Rete Wireless

Lo standard 802.11 nacque nel 1997 ma praticamente rimase solo sulla carta per via delle insufficienti prestazioni che consentiva (tra cui velocità solo fino a 1 o 2Mbps). Nel 1999 la IEEE emise due nuovi standard:

- **802.11a** che, sfruttando una delle più versatili tecniche di modulazione (QAM-64), poteva raggiungere i 54Mbps a 5.2GHz;
- **802.11b** con due nuove velocità: 5.5Mbps e 11Mbps a 2.4GHz.

- Molti governi hanno mantenuto libere alcune frequenze tra cui la 2,4 Ghz, nota come industrial scientific and medical
  - Si può usare da chiunque senza licenze a patto di rispettare dei limiti di potenza e spread spectrum che consente di distribuire il segnale su banda più larga del necessario in modo che appaia come rumore a dispositivi non interessati,, per evitare le interferenze
- Più aumenta la frequenza e più aumenta l'assorbimento
- A 2,4 Ghz si coprono distanza superiori alla 5 Ghz 80 vs 20
- Queste frequenze sono usati pure per forni a microonde, cordless, radiocomandi, apparti radar e bluetooth
- L'802.11b a 11 Mbps è noto come wi fi wireless fidelity

L'unico svantaggio della 802.11b rispetto alla 802.11a è la velocità (11Mbps contro 54Mbps). Nel 2003 l'IEEE propose una sua variante, l'**802.11g**, in grado di raggiungere i 54Mbps nella banda ISM tradizionale a 2.4GHz, mantenendo inoltre la compatibilità verso il basso con i dispositivi 802.11b.

- Gli standard b e g dividono lo spettro in 14 sottocanali di cui 13 utilizzabili in europa, da 22 Mhz ciascuno
  - I canali sono parzialmente sovrapposti tra in frequenza
  - Tra canali successivi c'è interferenza, quindi per evitarle si usa la regola del 5, cioè i 2 gruppi di canali distanti 5 non si sovappongono

I dispositivi che costituiscono le reti wireless sono due (figura 2):

1. i **Wireless Terminal** (WT): sono dispositivi mobili (notebook, palmari, cellulari, smartphone) dotati di interfaccia 802.11 integrata o su schede PCMCIA o USB, oppure fissi (personal computer) con schede PCI o adattatori USB;
2. gli **Access Point** (AP): hanno un doppio scopo, da un lato sono dei bridge che collegano la parte cablata (*wired*) con la parte wireless, dall'altro consentono ai WT di collegarsi alla rete wireless (agiscono quindi da gateway). È possibile anche usare dei computer dotati di apposito software per fungere da AP.

- E' possibile collegare tra loro più AP
- Nel wireless non si può rilevare la collisione, è un bel problema, tecniche come la csma/cd non sono utilizzabili, come le trasmissioni via ethernet
- Il modo più semplice è costringere chi trasmette a verificare che sia libero prima di trasmettere

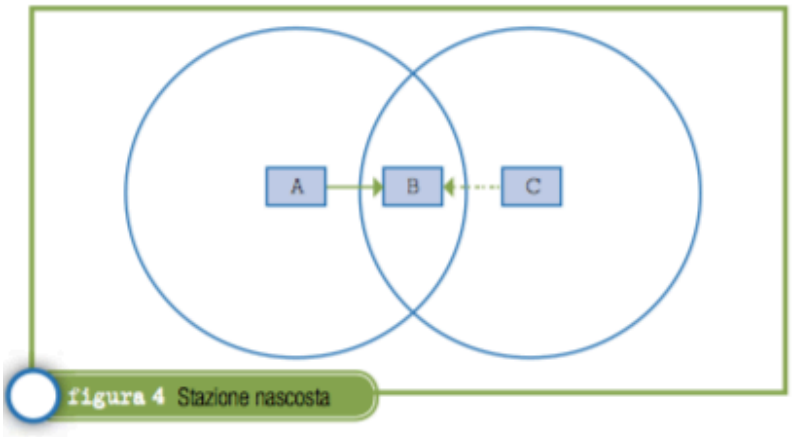

figura 4 Stazione nascosta

a. Problema della stazione nascosta (figura 4):
supponiamo di avere tre stazioni, A, B e C, con i raggi d'azione di A e C raffigurati, e che A stia trasmettendo a B:
Se ora C ascolta il canale, lo troverà libero e sarà convinta di poter trasmettere a B; cominciando a trasmettere disturberà la trasmissione di A, impedendo a B di riceverla; sia A che C saranno costrette a ritrasmettere.

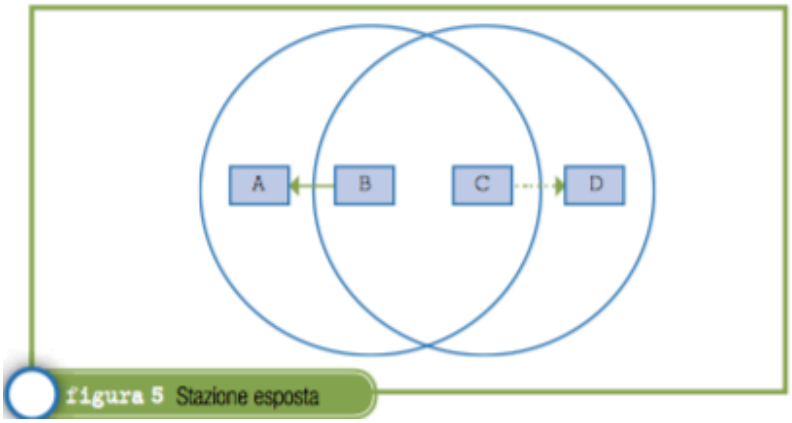

figura 5 Stazione esposta

b. Problema della stazione esposta (figura 5):
supponiamo di avere quattro stazioni, A, B, C e D, con i raggi d'azione di B e C raffigurati e che B stia trasmettendo ad A mentre C voglia trasmettere a D.
Ascoltando il canale, C sentirà la trasmissione di B e concluderà erroneamente di non poter trasmettere; invece, essendo D fuori della portata di B, e A fuori della portata di C, le due trasmissioni potrebbero avvenire parallelamente senza interferenze.

a: A trasmette a c, c non sente che dice a, ma tenta di parlare ad a, b sente tutto e non capisce una minchia, tipo stare al cinema con due logorroici a destra e sinistra
b: la comunicazione avviene tra b ed a, b trasmette o a c o ad a.
C sente b e non trasmette a B, quindi potrebbe esserci la collisione, si blocca lui proprio.

Il secondo problema della stazione esposta si può risolvere con una vuole progettazione fisica di rete, sistemando le stazioni nei rispettivi raggi di azione (situazione ideale ma frequente)

Il primo problema della nascosta è possibile risolverlo mediante Carrier Sensing Virtuale che consiste nell'invio di un frame che si chiama RTS Request to Send al destinatario contenente l'informazione sulla durata della trasmissione che vuole effettuare. Il destinatario risponde con il CTS clear to send, che è come l'ok per rispondere proprio. In

C'è il rischio che però che in due possano mandare la rts, quindi allora c'è un algortmo che riduce questa cosa che si chiama CSMA CA Cioè collision avoidment
Qui si da un intervallo di tempo che si chiama AIFS Cioè arbitration inter frame space) durante il quale il trasmettitore attende per evitare altri RTS REQUEST TO SEND.

Quindi invia la request to send aspetta l'aifs se non sente ctg o rts, invia, se l'altra trasmissione tenta di trasmettere in contemporanea, si ha ancora il back off esponenziale binario, tempo pseudocasuale, che si basa a finestra di contesa slotted back of window. finestra dotata di un numero di slot time

Che rappresentano la larghezza indicata con CW contention window. L'algoritmo sceglie random uno di questi slot time
Abbiamo una finestra quindi con degli slot time all'interno ogni slot è quindi x secondi
L'algoritmo sceglie random uno di questi slot, cioè nel secondo che va da per esempio 2 a 4 puoi trasmettere se ancora ci sono collisioni allora la finestra si raddoppia, e spam a manetta

più collidono e più ci sono persone e quindi più grandezza di sliding windows, di solito la finestra ha 7 slot time fino a 255 che è il massimissimissimo raggiungibile, appena si riesce ritorna a 7 più è alto il range è più è complicato che peschino lo stesso valore