the RTS/CTS exchange relieves both the hidden and exposed terminal problems:
  - If CSMA was used with the same network topology presented in the previous slides, **A1** would be an exposed terminal, while **A2** would be an hidden terminal



- Note that collision is still possible between RTS packets, but the effect of such collisions is much lower of DATA collisions for two reasons:
  1. No DATA information is lost
  2. RTS packets are usually very short (20 Bytes) and thus a collision keeps the channel busy for a short time

CSMA with Collision Avoidance (CSMA-CA)

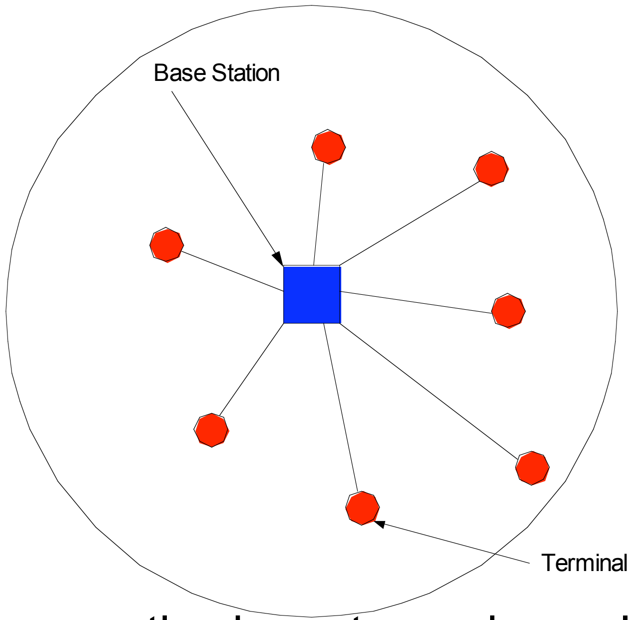
- Although MACA was proposed as an alternative to CSMA protocols, CSMA and In-band Collision Avoidance can be combined in order to get the advantages provided by MACA and reduce the probability of having collisions on the RTS packets (CSMA-CA)
- The CSMA-CA approach is adopted in the Distributed Foundation Wireless MAC (DFWMAC) adopted in the IEEE 802.11 standard (WiFi)
- In DFWMAC the handshaking is formed of four steps. The four steps are:

  1. RTS (Direction: S -> D)
  2. CTS (D -> S)
  3. Data (S -> D)
  4. Acknowledge (Ack) (D -> S)

- CSMA is adopted before transmitting the RTS packet

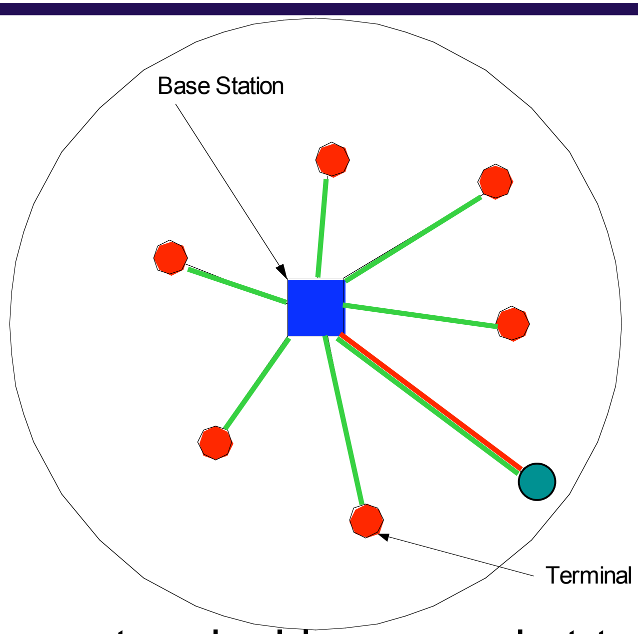
Out-of-Band CA: Busy Tone Multiple Access (BTMA)

- In BTMA the available bandwidth is split into two channels:
  - A message channel (used for DATA)
  - A busy-tone channel (used for Collision Avoidance)
- The BTMA was originally designed for a centralized network architecture, with a Base Station and a set of access terminals



- The Base Station uses the busy-tone channel to avoid collisions between access terminals

BTMA in the centralized architecture



Transmission on the busy-tone channel

Transmission on the message channel

- When a terminal has a packet to transmit to the Base Station, it senses the busy-tone channel for a time t_d
- If the busy-tone channel is idle, the terminal sends the packet on the message channel
- As soon as the Base Station detects that the message channel is busy, it emits a sinusoidal tone on the busy tone channel
- All access terminals will be inhibited from transmitting until the busy-tone channel will be released by the Base Station

BTMA in a distributed architecture

- In a centralized architecture BTMA is an effective way of avoiding collisions between DATA transmissions
- The adoption of BTMA in a distributed network architecture is attractive because it can address the hidden terminal problem
- In a distributed architecture, BTMA can be used as follows:
  - When a terminal **S** has a packet to transmit to the Base Station, it senses the **busy-tone** channel for a time t_d
  - If the busy-tone channel is idle, the terminal turns on the **busy-tone** signal and starts transmitting the packet on the **message** channel
  - Any other terminal that detects the **message** channel as busy turns on the **busy-tone** signal
  - In this way it is assured that when a terminal **S** is transmitting, all nodes within a two-hop range of **S** are inhibited from transmission
- This approach significantly reduces the probability of having hidden terminals in the network
- On the other hand, BTMA has a strong disadvantage: the amplification of the exposed terminal

BTMA and exposed terminals

- Example of the amplification of the exposed terminal problem