1 Lezione del 02-12-25

1.0.1 Numero di hop

Continuiamo la discussione delle reti mobili, introducendo una nuova caratteristica ortogonale: il **numero di hop** necessari per completare un percorso ricevitore-trasmetittore.

1.0.2 Classificazione delle reti wireless

Noto il numero di hop (se uno o più di uno), e dividendo fra reti ad hoc (vist in 26.3.4) o basate su infrastruttura locale, possiamo fare la seguente classificazione ortogonale:

	Hop singolo	**Hop multiplo**
A infrastruttura	Gli host si connettono alle stazioni base, che quindi si connettono ad una rete più grande (*WiFi*, *reti celullari*)	Gli host devono passare attraverso più nodi wireless per connettersi ad internet (*reti di sensori*)
Ad hoc	Non c'è stazione base (e quindi connessione ad Internet), i dispositivi si coordinano fra di loro (*Bluetooth*, *reti ad hoc*)	Non c'è stazione base (e quindi connessione ad Internet), e i dispositivi devono attraversare più hop per raggiungere l'un l'altro (reti *MANET* e *VANET*)

Noi in particolare tratteremo le reti *single hop* basate su infrastruttura, cioè reti WiFi e reti cellulari.

1.0.3 Caratteristiche del mezzo wireless

Prendiamoci un momento per analizzare le caratteristiche del **mezzo wireless** stesso, e in particolare le differenze dai mezzi cablati a cui siamo abituati.

- Notiamo innanzitutto che la **potenza di trasmissione** è molto minore, e viene persa man di mano che il segnale si propaga nello spazio (il cosiddetto *path loss*);
- Esiste **interferenza** fra più fonti: ad esempio, la banda ISM a 2.4 GHz è pubblica, e condivisa da diversi dispositivi (WiFi e reti cellulari);
- **Propagazione multipath**: i segnali radio si riflettono, arrivando alla destinazione a tempi leggermente diversi.

Diversi tipi di trasmettitori sul mezzo wireless possono dedicare più energia alla trasmissione del singolo bit: questo solitamente si traduce in una maggiore sicurezza della trasmissione effettiva del bit, ma di contropartita in una riduzione del bitrate (al pari dell'energia usata).

1.0.4 Metriche per la qualità del segnale

Abbiamo a disposizione 2 metriche principali per la valutazione della qualità del segnale su un mezzo:

- **SNR** (*Signal-to-Noise Ratio*): rappresenta il rapporto fra la potenza del segnale ricevuto e la potenza del rumore ricevuto, dove il rumore è l'interferenza che si aggiunge al segnale in fase di trasmissione e propagazione. Chiaramente, più l'SNR è grande, maggiore è la qualità del mezzo;
- **BER** (*Bit Error Rate*): rappresenta la frequenza di bit persi sul mezzo. Chiaramente, più il BER è piccolo, maggiore è la qualità del mezzo.

Esiste quindi una relazione fra potenza spesa per bit, SNR e BER, che è sostanzialmente:

$$\text{aumenta potenza per bit} \rightarrow \text{aumenta l'SNR} \rightarrow \text{diminuisce il BER}$$

Nel caso non si possa aumentare la potenza per bit, o comunque l'SNR sia fisso, è invece necessario agire sul protcollo di livello fisico usato per raggiungere i requisiti sul BER (chiaramente perdendo in throughput).

Infine, notiamo che l'SNR può cambiare dinamicamente nel caso di reti mobili (cioè quando gli host si spostano all'interno della rete). Chiaramente, può essere utile in questo caso (ma anche nel caso di reti wireless non mobili) prevedere sistemi *adattivi*, che modulano il bitrate sulla base dell'SNR effettivo rilevato.

1.0.5 Problema del nodo nascosto

Per farci un'idea del tipo di problematiche che si possono incontrare sfruttando il mezzo wireless, ipotizziamo la seguente situazione:

- Un nodo B può sentire altri due nodi, A e C;
- I nodi A e C non possono sentirsi fra di loro (magari per via di un ostacolo, o solamente per causa della perdita di segnale causata per path loss).

Il risultato di questa situazione è che A e C possono provare contemporaneamente a parlare con B, e non hanno modo di rilevare tale collisione, in quanto non possono parlare fra di loro.

1.1 IEEE 802.11 Wireless LAN

Lo standard **IEEE 802.11 Wireless LAN**, noto anche col nome commerciale *Wi-Fi* è stato uno dei primi standard (dal 1999) per la trasmissione di dati su mezzo wireless fra computer (in un epoca dove le reti mobili erano già distribuite).

Tutti usano *CSMA/CA* per il MAC, e prevedono modalità sia *ad infrastruttura* che *ad hoc*.

Il bitrate andava da 10 Mbps circa delle prime versioni, ai 46 Gbps di WiFi 7.

Le frequenze operative sono state storicamente 2 principali:

- 2.4 GHz ISM, una banda pubblica che veniva largamente utilizzata;
- 5 GHz, introdotta per risolvere i problemi di affollamento dati dalla banda a 2.4 GHz.

Il raggio di copertura va dai 30 ai 70 metri circa, con l'eccezioni delle reti medium range (le af e le ah) che si trovano intorno al kilometro (sacrificando però il bitrate, che è intorno ai 350 Mpbs). Per riuscire a raggiungere tali raggi di copertura si trasmette su frequenze che vanno dai 54-790 MHz (vecchie frequenze televisive) per ah, e 900 MHz per af.

La configuraione ad infrastruttura base del Wi-Fi si basa su *access point*, detti nella nomenclatura **BSS** (*Basic Service Set*) (anche se noi li chiameremo comunque *access point*), a loro volta collegati a switch o router che quindi instradano i dati sulla rete internet. Gli host parlano quindi coi BSS, e attraverso questi raggiungono la rete Internet. Nel caso di Wi-Fi in modalità ad hoc, invece, gli host parlano direttamente fra di loro.

1.1.1 Associazione agli access point

La banda dedicata al Wi-Fi viene suddivisa in canali a frequenze diverse: per ogni AP, l'amministratore dovrà scegliere una banda. Nulla nega che pià AP adiacenti abbiano collisioni (scelgano la stesso canale).

In ogni caso, per potersi connettere un host Wi-Fi dovrà **associarsi** con un AP. Ciò che farà sarà *scannerizzare* i diversi canali, mettendosi in ascolto di frame *beacon* (dalla parola inglese per *faro*). I frame beacon contengono il nome dell'AP (**SSID**), e l'indirizzo **MAC** dell'access point. Notiamo che possono venire rilevati più di un AP su diversi canali, ed è quindi necessario un criterio di scelta: quello più semplice è scegliere l'access point che ha potenza maggiore. A questo punto si può portare avanti un passo di **autenticazione**, e quindi provvedere a passare sulla rete Internet, ad esempio ottenere un indirizzo IP tramite DHCP.

1.1.2 Accesso mulitplo IEEE 802.11

Lo scopo del **MAC IEEE 802.11** è evitare le *collisioni*, cioè situazioni in cui 2 o più nodi trasmettono contemporaneamente. 802.11 sfrutta il CSMA/CA (non CSMA/CD come Ethernet!), già visto in 13.1.5, per il rilevamento preventivo sul mezzo condiviso prima delle trasmissioni, e il successivo recupero dopo collisioni.

In particolare, il funzionamento del trasmettitore sarà:

1. Il trasmettitore aspetta che il mezzo resti libero per un certo tempo detto **DIFS** (*Distributed InterFrame Space*);
2. Se il canale è rilevato libero si trasmette l'intero frame;
3. Se il canale è rilevato occupato allora:
    - Si imposta un tempo di backoff casuale;
    - Si aspetta tale tempo di backoff;
    - Se non si riceve un ACK si aumenta l'intervallo di backoff e si torna al passo 3.

Il ricevitore si comporterà invece come segue:

1. Se il nodo viene ricevuto in sicurezza (senza collisioni), si aspetta un certo tempo detto **SIFS** (*Short InterFrame Space*);
2. Si invia l'ACK.

Il SIFS deve essere minore del DIFS: questo è per avvantaggiare il ricevitore in caso di collisioni (cioè avvantaggiare trasmissioni già avvenute a metà).

1.1.3 Scelta del backoff

Per l'intervallo di backoff, questo viene scelto uniformemente fra 0 e $CW - 1$, dove CW è la cosiddetta **contention window**. Inizialmente, CW vale $CW_{\min}$. Per ogni ACK perso CW viene moltiplicato per 2, fino ad un certo valore $CW_{\max}$.

1.1.4 Differenza fra MAC Ethernet e 802.11

Notiamo ulteriormente le differenze fra i protocolli MAC di Ethernet e 802.11. Nel caso di 802.11, sfruttiamo *collision avoidance*: prevediamo che sarà impossibile rilevare collisioni in corso sul mezzo wireless, e fondiamo il nostro rilevamento errori su segnali di ACK. Ethernet, di contro, implementa *collision detection*: le collisioni vengono rilevate elettricamente attraverso segnali di jam.

Questo ci permette di risolvere il problema del nodo nascosto, introdotto in 27.0.5: se il nodo centrale (avevamo detto C) non invia ACK agli altri nodi, questi sanno che una collisione è avvenuta, e possono entrare nelle loro fasi di backoff senza dover direttamente parlare l'uno con l'altro.

1.1.5 Virtual carrier sensing

Una soluzione usata in 802.11 è il **virtual carrier sensing**. In questo caso l'idea è che il trasmettitore *"prenoti"* il canale per l'invio di frame dati, usando frame di *prenotazione*.

1. Il primo frame inviato è l'**RTS** (*Request-To-Send*), inviato via CSMA all'AP;
2. L'AP risponde con un frame **CTS** (*Clear-To-Send*). Questo CTS ha 2 scopi:
    - Viene ricevuto dall'host originale, che sa quindi di poter iniziare la sua trasmissione di dati;
    - Anche gli altri host collegati all'AP rilevano il segnale, e differiscono le loro comunicazioni fino al termine di quella dell'host originale.
      Per fare ciò ci dotiamo di un nuovo timer, detto **NAV** (*Network Allocation Vector*), che viene caricato col tempo durata del frame CTS originale. Finché il NAV è attivo, ogni successiva trasmissione viene differita.

1.1.6 Frame IEEE 802.11

Vediamo quindi la struttura di un **frame IEEE 802.11**:

```
2 byte         2 byte    6 byte  6 byte  6 byte
frame control  duration  addr. 1 addr. 2 addr. 3
2 byte      2 byte  0 - 2312 byte 4 byte
seq control addr. 4 payload       CRC
```

Notiamo la presenza dei capmi:

- Il `frame control` contiene informazioni sulla versione del protocollo, tipo del frame, ecc...
- Il campo `duration` contiene la durata della trasmissione richiesta nel caso di CTS o RTS;
- Si hanno poi 4 campi di indirizzo:
    1. Indirizzo MAC dell'host o dell'AP che deve ricevere il frame;

2. Indirizzo MAC dell'host o dell'AP che invia il frame;
3. Indirizzo MAC dell'interfaccia router a cui l'AP è agganciato;
4. Usato in modalittà ad hoc.

-