MSA - Wireless LAN

- LLC è il Logical Link Control, del quale non ci occuperemo, e che il protocollo 802.11 ha in comune con tutti gli altri protocolli della famiglia 802.*. Dal punto di vista di *chi sta sopra*, non importa chi sta sotto in quanto LLC agisce da strato di trasparenza
- Il protocollo nsce con l'obiettivo di realizzare una rete wireless di tipo locale che non usasse una porzione dello spettro non regolamentata, dunque senza la richiesta di licenze. La banda inizialmente individuata era attorno ai 2.4 GHz, con un throughput nominale di 2 Mbps. Requisito iniziale era che il canale wireless venisse utilizzato per la gestione di dati senza vincoli stringenti sul ritardo massimo di trasmissione, anche se successivamente vengono aggiunte delle garanzie sul ritardo massimo

Vocabolario

- **STA:** station, indica un'entità che ospita il protocollo, parte fisica e parte MAC
- **BSS:** insieme di nodi che condividono un canale per interagire tra di loro, sotto il controllo di un singolo coordinatore, AP. I nodi non parlano tra di loro, ma unicamente con l'AP
- **AP:** access point, coordinatore all'interno del BSS
- **IBSS:** insieme di nodi che condividono un canale per interagire tra di loro senza il controllo di un coordinatore (es. P2P, Bluetooth). I nodi parlano tra di loro
- **ESS:** BSS connesse tra di loro tramite DS (Distribution System), permettono ad un singolo nodo di utilizzare il protocollo 802.11 per parlare con un nodo appartenente ad un BSS differente. Proposta standardizzazione con protocollo 802.11f, ma successivamente abbandonato. Ad oggi ogni produttore costruisce il suo sistema di distribuzione

Mobilità

- **BSS/IBSS:** fin quando sono nella portata dell'AP o degli altri partner, sono libero di cambiare la mia posizione nello spazio
- **ESS/DS:** se il nodo che si sposta percepisce la degradazione del segnale della BSS a cui è connesso, inizia il processo di esplorazione dell'ambiente circostante per rilevare presenza di altri BSS tramite messaggi *beacon*. Rilevata la presenza di una rete di qualità adeguata il nodo manda una richiesta di associazione alla rete, che può essere raccolta da più AP, se presenti. Ricevuta risposta, la stazione stabilisce la connessione con il nuovo BSS. A questo punto il nuovo AP manda al vecchio AP la comunicazione di presa in carico del nodo mobile, per l'eventuale rilascio di risorse

Trasmissione

- Trasmissione affidabile ed atomica, dall'inivio del pacchetto alla ricezione dell'ACK
- **Two-way:** Data-ACK
- **Four-way:** Data-RTS-CTS-ACK

Composizione Pacchetto

- Versione generale del protocollo, non tutti i campi presenti necessariamente
- Sempre presenti **Frame Control** e **Duration**
- **Frame Control:** lunghezza *2 byte*
  - **Protocol Version (2 bit):** indicano la versione del protocollo. Sempre 00, per la versione h si indica 01
  - **Type (2 bit):** indica il tipo del pacchetto
    - **Controllo:** legati al meccanismo di associazione alla rete
    - **Gestione:** ACK, RTS, CTS
    - **Dati:** pacchetto dati vero e proprio
  - **Subtype (4 bit):** sottotipi all'interno dello stesso tipo
  - **To DS/From DS (2 bit):** danno informazioni sulla gestione dei quattro indirizzi del pacchetto
    - **(0, 0):** comunicazione direttamente dai nodi senza ifrastruttura, *IBSS*
    - **(0, 1):** BSS, comunicazione da AP a stazione ricevente. Mittente fisico è AP, mittente logico è stazione mittente, destinatario logico e fisico è la stazione ricevente
    - **(1, 0):** BSS, comunicazione da stazione mittente ad AP. Mittente fisico e logico coincidono, mentre AP destinatario fisico e stazione ricevente destinatario logico
    - **(1, 1):** EBSS, sistema distribuito realizzato tramite comunicazione wireless tra gli AP. In questo caso ho necessità di quattro indirizzi in quanto destinatario logico e fisico, come il mittente logico e fisico, sono quattro entità differenti
- **Duration/ID:** durata della trasmissione del pacchetto

DCF (Distributed Coordination Function)

- Tutte le stazioni competono alla pari, anche l'AP
- Essendo un protocollo a contesa, è basato sullo schema SCMA/CA
- **Carrier Sensing:** tento di trasmettere solamente se il canale non è occupato. Ascolto dello stato del canale può avvenire in due modi
  - **Fisico:** se rilevo la presenza di un segnale sul canale wireless su cui sono sintonizzato
  - **Virtuale (NAV):** anche se non ascolto nulla, se sono stato informato che c'è una trasmissione in corso, ho memorizzato quest'informazione all'interno del *NAV* e considero il canale occupato fin quando il valore del contatore non arriva a 0
- **Collision Avoidance:** entra in gioco quando il canale viene percepito libero, in modo fisico o virtuale
  - Una stazione non tenta subero di occupare il canale, ma aspetta un determinato tempo DIFS. Se il canale risulta libero anche durante l'attesa, al termine inizia a trasmettere
  - Se invece mentre la stazione è in attesa che trascorra l'intervallo DIFS sente il canale occupato:

        - Una volta sentito nuovamente il canale libero aspetterà come sempre un tempo DIFS
        - Sommo un altro intervallo di durata variabile (*back-off*) random, in quanto altre diverse stazioni potrebbero aver sperimentato questa situazione
        - Chi estrae il valore più piccolo vince la competizione ed avrà il diritto di tasmettere
        - Tutti gli altri, congeleranno il valore del proprio timer, e riprenderanno il conteggio sempre dopo aver sentito il canale libero, a cui va sempre aggiunto il tempo DIFS
        - **NB:** se due stazioni *estraggono* lo stesso valore, trasmetteranno in contemporanea causando una collisione. Non ricevendo ACK, tenteranno la ritrasmissione, perdendo però il *vantaggio* di prima con il congelamento del valore del timer
    - Ottenuto il diritto di trasmettere lo scambio dati è affidabile, oltre che atomico. Atomocità garantità dall'intervallo *SIFS* che si attende prima di inviare l'ACK. SIFS < DIFS, in modo che nessun altro possa intromettersi nella comunicazione sentendo il canale libero
    - In ogni caso, durante la trasmissione dei dati tutte le altre stazioni che ricevono il pacchetto aggiorneranno il loro NAV

DCF con RTS/CTS

- Stessa logica di prima, ma dopo aver sentito il canale libero anche per temo DIFS, invio prima RTS
- Dovendo essere anche questa trasmissione atomica, dopo l'inivio del CTS tutti i successivi pacchetti verranno inviati dopo l'attesa di un tempo SIFS
- Alla ricezione di ogni pacchetto CTS/RTS/Data, tutte le altre stazioni avranno l'informazione su quanto tempo manca ancora per completare la trasmissione, aggiornando in questo modo il proprio NAV

DCF con frammentazione

- La frammentazione viene avviata se il pacchetto da inviare è troppo grande o se il tasso di errore del canale è troppo alto
- In questo caso, la comunicazione deve continuare ad essere atomica
- Tra l'inivio di Data+ACK, il tempo di attesa è SIFS

Point Coordinatio Function

- Nel meccanismo DCF c'è il meccanismo di fairness ce rende improbabile che con il passare del tempo l'attesa si prolunghi
- Ma non è possibile dare una certezza sul tempo massimo di attesa prima della trasmissione del pacchetto
- Lo schema **PCF** è applicabile solamente in situazione con infrastruttura

- Organizzo l'asse dei tempi in intervalli consecutivi etichettati con **CFP**, la cui durata può essere decisa dall'AP. Divido osngi singolo intervallo in:
  - **DCF:** l'accesso al canale avviene in modalità a contesa
  - **PCF:** l'accesso al canale avviene in modalità polling. L'AP raccoglie le richieste da parte dei nodi, e durante questo intervallo interpellerà le varie stazioni per il permesso alla trasmissione
- La lunghezza totale dell'intervallo *CPF* dice quanto tempo, chi vuole trasmettere in modalità PCF, deve aspettare prima che gli venga assegnato il diritto di trasmettere. Più lungo l'intervallo, maggiore la quantità di dati che si accumulano al mittente in attesa di trasmissione. La lunghezza dell'intervallo *CFP* e e la frazione dedicata alla trasmissione *PCF* vengono negozioate tra l'AP e le stazioni che vogliono utilizzare questa modalità
- All'interno dell'intervallo *PCF*, tra una trasmissione e l'altra viene atteso il tempo SIFS
- Se l'AP non riceve risposta entro l'intervallo PIFS > SIFS, interpella la stazione successiva
- L'avvio di ogni intervallo di trasmissione *PCF* è segnalata dal messaggio di beacon, emesso ad intervalli regolari dall'AP
  - L'AP, dovendo contendere con gli altri, potrebbe trovare il canale occupato prima di trasmettere il proprio beacon
  - Caso peggiore è il caso in cui la trasmissione che rende il canale occupato inizi un'istante prima del periodi di invio del beacon. In questo caso l'attesa massima sarà quella necessaria al trasferimento di un pacchetto di 2000 byte
- Tramite il beacon generato, tutte le altre stazioni non interessate al tipo di trasmissione aggiorneranno il loro NAV
- Se una stazione arriva successivamente, e dunque non ha aggiornato il NAV, non riuscirà a sentire il canale libero per un tempo DIFS dunque si asterrà dal trasmettere

Sincronizzazione orologi

- Tutte le stazioni devono essere in accordo sullo scorrere del tempo
- **Infrastruttura (BSS):**
  - Tutte le stazioni sono tenute ad aggiustare il loro orologio su quello dell'AP
  - Informazione che viene diffusa tramite il messaggio di beacon ad intervalli regolari, 100 millisecondi per le implementazioni attuali
  - L'inivio del beacon può essere ritardato, ma in ogni caso il valore dell'orologio inglobato è quello attuale e non quello teorico
- **Senza Infrastruttura (IBSS):**
  - Ogni stazione, in base al proprio orologio interno, ad intervalli regolari cerca di inviare un beacon
  - Tutte cercano di trasmettere in contesa e, chi vince, manda il valore del suo orologio che viene recepito dagli altri
  - Non c'è un orologio privilegiato, ed a causa di ciò l'avanzamento del tempo è un po meno uniforme rispetto al caso precedente

Risparmio energetico

- Si basa sul meccanismo fisico di operare delle schede di rete. Anche se inattiva, dunque ne in ricezione e ne in trasmissione, il consumo energetico è molto elevato. Per questo motivo le schede di rete sono tipicamente dotate della modalità sleep. In questo stato tutti i circuiti sono spenti, tranne quelli relativi alla gestione del clock
- L'idea è che se una scheda di rete non ha nulla da trasmettere si mette in modalità sleep, svegliandosi periodicamente per capire se ci sono dati destinati a questa stazione
- Chi ha dati da trasmettere, in attesa che il destinatario si risvegli, deve mantenere al suo interno i dati da inviare
- Questo comporta un ritardo nell'invio dei dati, ed è un compromesso da accettare per poter attuare la politica di risparmio energetico

Risparmio energetico con infrastruttura (BSS/PCF)

- Dati memorizzati nell'AP in attesa di essere trasmessi
- AP ha conoscenza, tramite mappa, di tutte le stazioni che hanno deciso di attuare la politica di risparmio energetico
- Meccanismo realizzato tremite beacon che contiene due mappe:
  - **TIM:** mappa che segnala la presenza di dati per le singole stazioni
  - **DTIM:** mappa che segnala la presenza di dati di tipo broadcast, destinati a tutte le stazioni. Questo tipo di mappe vengono inviate con una spaziatura temporale maggiore rispetto alle mappe *TIM*
- Stazione che mette in atto una politica di risparmio energetico è tenuta a svegliarsi nell'istante di tempo in cui l'AP potrà trasmettere il suo beacon. Se la trasmissione dovesse ritardare, la stazione non può tornare in *sleep* prima della ricezione del beacon
- Se stazione si riconosce nella mappa, segnala all'AP di essere sveglia in modo da poter avviare lo scambio di dati e successivamente ritorna in modalità *sleep* fino all'arrivo del prossimo beacon

Risparmio energetico senza infrastruttura (IBSS/DCF)

- Sincronizzazione degli orologi fattore importante
- Stazioni si svegliano in parallelo e cercano di inviare segnale di beacon. Chi vince la contesa invia il proprio segnale che, ricevuto da tutti, segnalerà l'inizio della *ATIM Window*
- In questa finestra di tempo, tutte le stazioni sono tenute ad essere accese e sono autorizzate ad inviare la loro mappa di dati destinati ad altre stazioni
- Allo scadere dell'ATIM Window, le stazioni che hanno qualcosa da inviare/ricevere rimarranno attive per procedere con la trasmissione dei dati. Tutte le altre torneranno in sleep fino all'invio del prossimo segnale di beacon

Paradosso risparmio energetico

- Trasferimento TCP di 500 Kb tramite link wireless con risparmio energetico abilitato

- Tempo tra due beacon è 100ms
- **RTT 25 ms**
  - RTT lontano dal periodo di risveglio, quindi impiego più tempo prima di arrivare alla saturazione del canale
- **RTT 75 ms**
  - RTT molto vicino al periodo di risveglio, impiego molto meno tempo per la saturazione del canale
- Se sommo tutti i tempi in cui una scheda di rete dovrà essere accesa per consetire l'inivio e la ricezione dei dati, nel primo caso la somma dei tempi saà maggiore del caso in cui la scheda di rete sarebbe rimasta accesa in assenza della politica di risparmio energetico
- Quando si vogliono ottimizzare le prestazioni di un sistema costituito da una stratificazione di livelli, ognuno dei quali sfrutta le funzioni offerte dai livelli sottostanti, cercare di raggiungere degli obiettivi di efficienza ed ottimizzazione lavorando solo ad un livello ignorando le possibili interazioni con gli altri livelli, rischia di essere una scelta miope e non efficace

Nuovi scenari - 802.11h

- Nuovi scenari emersi con il tema dell'IoT
  - Ambienti esterni
  - Velocità di trasmissione dei dati minore (kb/s)
  - Entità stazionarie o poco mobili
  - Grande numero di stazioni, ordine delle migliaia
  - Alimentazione a batteria e poca manutenibilità
  - Comunicazione verso un AP che funge da punto di collezione dei dati
- Problemi della configurazione attuale
  - La configurazione attuale non consente un numero superiore a 2007 stazioni connesse allo stesso AP
  - Il meccanismo di risparmio energetico non è ottimale in certe situazioni, in quanto 802.11 come visto fino ad ora è prensato per uno scenario con un alto throughput
  - Distanze da percorrere tipicamente brevi pensando a scenari indoor

802.11h - Bande trasmissive sotto al Ghz, per una maggiore penetrazione e propagazione rispetto alle banda 2.4/5 GHz classiche

Incremento stazioni connesse

- Attuale formato mappa TIM è composto da 5 byte che danno informazioni sulla mappa. Il campo *length*, composto da un byte, ha lunghezza massima 255 e la lunghezza massima della bitmap è di 251 byte
  - 4 byte persi per il campo stesso ed i tre successivi
  - 251 x 8 = 2008
  - Bit 0 non viene utilizzato, dunque ritrovo il valore 2007

- Nuovo formato della TIM aumenta il numero di byte per il campo *lenght* da 1 a 2, portando la lunghezza della bitmap a 1018 byte
  - Possibilità di codificare poco meno di 10000 stazioni
  - In schemi più sofisticati è possibile estendere il numero di stazioni rappresentabili facendo un uso non piatto della bitmap
- Modifica della TIM ha richiesto la modifica dell'interpretazione del campo *Duration/ID*, in quanto se utilizzato nel secondo modo (quando il bit 14 e 15 valgono 1) indica l'ID da associare alla stazione. Nella versione h, come visto, questo valore ha un range maggiore rispetto alle altre versioni

Short Header

- Introdotto un nuovo header con lunghezza minore del classico
  - **Frame Control -> Protocol Version:**
    - **0, 0:** vecchio header
    - **1, 0:** nuovo short header
  - Essendo una situazione statica, negli scenari descritti tipicamente mittente e destinatario logico e fisico coincidono, potendo utilizzare solamente due indirizzi
  - Durante il preambolo iniziale ci si conosce reciprocamente, si assegnano i ruoli del mittente e destinatario logico e fisico, ed una volta memorizzata questa informazione cessa la necessità di ripeterla
  - Il nodo destinatario o mittente, non AP, può essere individuato con un campo indirizzo di dimensione ridotta di soli 2 byte
  - Mettendo assieme queste possibili riduzioni, l'header si riduce notevolmente
  - Può anche essere omesso il campo *Duration*, in quanto il carrier sensing virtuale viene eseguito in modo diverso

Riduzione probabilità collisioni

- Partiziono stazioni in gruppi distinti e canale viene diviso in slot temporali consecutivi, assegnando uno slot ad ogni gruppo
  - Ogni stazione che fa parte di un gruppo è autorizzata a provare ad accedere al canale solo nello slot di pertinenza per il gruppo
  - L'accesso avviene in modalità DCF a contesa
  - Ripartizione dei gruppi e del canale trasmessa in broadcast tramite segnale di beacon
  - Riduco il numero di stazioni che possono contemporaneamente provare ad accedere al canale riducendo la contesa, ma per essere utilizzato questo schema richiede una sincronizzazione precisa tra tutte le stazioni, in quanto ognuna dev avere una nozione precisa di quando scatta e quando scade lo slot in cui è autorizzata a trasmettere
- Partiziono lo spazio attortno all'AP in settori
  - Tempo viene organizzato in slot successivi

- AP concede il diritto di trasmettere in maniera circolare solo alle stazioni appartenenti ad un determinato settore
- Stazioni che fanno parte dello stesso settore sono in grado di ascoltarsi l'uno con l'altra, riducendo la probabilità di collisioni ed aumentando il throughput ed il risparmio di energia