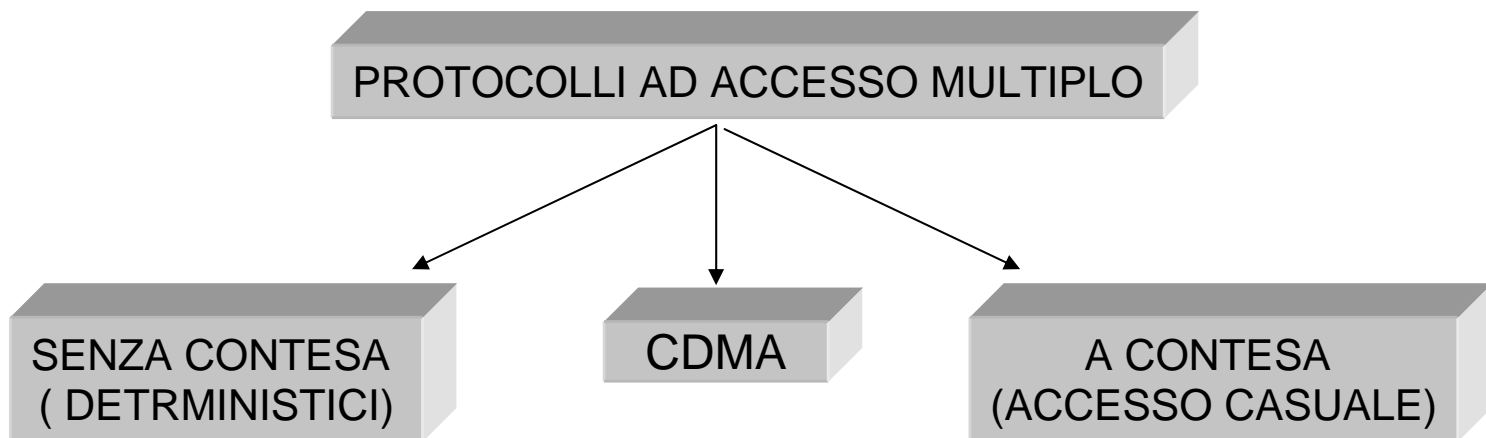


Classificazione delle tecniche di accesso multiplo

- Le tecniche di accesso multiplo si dividono in tre classi:
 - **Protocolli deterministici o senza contesa:** evitano la possibilità che due utenti accedano al canale contemporaneamente (collisione) programmando l'accesso di ogni utente.
 - **Protocolli ad accesso casuale o contesa:** si possono avere interferenze tra le stazioni. Le interferenze sono recuperate mediante opportune procedure.
 - **CDMA (Code Division Multiple Access):** le stazioni operano in continua sovrapposizione e interferenza, ma i segnali di ciascuna stazione possono essere recuperati grazie ad un opportuno codice.



Protocolli di accesso multiplo deterministici

- I principali protocolli di accesso multiplo di tipo deterministico sono:
 - Protocolli di accesso multiplo a divisione di frequenza (FDMA = Frequency Division Multiple Access): gli utenti utilizzano frequenze diverse per trasmettere.
 - Protocolli di accesso multiplo a divisione di tempo (TDMA = Time Division Multiple Access): gli utenti trasmettono in intervalli di tempo diversi.

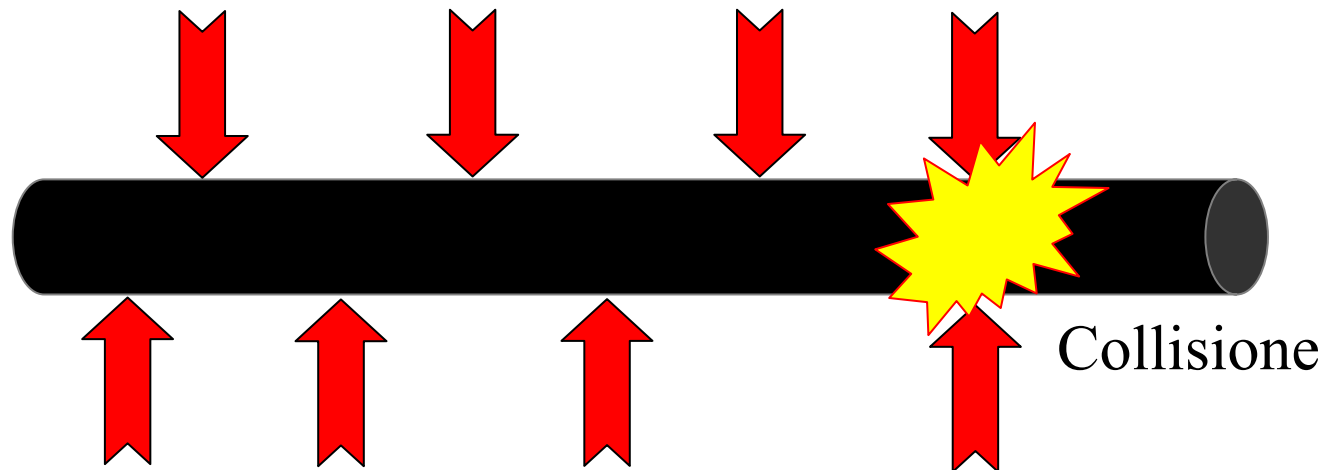
Protocolli di accesso multiplo casuali o a contesa

- Le tecniche di accesso multiplo a contesa, non prevedono nessuna gestione, centralizzata o distribuita, dell'accesso al canale da parte delle stazioni ad esso connesse.
- Nel caso più generale, quando una stazione ha dei dati da trasmettere accede immediatamente al canale senza preoccuparsi se questo è già occupato, rendendo così molto alta la probabilità di una collisione.
- Le tecniche di accesso random devono quindi essere in grado di risolvere le collisioni in modo da non portare il sistema ad una situazione di blocco.
- Le tecniche di accesso multiplo casuali più note sono:
 - ALOHA (Puro e slotted)
 - CSMA/CD (Carrier Sense Multiple Access / Collision Detection)

Protocolli di accesso multiplo

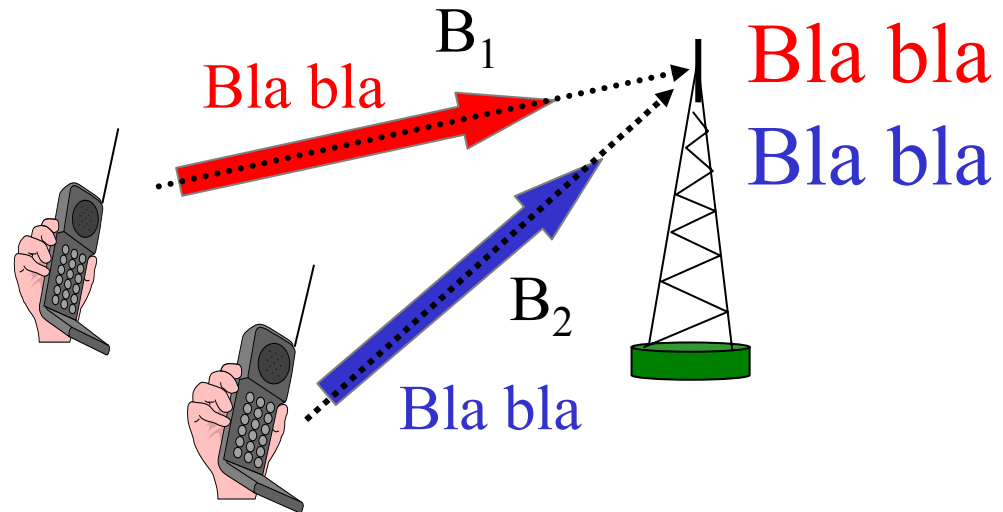
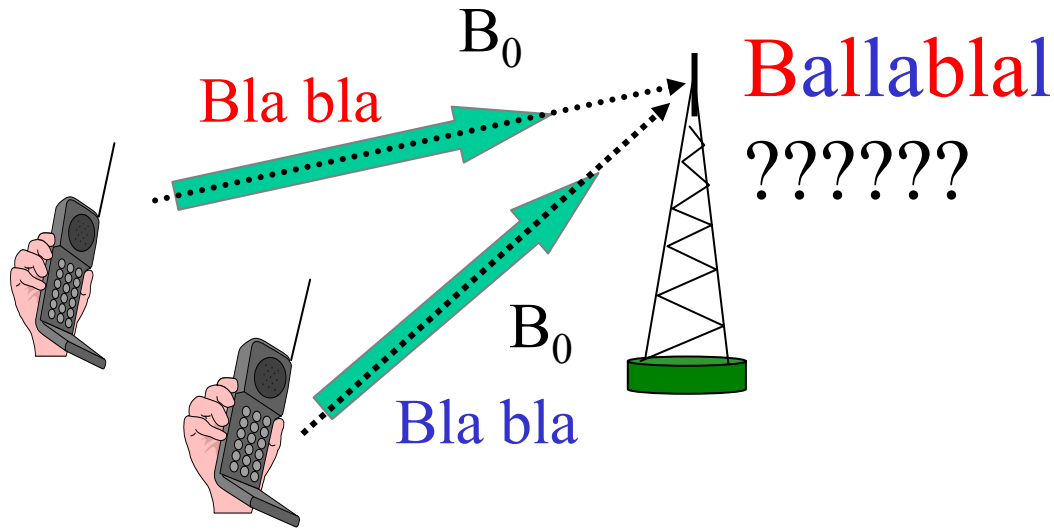
Quando l'accesso ad una risorsa può avvenire da parte di più utenti indipendenti, si parla di *risorsa condivisa* ed è necessaria l'implementazione di particolari protocolli di **accesso multiplo**. La necessità di condividere una risorsa può derivare dal costo o dalla scarsa disponibilità di quest'ultima ma anche dalla necessità di ottenere una connettività rappresentata da un mezzo di comunicazione comune.

In molte reti di telecomunicazione la risorsa condivisa è rappresentata dal **canale di comunicazione**

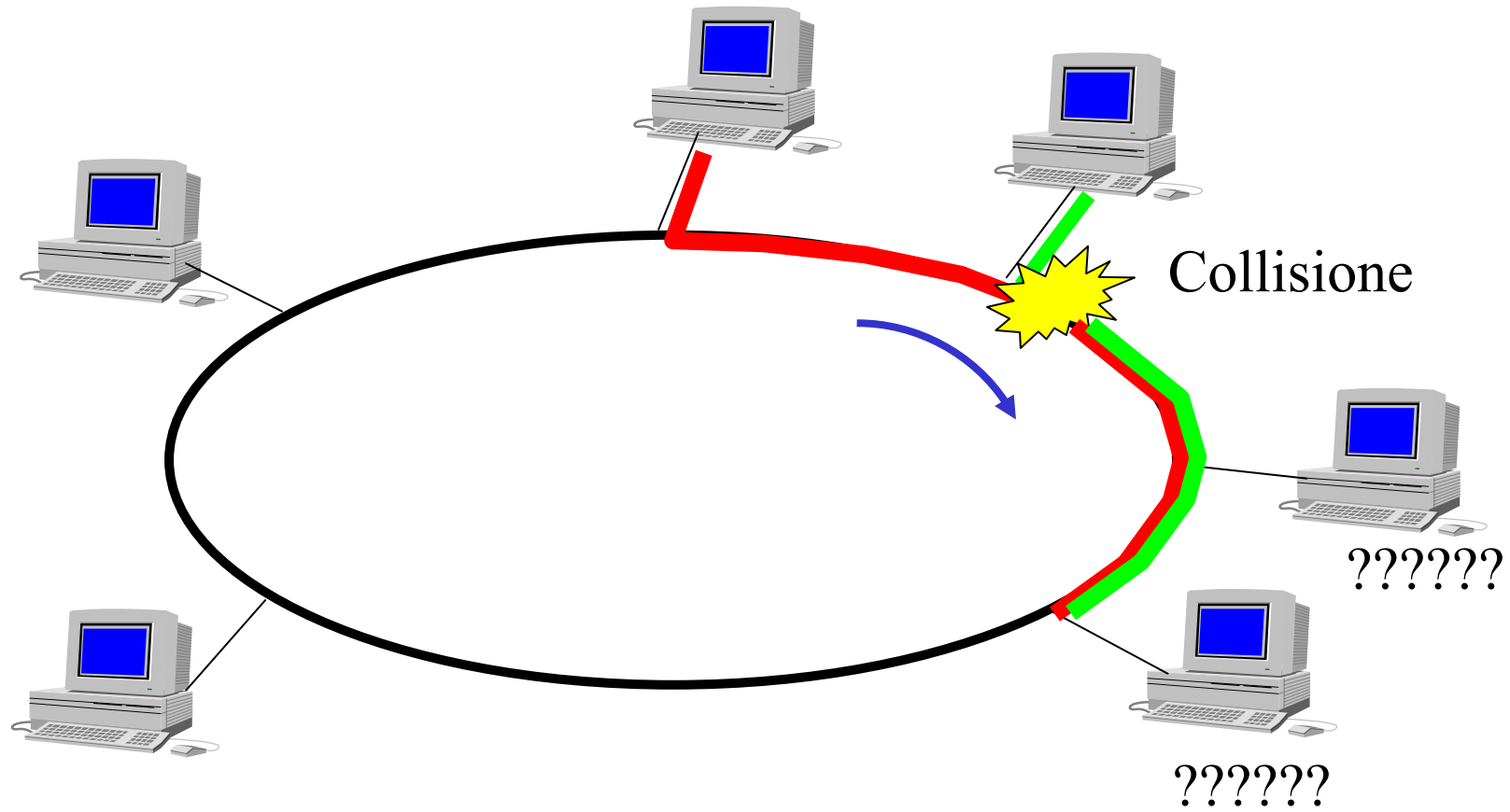


Esempi

Interferenza



Esempi



Metodi di accesso multiplo senza contesa

Accesso multiplo a divisione di tempo (TDMA: *Time Division Multiple Access*)

Nel protocollo TDMA, l'asse temporale è suddiviso in *frames* di durata fissata e a loro volta suddivisi in un numero fisso di intervalli più piccoli denominati *slots*. Ogni slot in una particolare posizione all'interno del frame è assegnato ad un utente. Ciascun utente, può quindi trasmettere per un periodo di tempo pari ad uno slot ad intervalli pari alla durata di un frame, in questo tempo, esso ha a disposizione tutta la banda del sistema.

Accesso multiplo a divisione di frequenza (FDMA: *Frequency Division Multiple Access*)

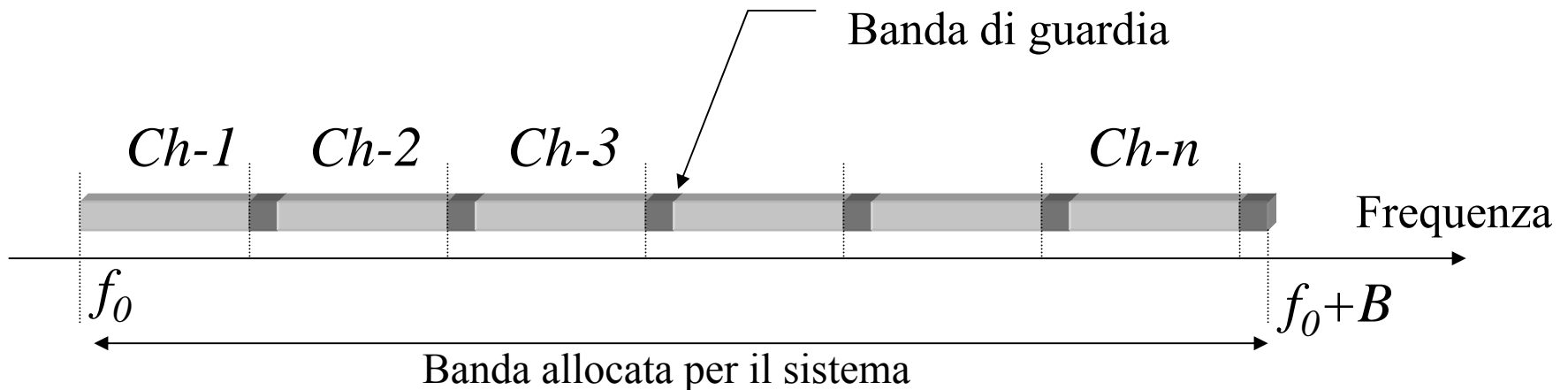
La tecnica FDMA prevede la suddivisione della banda disponibile in un certo numero di sottobande uguali ognuna centrata intorno ad una frequenza che identifica il canale. Ciascuna sottobanda è concessa ad un solo utente che ne detiene il controllo per tutta la durata della connessione.

Si utilizzano bande diverse per i due sensi della comunicazione.

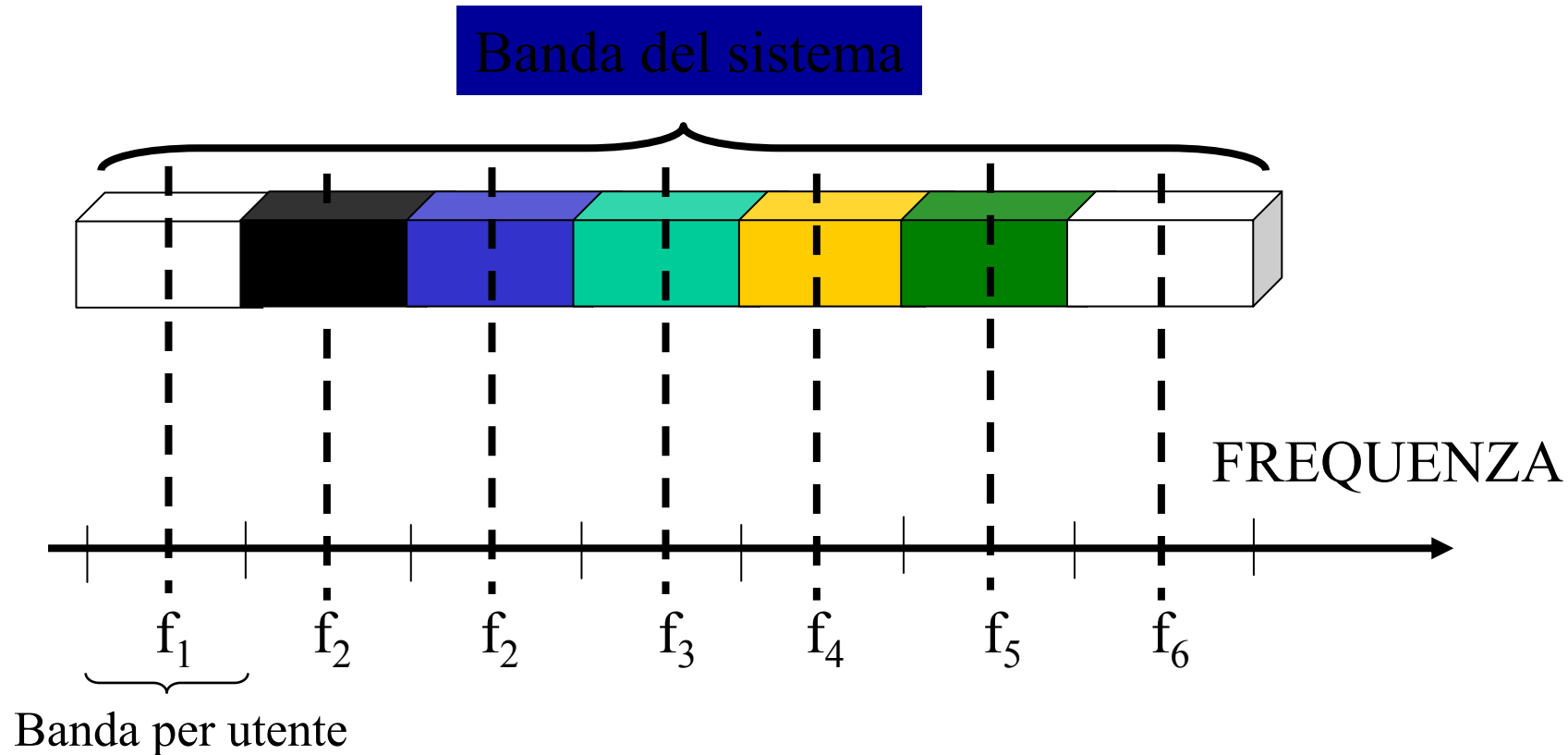
Non è richiesta la sincronizzazione fra le varie stazioni.

FDMA (Frequency Division Multiple Access)

- La banda del canale è suddivisa in un certo numero di sottobande ognuna centrata intorno ad una frequenza che identifica il canale.
- Una sottobanda può essere utilizzata da un solo utente che ne detiene il controllo per tutta la durata della connessione.
- Tra le diverse bande sono previste delle bande di guardia in modo da limitare le interferenze fra canali vicini.
- Le tecniche a divisione di frequenza sono di solito usate nei sistemi analogici



FDMA



Utente 1



Utente 2



Utente 3



Utente 4



Utente 5

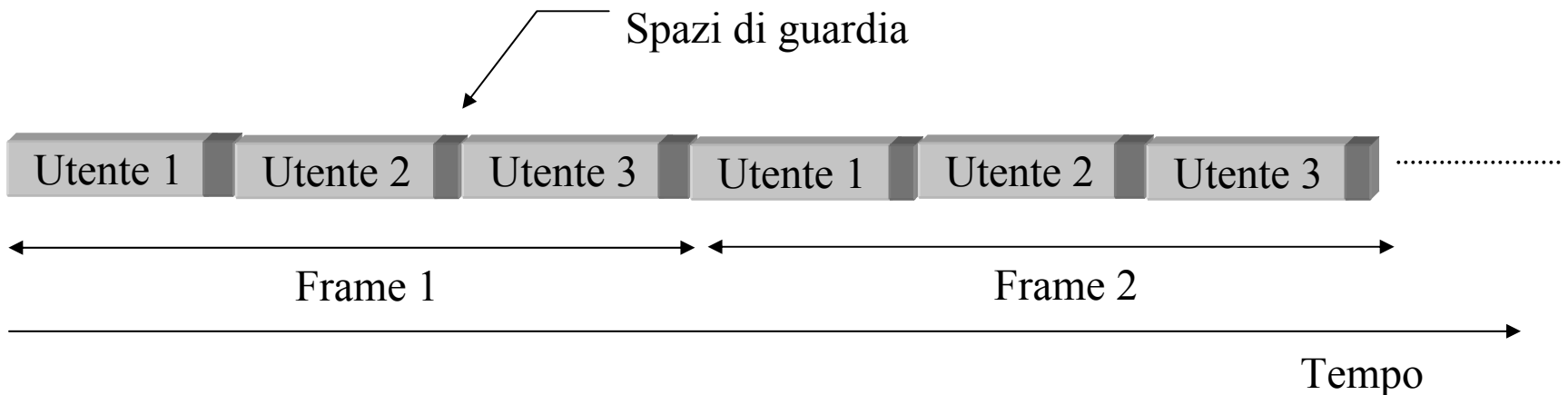


Utente 6

Per i due sensi della comunicazione vengono solitamente utilizzate bande diverse (FDD)

TDMA (Time Division Multiple Access)

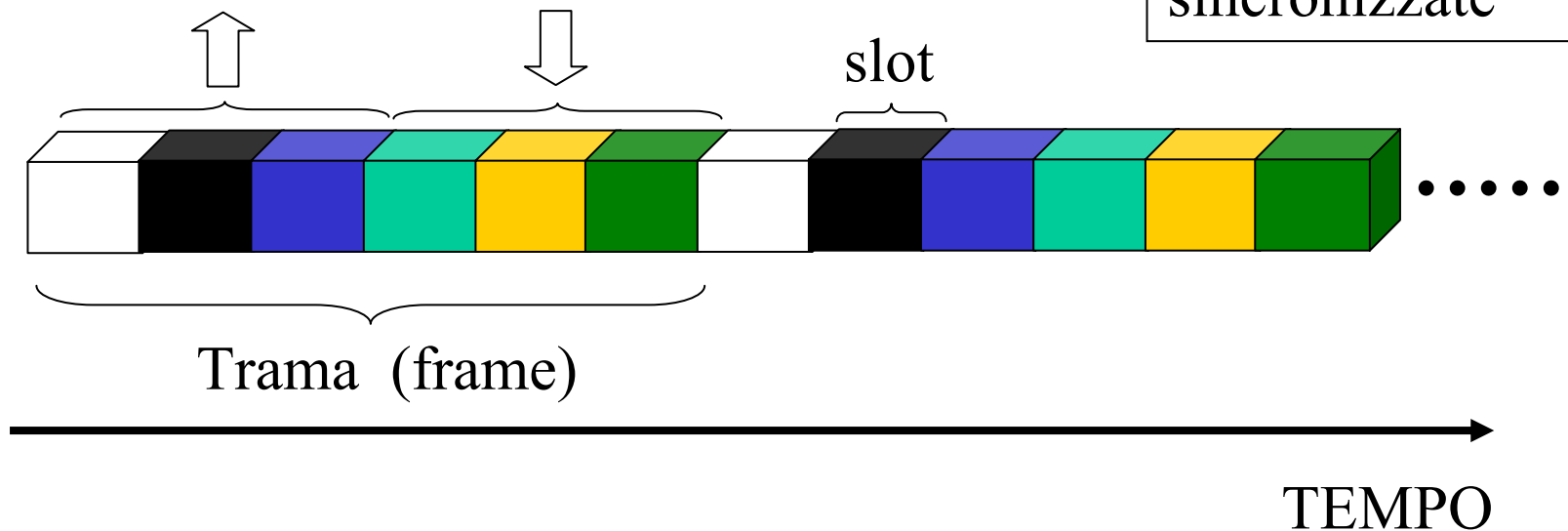
- Il tempo è suddiviso in *frames* di durata fissata e a loro volta suddivisi in un numero fisso di intervalli più piccoli denominati *slots*.
- Ogni slot in una particolare posizione all'interno del frame è assegnato ad un utente.
- Ciascun utente, può quindi trasmettere per un periodo di tempo pari ad uno slot ad intervalli pari alla durata di un frame, in questo tempo, esso ha a disposizione tutta la banda del sistema. All'interno del frame, fra uno slot e quello successivo, sono previsti degli intervalli di guardia in cui nessun utente è abilitato alla trasmissione, essi servono per compensare i ritardi di propagazione del segnale che ci possono essere fra utenti geograficamente distribuiti.



TDMA

La trama può essere suddivisa in due parti che servono per la trasmissione nei due sensi (TDD: *Time Division Multiplex*) oppure si possono utilizzare due bande diverse per i due sensi della trasmissione (FDD: *Frequency Division Multiplex*)

Le varie stazioni che accedono al canale devono essere sincronizzate



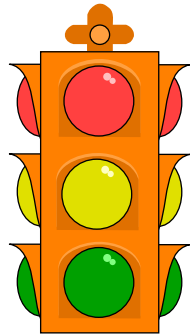
 Utente 1 ↑
 Utente 2 ↑
 Utente 3 ↑

 Utente 1 ↓
 Utente 2 ↓
 Utente 3 ↓

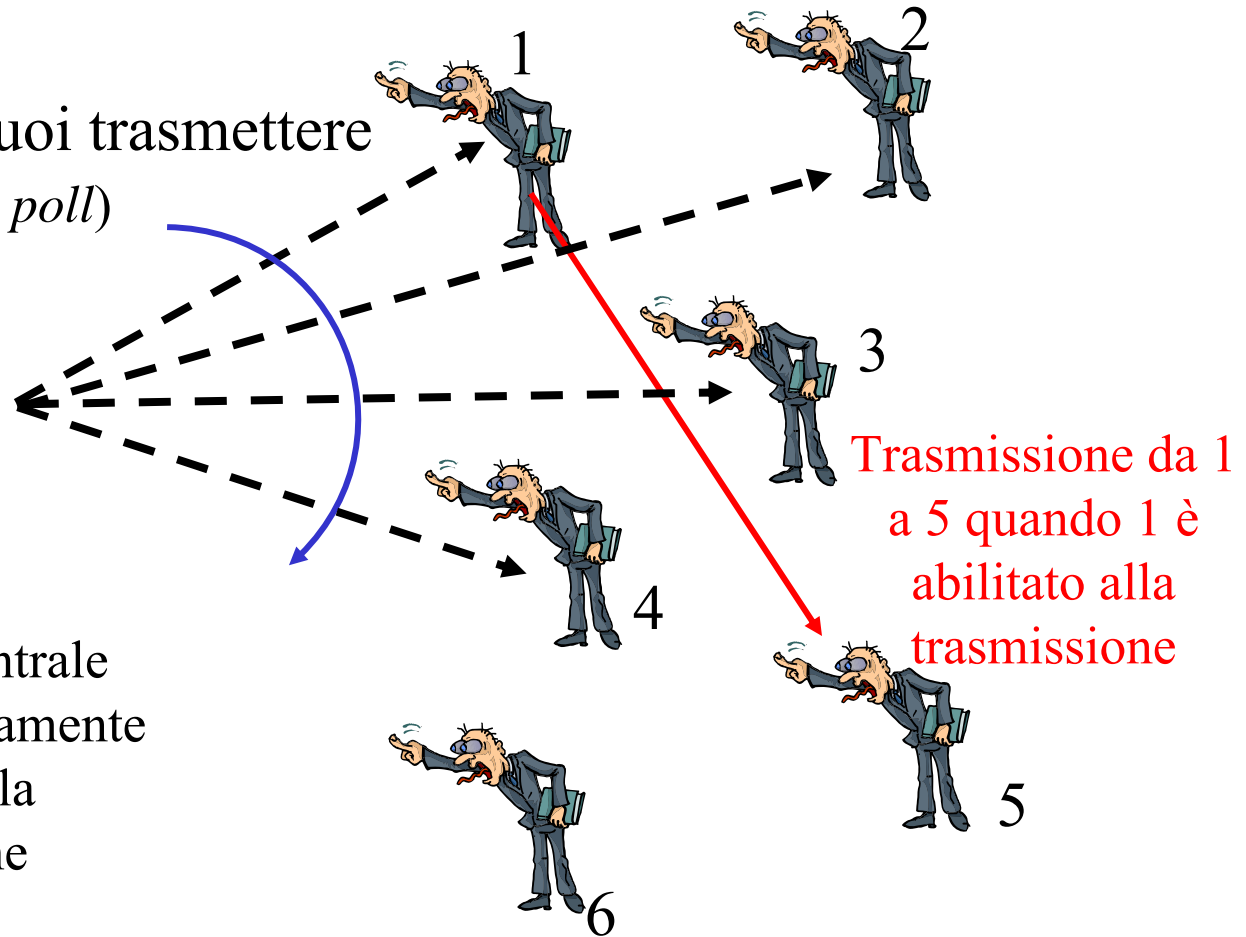
Esempio: **GSM**
durata frame: 4.62 ms
durata slot: 0.577 ms
 $n^{\circ} \text{ slot/frame} = 8$

Polling

Tocca a te, puoi trasmettere
(pacchetto di *poll*)



Controllore centrale
che abilita ciclicamente
gli utenti alla
trasmissione



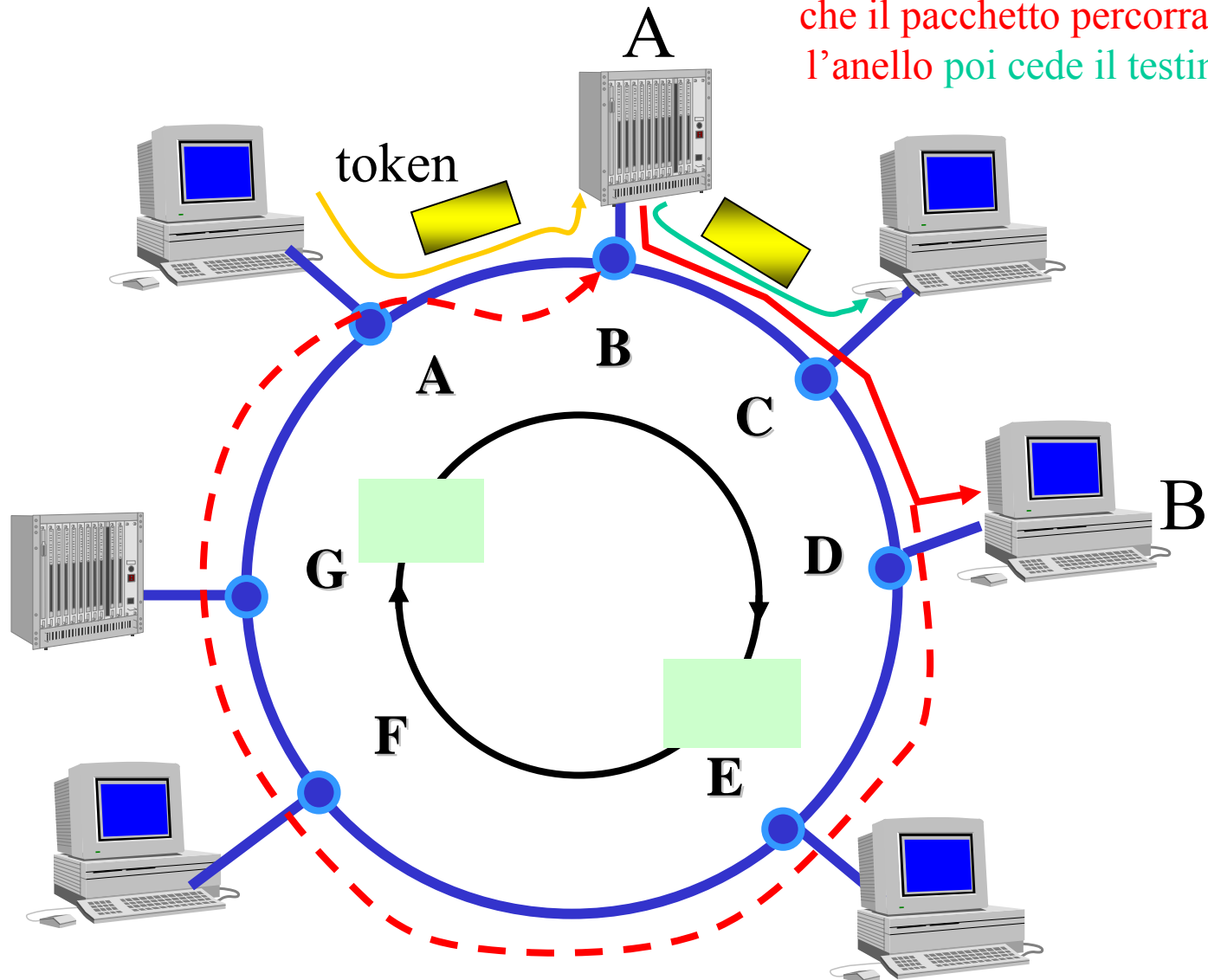
La tecnica di polling è di tipo centralizzato, essa prevede infatti una stazione *primaria* che gestisce l'accesso al canale comune da parte delle altre stazioni (*secondarie*). La stazione primaria effettua l'interrogazione di ogni stazione secondaria (SS) secondo una sequenza predefinita di polling, indipendentemente dal fatto che le SS abbiano o meno qualcosa da trasmettere

Tecniche di passaggio del testimone (Token passing)

Come abbiamo visto, gli algoritmi di *polling* necessitano di una stazione primaria che gestisce il protocollo. L'idea base dell'algoritmo di *polling* può essere estesa anche al caso in cui vi siano N stazioni di pari importanza, senza la necessaria presenza di una stazione primaria. Nel protocollo *Token Passing*, le N stazioni sono disposte secondo un ordine logico ad anello (*ring*), non necessariamente coincidente con quello fisico, ed ognuna ha un preciso indirizzo. Ogni stazione conosce l'indirizzo della successiva e della precedente, secondo l'ordine logico. Una stazione può accedere al canale solo quando riceve un particolare pacchetto detto *token* dalla stazione che la precede; se ha un pacchetto da trasmettere, vi appenderà l'indirizzo della stazione destinataria e lo immetterà sul canale comune. La stazione che riconosce il proprio indirizzo catturerà il pacchetto. Quando una stazione termina i dati da trasmettere o dopo un certo tempo massimo, invia il *token* alla stazione successiva e così via.

Tecniche di passaggio del testimone (Token passing)

A è abilitato a trasmettere (ha il token), trasmette a B ed aspetta che il pacchetto percorra tutto l'anello poi cede il testimone

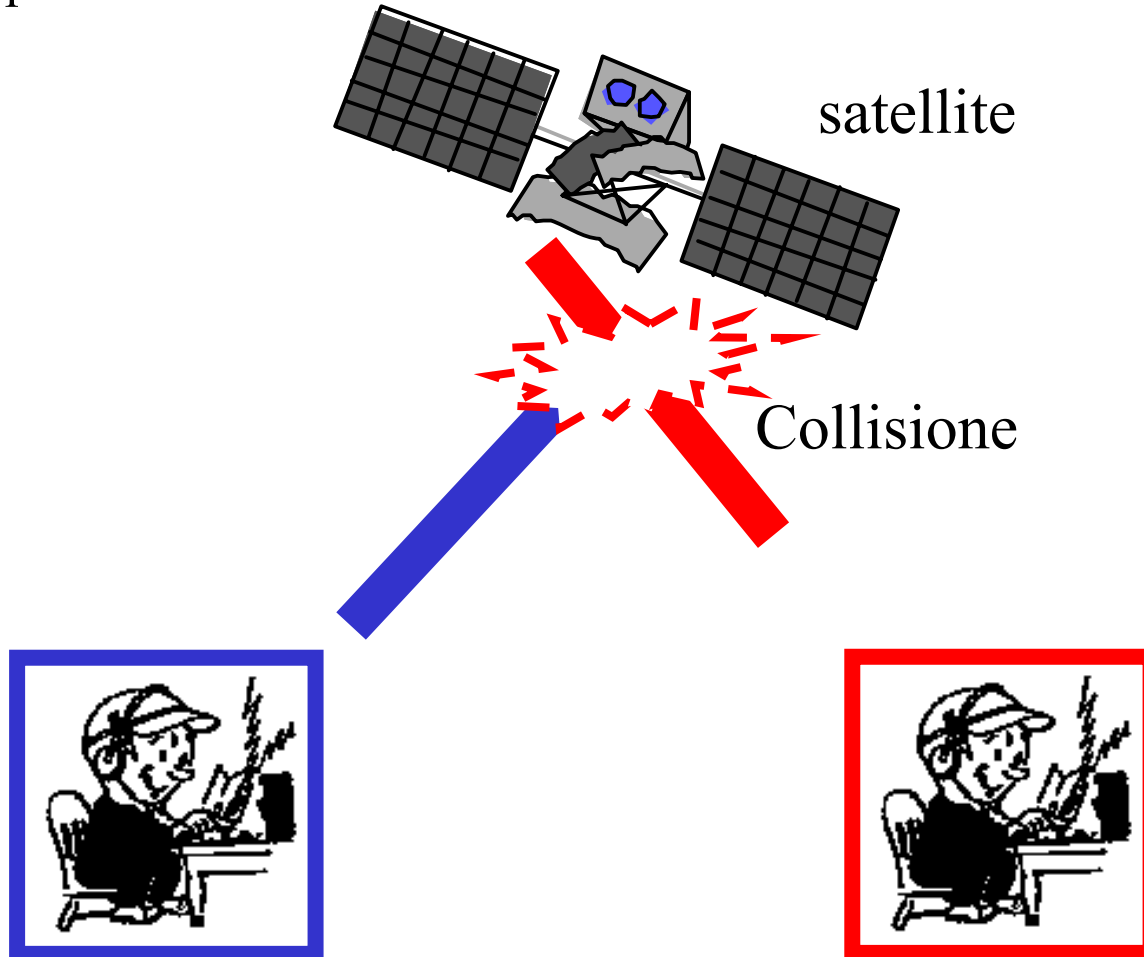


Metodi di accesso multiplo con contesa

Le tecniche di accesso multiplo a contesa, non prevedono nessuna gestione, centralizzata o distribuita, dell'accesso al canale da parte delle stazioni ad esso connesse. Nel caso più generale, quando una stazione ha dei dati da trasmettere accede immediatamente al canale senza preoccuparsi se questo è già occupato, rendendo così molto alta la probabilità di una collisione. In altri casi, la stazione “ascolta il canale” prima di trasmettere e se lo rivela occupato, ritarda la trasmissione.

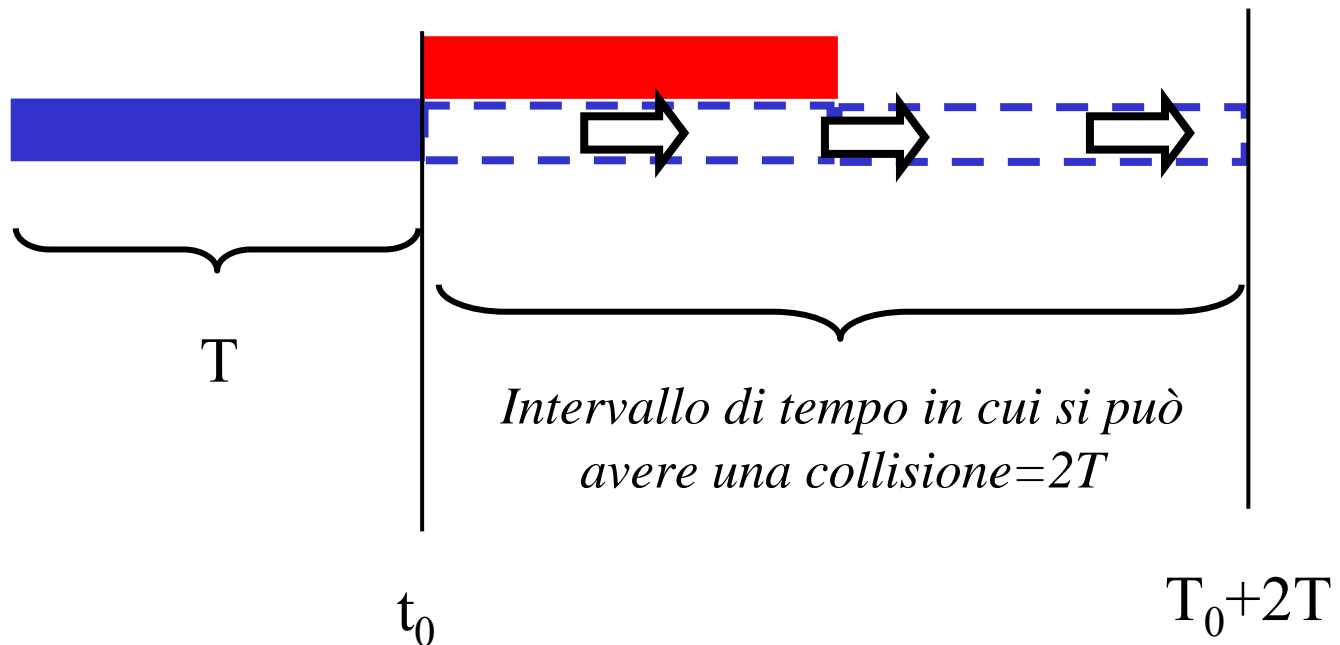
Aloha

Ogni stazione inizia la trasmissione non appena ha dei pacchetti da trasmettere, senza considerare in nessun modo le condizioni di occupato/libero del canale.



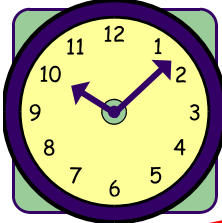
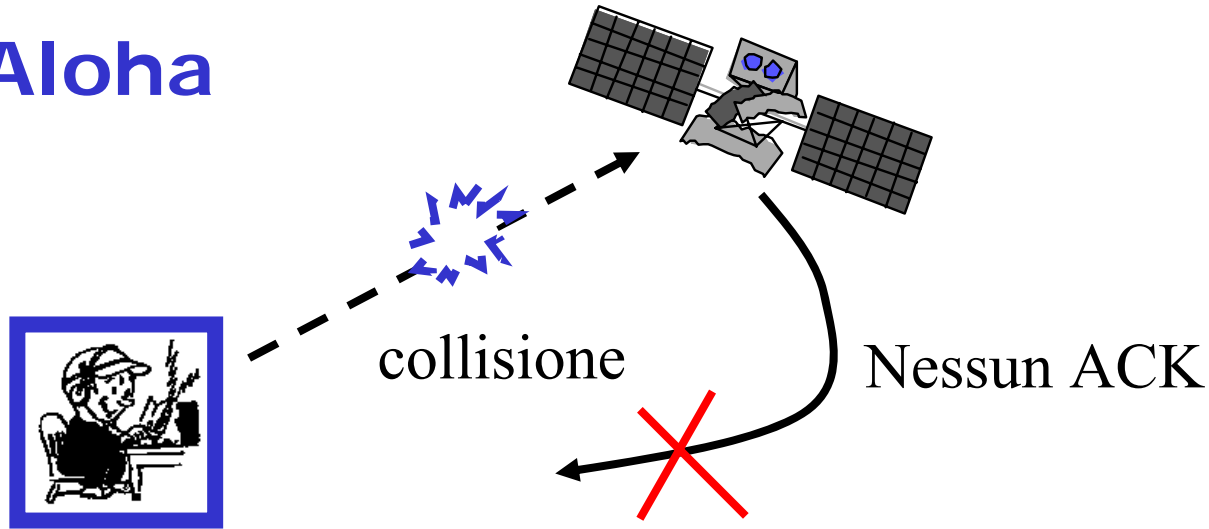
Aloha

Dal momento che ogni stazione ignora completamente tutte le altre, un pacchetto subirà una collisione se la sua trasmissione si sovrapporrà tutta o in parte a quella di un altro pacchetto.



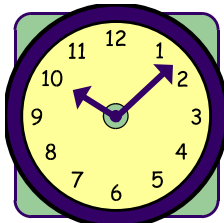
Se avviene una collisione il ricevitore non invierà nessun riscontro positivo (ACK) al trasmettitore

Aloha



Attesa ACK per un tempo di andata e ritorno

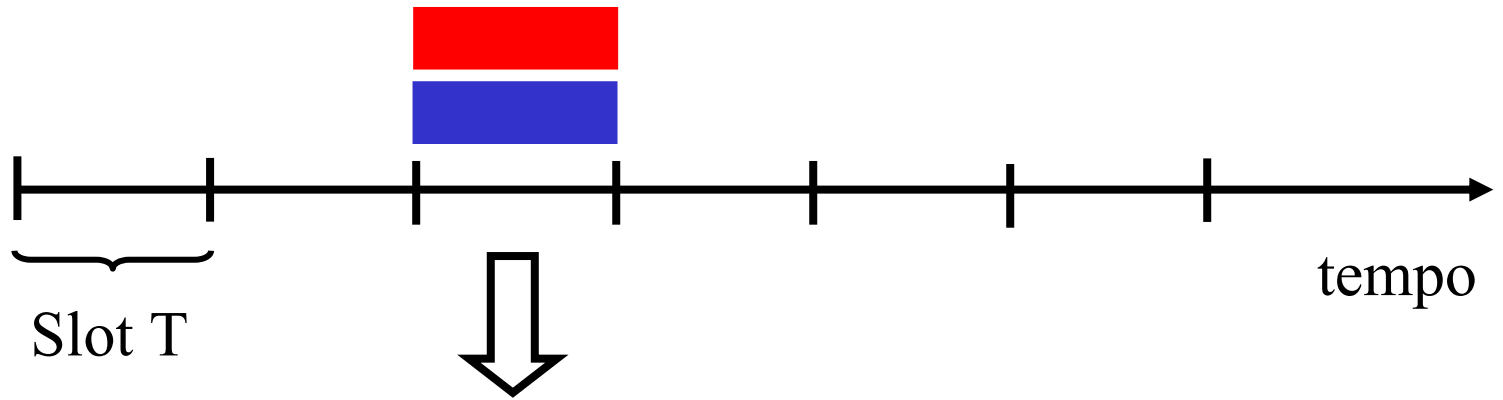
???????



La stazione riprogramma una nuova trasmissione del pacchetto dopo un tempo casuale fra 0 e un valore massimo T_{\max} (tempo di *back off*) in modo da evitare ridurre la probabilità che due stazioni che hanno colliso collidano di nuovo

Aloha slotted

Per migliorare le caratteristiche dell' *Aloha* si può pensare di dividere il tempo in *time-slot* di lunghezza pari al tempo che occorre per trasmettere un pacchetto. Una stazione che ha un pacchetto da trasmettere dovrà attendere l'inizio dello slot successivo per iniziare la trasmissione.



La collisione avviene solo quando due stazioni decidono di trasmettere nello stesso slot di durata T .

Adesso l'intervallo di tempo in cui si può avere la collisione è T e non $2T$ come nell'Aloha puro.

ALOHA Puro

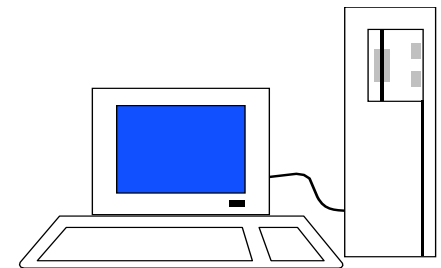
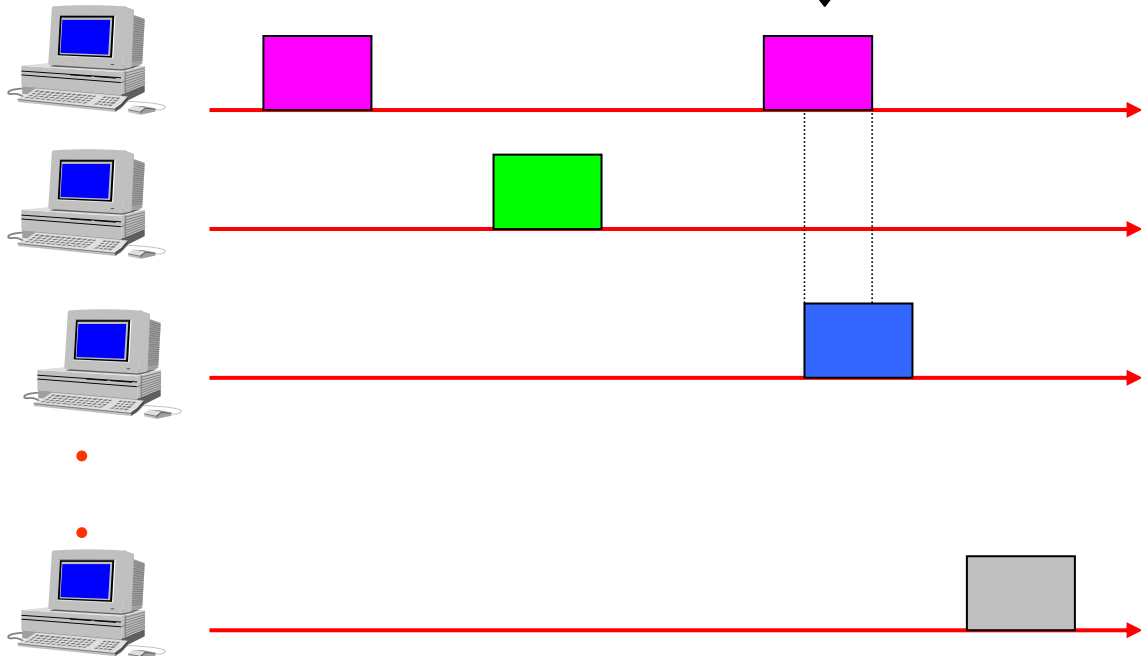
Definito nel 1970 da N.
Abramson all'università delle
Hawaii

- Ogni stazione trasmette un pacchetto composto da:
 - Testata (H = header) : contenete l'indirizzo della stazione trasmittente
 - Dati
 - Simboli per il controllo degli errori (CRC)

Pacchetto dati

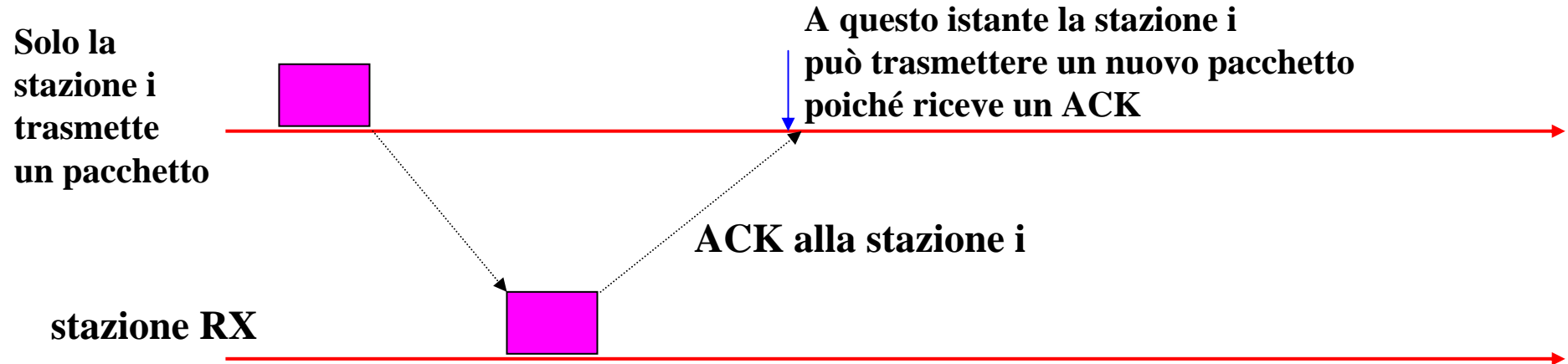


INTERFERENZA



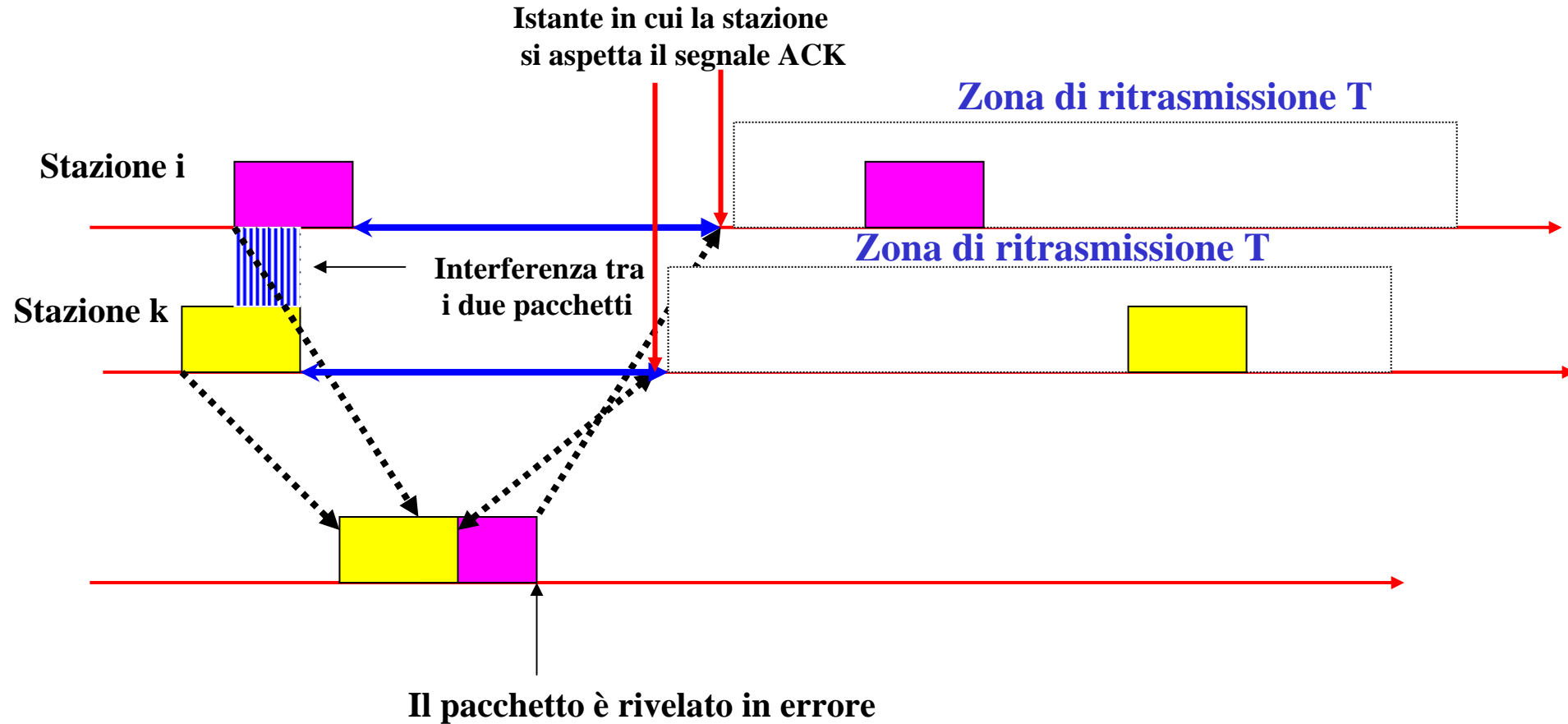
mainframe

Assenza di interferenza



- La stazione di ricezione effettua le seguenti operazioni:
 - controlla se il pacchetto è stato ricevuto correttamente
 - in caso positivo legge nella testata del pacchetto l'indirizzo della stazione trasmittente (nell'esempio l'indirizzo i) e invia un riconoscimento positivo (ACK) alla stazione trasmittente.
 - Nel caso in cui il pacchetto sia rivelato in errore la stazione ricevente non può sapere se l'indirizzo contenuto nella testata del pacchetto è corretto oppure no e quindi non può inviare nessuna informazione (perché non sa con certezza quale stazione ha trasmesso il pacchetto)

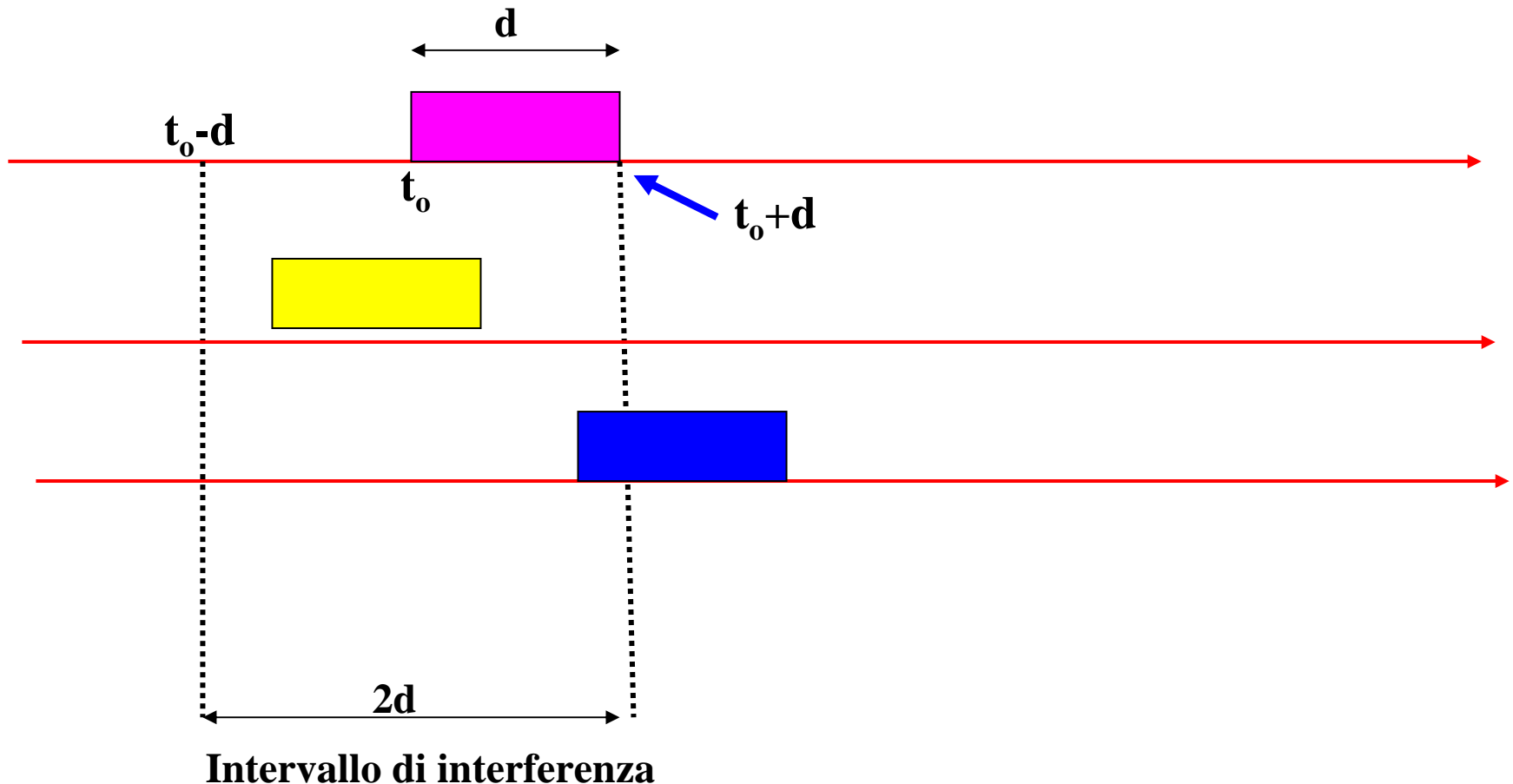
Interferenza tra stazioni



- Quando una stazione non riceve dopo il tempo prestabilito la conferma di ricezione corretta del pacchetto provvede a ritrasmetterlo adottando le seguenti regole:
 - la ritrasmissione può avvenire in un istante qualunque della zona di ritrasmissione
 - la stazione genera a caso l'istante di ritrasmissione generando un numero casuale tra 0 e T

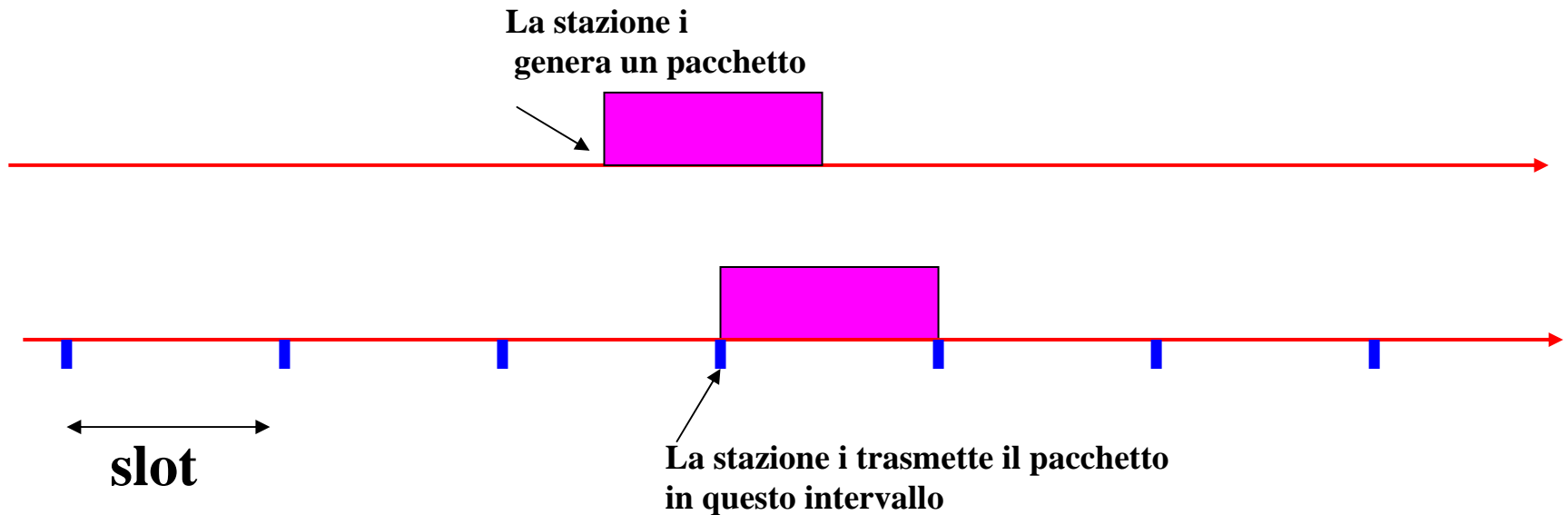
ALOHA Puro

- Se la stazione i genera un pacchetto nell'istante t , questo pacchetto viene interferito se almeno un'altra stazione genera un pacchetto tra $t-d$ e $t+d$ (d durata temporale del pacchetto)

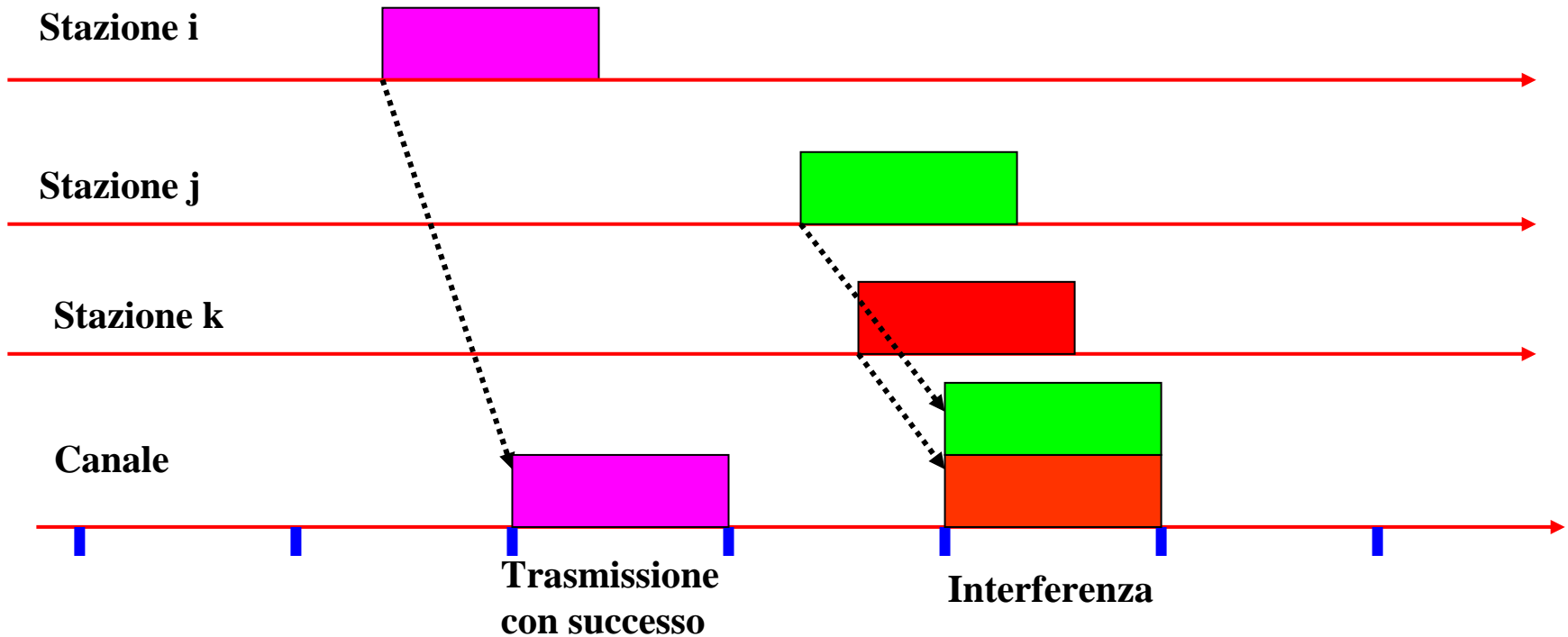


ALOHA Slotted

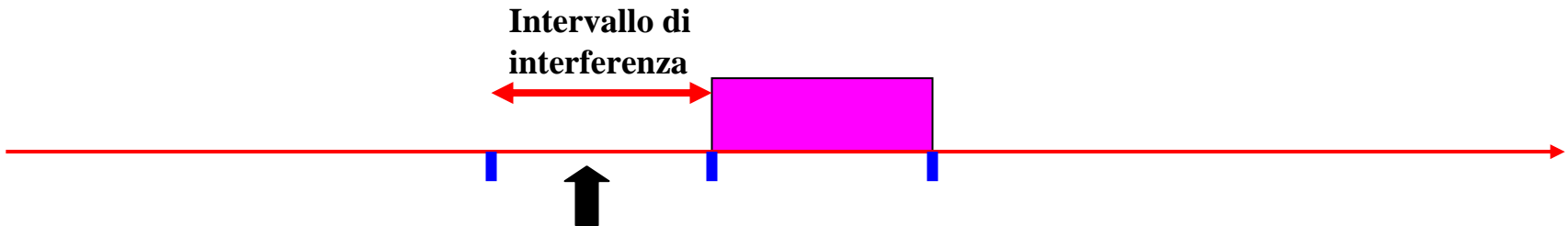
- Una stazione può trasmettere un pacchetto solo all'inizio di uno slot, per cui un pacchetto generato all'istante t può essere trasmesso soltanto all'inizio dell'intervallo successivo



ALOHA Slotted



Intervallo di interferenza



Tutti i pacchetti generati in questi intervallo sono trasmessi nello slot successivo e quindi interferiscono tra loro.
Rispetto al protocollo ALOHA puro l'ampiezza dell'intervallo di interferenza ha un'ampiezza metà.

Parametri per la caratterizzazione di un protocollo di accesso multiplo

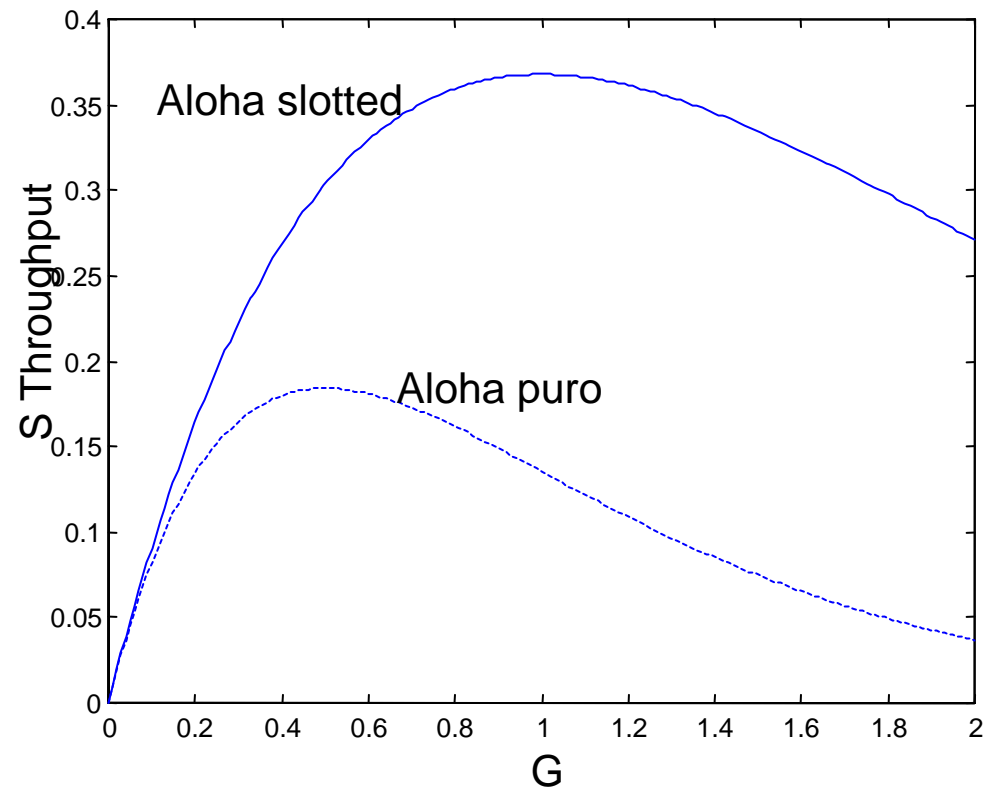
- **Throughput o efficienza S:** numero di pacchetti trasmessi con successo in uno slot.
 - S è minore o uguale a 1
 - un protocollo di accesso multiplo è tanto migliore quanto più è vicino S a 1.
- **Traffico di canale G:** numero di pacchetti presenti nel canale in uno slot-
 - G può essere maggiore di 1.
 - G è sempre maggiore o uguale a S.

ALOHA PURO

$$S = G e^{-2G}$$

ALOHA SLOTTED

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



Aloha puro / Aloha slotted

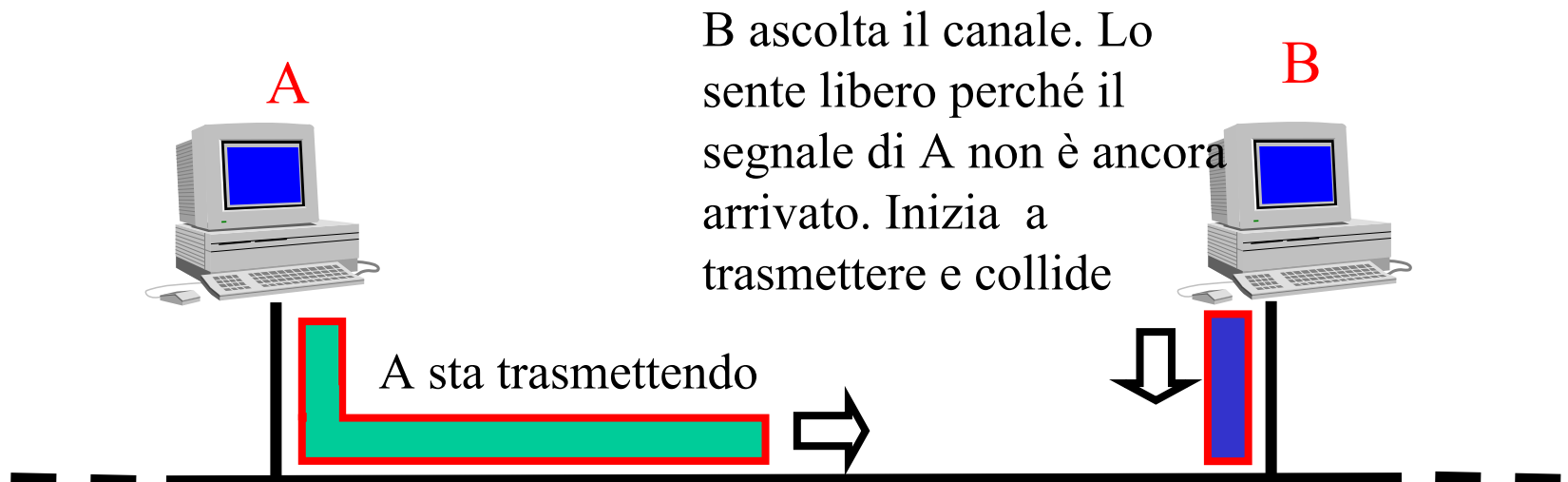
- Grazie all'introduzione degli slot l'Aloha slotted riesce ad avere un'efficienza doppia rispetto all'Aloha puro.
- L'Aloha slotted richiede una sincronizzazione fra le stazioni che comporta una maggiore complessità e costo delle stesse.
- In ogni caso l'efficienza massima (throughput) che si ottiene con lo slotted è solo 0.36 che è comunque molto bassa.

CSMA (*Carrier Sense Multiple Access*)

Accesso multiplo con ascolto della portante.

Il CSMA è molto simile all'Aloha, ma in questa tecnica, ogni stazione può analizzare (ascoltare) il canale per rivelare o meno una trasmissione in corso. L'accesso al canale avviene solo se questo è rivelato libero.

Questo non elimina del tutto la probabilità di collisioni. Infatti, occorre considerare i **tempi di propagazione** del segnale fra due stazioni.



CSMA

- Ambito LAN: le stazioni possono monitorare lo stato del canale di trasmissione
- Le stazioni sono in grado di “ascoltare” il canale *prima di iniziare a trasmettere* per verificare se c'è una trasmissione in corso
- **Algoritmo CSMA**
 - se il canale è libero, si trasmette
 - se è occupato, sono possibili diverse varianti
 - **non-persistent** : rimanda la trasmissione ad un nuovo istante, scelto in modo casuale
 - **Persistent** : nel momento in cui si libera il canale, la stazione inizia a trasmettere, se c'è collisione, come in ALOHA, si attende un tempo casuale e poi si cerca di ritrasmettere

CSMA: collisioni

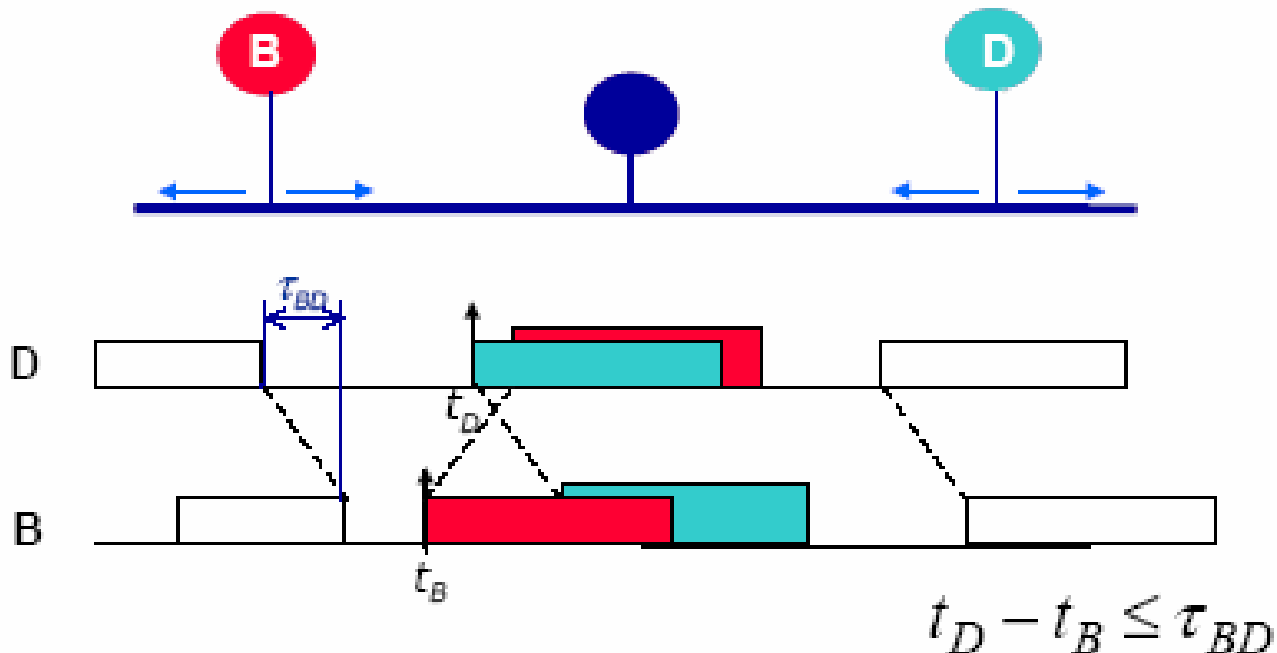
- **A causa dei ritardi di propagazione il protocollo CSMA NON evita le COLLISIONI**



- il ritardo di propagazione implica che due nodi non possano sentirsi reciprocamente all'inizio della trasmissione

CSMA: collisioni

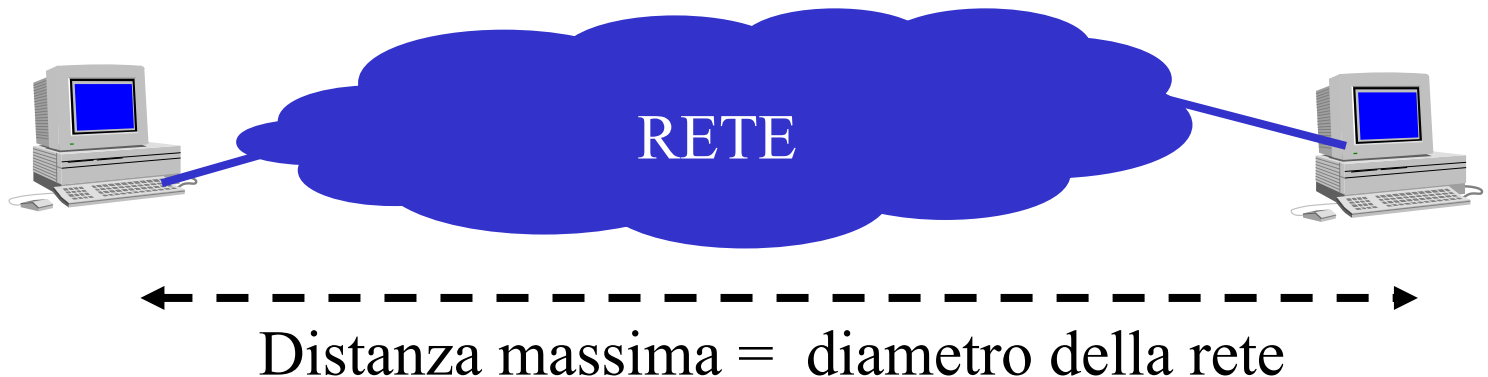
- Si ha collisione tra due stazioni se esse accedono al canale in istanti che distano tra loro un tempo inferiore a quello di propagazione tra le due stazioni



CSMA (*Carrier Sense Multiple Access*)

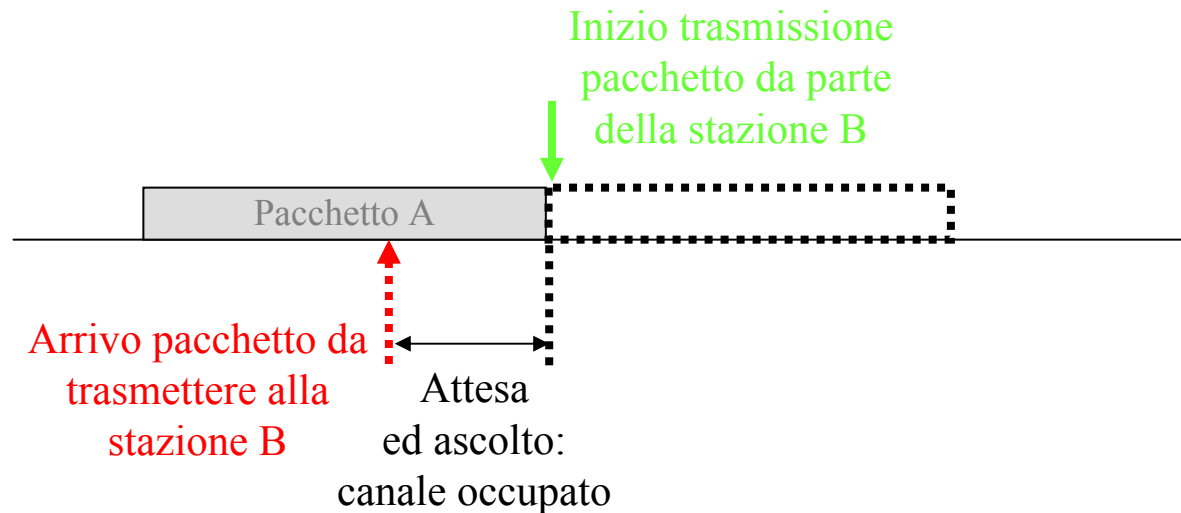
Accesso multiplo con ascolto della portante.

Nell'analisi dei protocolli CSMA, i ritardi di propagazione rivestono una grande importanza. Quando una stazione inizia la trasmissione, le altre stazioni connesse al mezzo potranno accorgersene solo dopo il tempo necessario perchè il segnale si propaghi fino a loro. Si può dire che ogni pacchetto trasmesso con CSMA ha una finestra di vulnerabilità che coincide con il tempo che occorre affinchè la stazione più distante possa ricevere l'inizio del pacchetto. Per questo motivo, **i protocolli CSMA funzionano bene in reti abbastanza piccole e con lunghezza dei pacchetti elevata dato che i ritardi di propagazione devono essere piccoli rispetto alla lunghezza dei pacchetti.**



1-persistent CSMA

Ogni stazione ascolta il canale: se lo rivela libero trasmette subito, altrimenti continua ad ascoltarlo finché non diviene libero e subito dopo trasmette

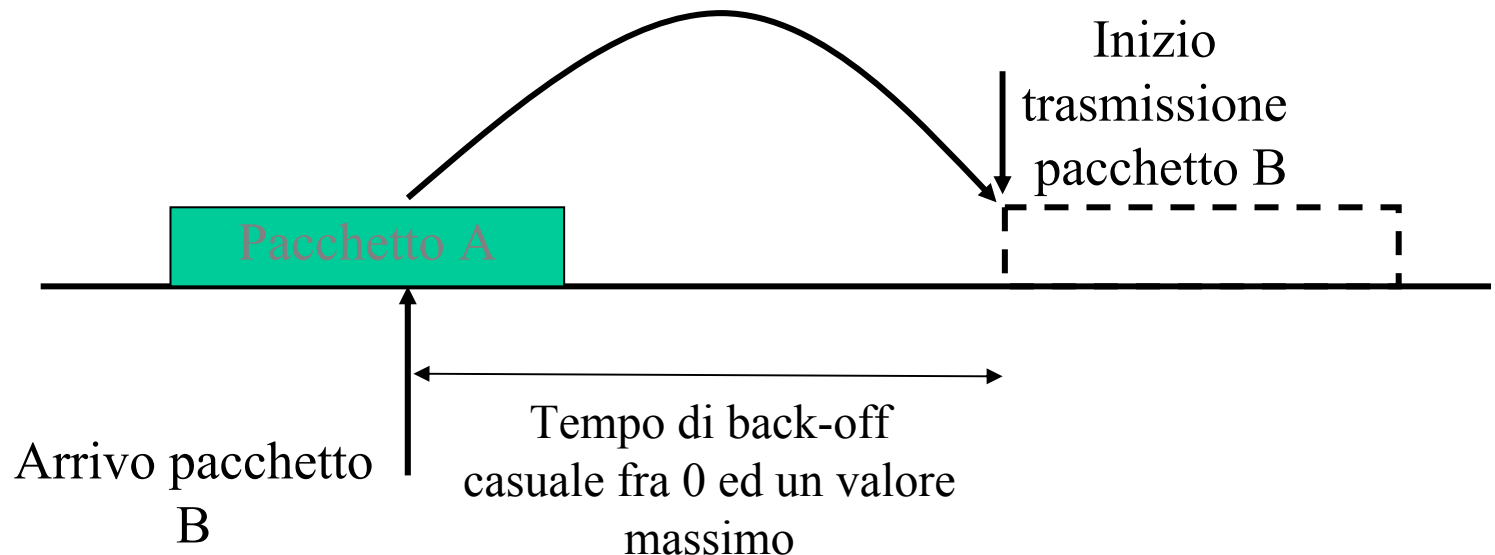


PROBLEMA: se due stazioni generano un pacchetto durante la trasmissione di A, attenderanno entrambe la fine della trasmissione in atto e poi occuperanno entrambe il canale creando una collisione.

QUINDI questo sistema funziona se il traffico è poco e la probabilità che due o più stazioni generino pacchetti durante una trasmissione è molto bassa.

Non-persistent CSMA

La stazione che ha un pacchetto da trasmettere ascolta il canale. Se lo rivela libero inizia la trasmissione. Se il mezzo è occupato, cessa di ascoltare il canale e genera, in modo casuale, un tempo di *back-off* dopo il quale ritenterà l'accesso.



In questo modo si riduce la probabilità che più stazioni accedano contemporaneamente non appena il canale diventa libero.

P-persistent CSMA

E' una tecnica che permette di ottenere le prestazioni dell' 1-persistent per bassi carichi e del non-persistent per alti carichi.

Si tratta comunque di un protocollo poco usato perché richiede un'elevata complessità hardware.

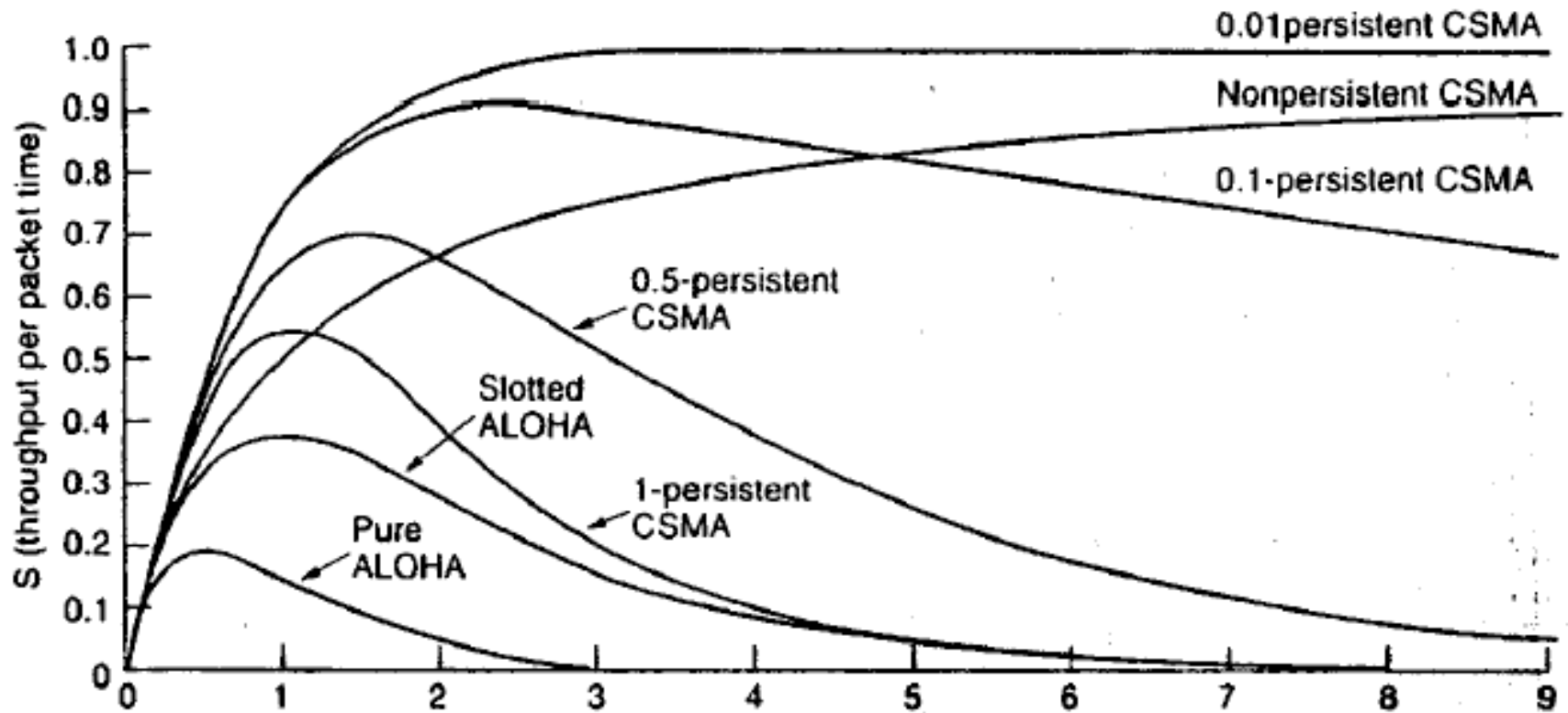
CSMA: p-persistente

- Il tempo viene suddiviso in intervalli
- la lunghezza degli intervalli è uguale al periodo di vulnerabilità *round trip propagation delay* 2τ
- Algoritmo
- 1. ascolta il canale
 - se il canale è libero
 - si trasmette con probabilità p ;
 - se si è deciso di trasmettere, si passa al punto 2
 - se non si è deciso di trasmettere, si attende un intervallo di tempo e si torna al punto 1
 - se è occupato, si attende un intervallo di tempo e si torna al punto 1
- 2. se c'è collisione
 - si attende un tempo casuale e poi si torna al punto 1

Periodo di vulnerabilità

- Il periodo di vulnerabilità è legato al ritardo di propagazione del segnale sul canale.
- Se indichiamo con τ il tempo di propagazione tra le due stazioni più distanti il periodo di vulnerabilità è 2τ
- se una stazione ha iniziato a trasmettere, ma il suo segnale non è ancora arrivato a tutte le stazioni, qualcun altro potrebbe iniziare la trasmissione
- In generale, il CSMA viene usato in reti in cui il ritardo di propagazione τ è \ll di T (tempo di trama)

Prestazioni sistemi CDMA



CSMA/CD (Collision Detection)

CSMA con rivelazione delle collisioni

Nei protocolli che abbiamo visto, le stazioni non si accorgono quando avviene una collisione e quindi continuano a trasmettere tutto il pacchetto inutilmente.

Il protocollo CSMA/CD è stato studiato proprio per eliminare questo spreco di banda.

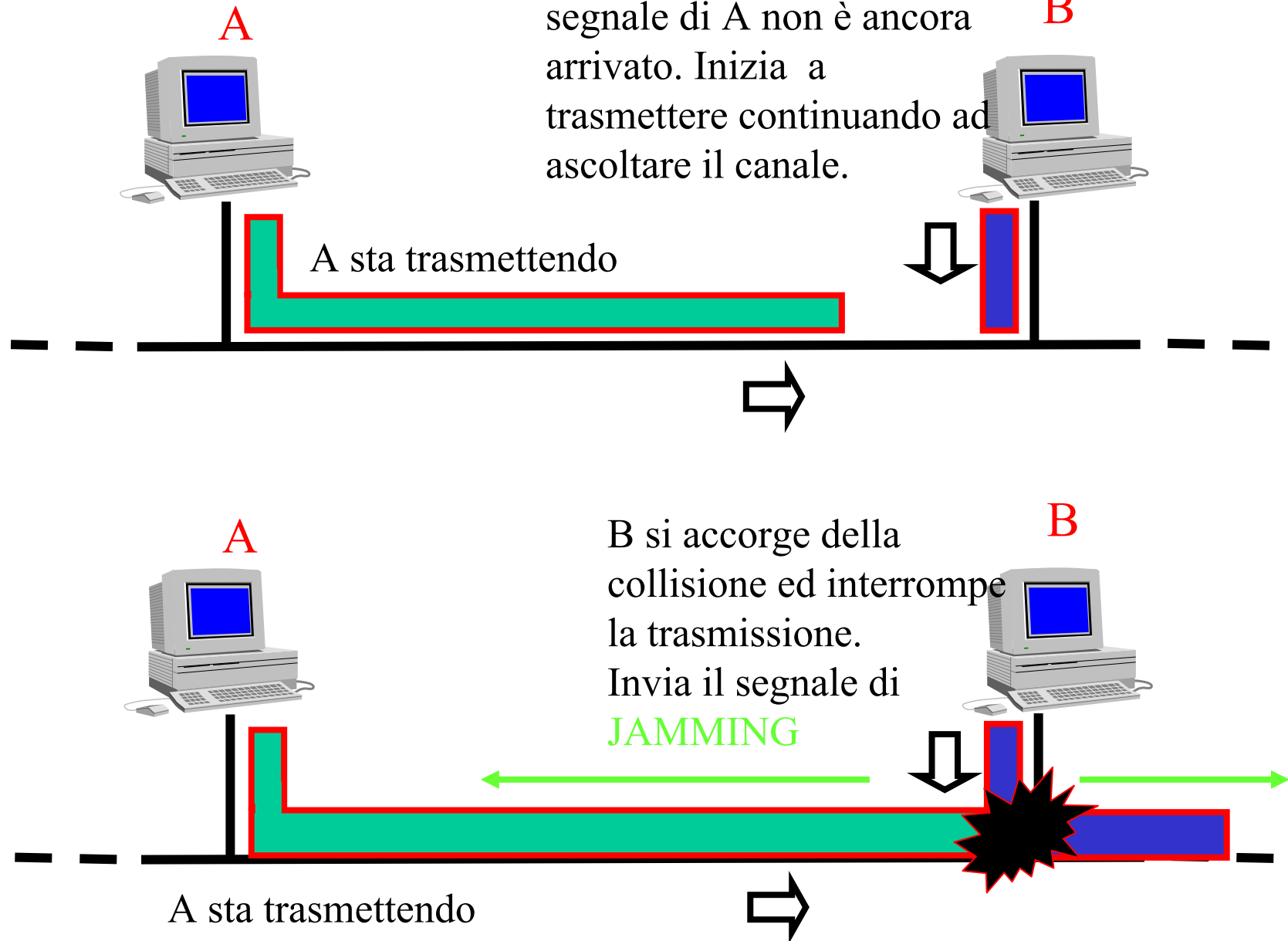
Ogni stazione è dotata di un hardware che permette di rilevare una collisione. In pratica ogni stazione ascolta il canale anche quando sta trasmettendo.

Non appena la stazione si accorge di una collisione, cessa immediatamente la trasmissione ed invia sul mezzo un segnale di **jamming** per comunicare alle altre stazioni che il canale è occupato dall'estinzione di una collisione. La stazione aspetta un periodo di tempo casuale (*back-off*) e tenta nuovamente l'accesso.

Protocollo CSM/CD

- Se la stazione che sta trasmettendo rileva la collisione, interrompe immediatamente
- Una volta rilevata collisione, non si continua a trasmettere trame già corrotte
- Quando si verifica un collisione, si trasmette una particolare sequenza, detta di jamming

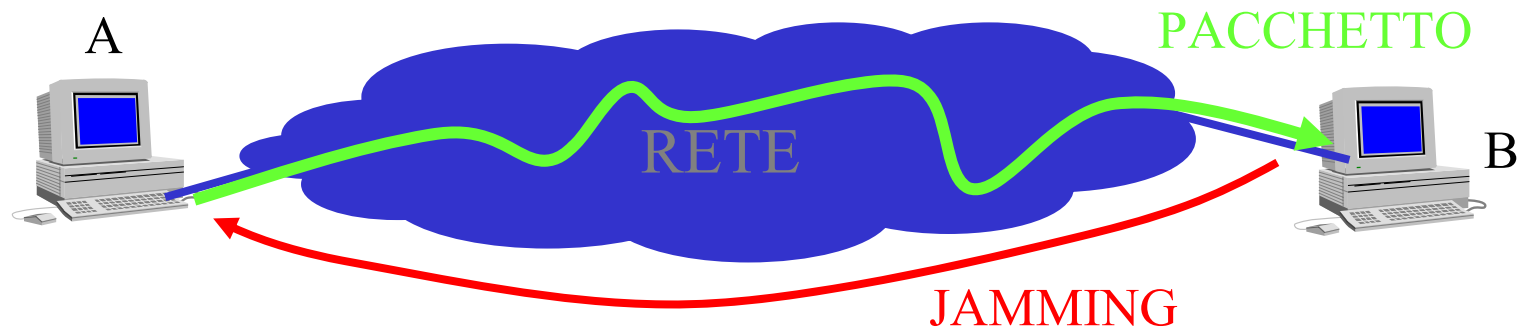
CSMA/CD



CSMA/CD

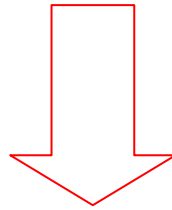
Nel CSMA/CD il tempo di propagazione dei segnali attraverso l'intera rete è un parametro fondamentale. E' infatti necessario che quando avviene una collisione tutte le stazioni lo sappiano e per questo occorre un tempo che dipende dalla velocità di trasmissione e dalle dimensioni della rete.

Perché il protocollo sia efficiente occorre che vi sia un certo rapporto fra le dimensioni della rete e la durata di un pacchetto. In particolare, la stazione A deve sapere della collisione prima che abbia finito di trasmettere il pacchetto



CSMA/CD

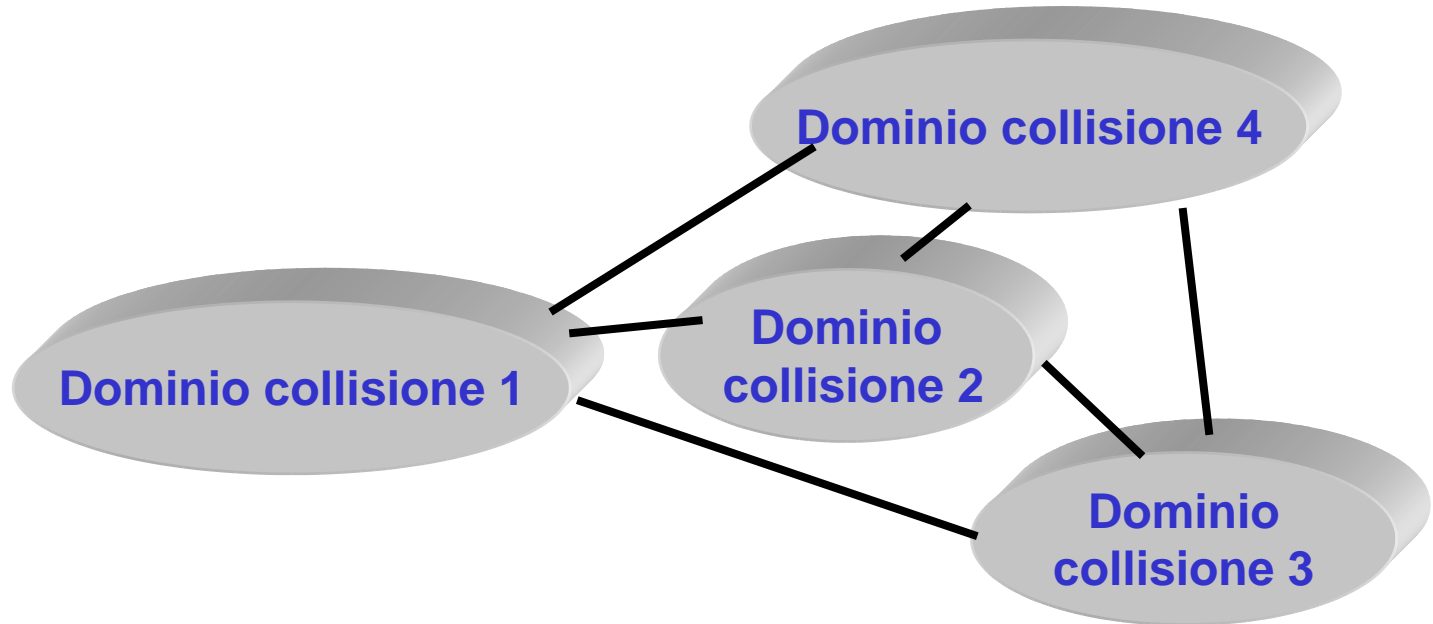
Quindi la durata temporale di un pacchetto deve essere superiore al tempo di propagazione (andata e ritorno) fra le stazioni più distanti della rete.



- A parità di lunghezza del pacchetto, per aumentare la velocità di trasmissione occorre diminuire le dimensioni della rete.
- A parità di dimensioni della rete, per aumentare la velocità occorre aumentare la lunghezza in bit del pacchetto

CSMA/CD

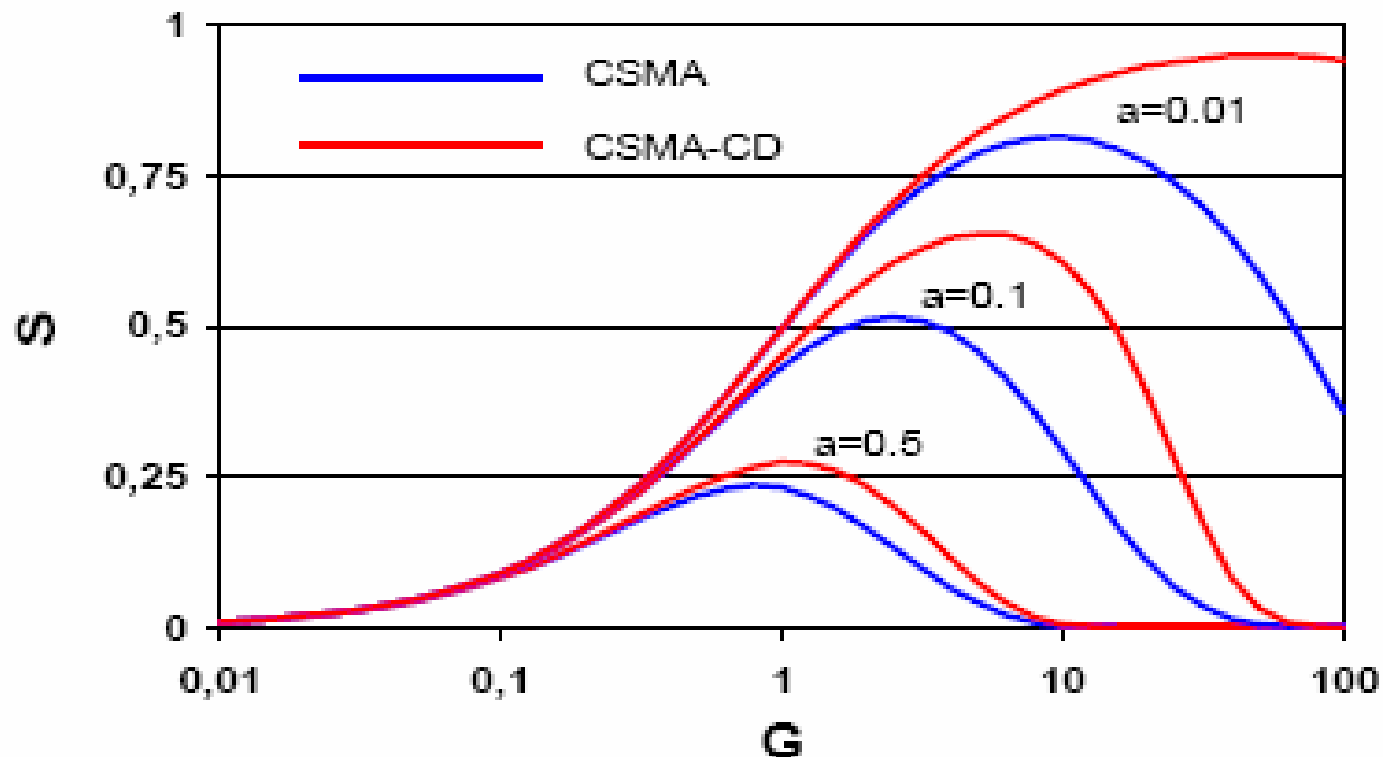
- Per realizzare reti estese e ad elevata velocità occorre suddividere tali reti in parti più piccole dette **domini di collisione**. Ogni stazione può **collidere solo con le macchine del proprio dominio di collisione**. Questa suddivisione si può realizzare attraverso particolari apparati di rete quali BRIDGE e SWITCH.



CSMA / CD: prestazioni

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

- per $\delta=0$:



Le risorse radio

Le trasmissioni degli utenti si differenziano per il tempo in cui trasmettono, per la banda in frequenza usata, per il codice.

