MSA - 10.03.2021

MACA

L'ambito che consideriamo è quello di un canale wireless. Ieri abbiamo detto che quando si utilizza un canale wireless emergono alcuni problemi come il terminale nascosto, che rendono nel caso di protocolli basati su contesa nell'uso della risorsa, possono rendere problematico la piena realizzazione dei meccanismi alla base di questi protocolli: meccanismi di ascolto dell'occupazione del canale e della presenza di collisioni. Avevamo evidenziato la presenza di questi problemi che si verificano, come rimarcavo ieri, in caso di protocolli basati su contesa nell'uso del canale da parte delle varie entità interessate. Un protocollo di gestione della contesa che cerca di risolvere questo è quello che vedete nelle slide, **MACA (Multiple Access with Collision Avoidance).**

Diamo una figura per illustrare come opera, poi vi do una spiegazione più precisa usando una macchina statica. L'idea di fondo è che la trasmissione vera e propria di dati è preceduta da un preambolo, in cui chi è interessato a trasmettere manda un pacchetto RTS (Request to Send). L'invio del pacchetto avviene usando un meccanismo di competizione, se rileva il canale non occupato invia il pacchetto. Il pacchetto contiene in linea di principio chi è il mittente, chi è il destinatario della comunicazione e quanto tempo durerà la comunicazione se avrà luogo. Il pacchetto si diffonde nello spazio libero, viene raccolto da tutti i nodi nel raggio di percezione del segnale. Tra tutti gli ascoltatori uno si riconoscerà come il destinatario della comunicazione, che invia il pacchetto CTS (Clear to Send) che contiene l'inverso degli indirizzi iniziali. Questo pacchetto replica l'informazione sulla durata della comunicazione. Questo pacchetto viene ascoltato da tutte le stazioni nella portata del segnale emesso da B. Chi si riconosce come il destinatario viene autorizzato ad inviare i dati. Tutte le stazioni che si riconoscono non destinatarie si bloccano per tutta la durata indicata nel pacchetto. Anche se non sono in grado di ascoltare fisicamente la presenza della comunicazione, evitano di impegnare il canale per tutta la durata indicata nel pacchetto.

Vediamo un esempio. Risolve il problema del terminale nascosto. A manda il messaggio di richiesta di invio. Per come sono disposti i nodi, la comunicazione tra A e B non può essere ascoltata da C, che sentirebbe il canale libero ma causerebbe una collisione. In questo modo anche se non può sentire il segnale di A può sentire il segnale di B, quindi virtualmente viene informato che c'è una comunicazione in atto e non disturba la comunicazione anche se non la sente fisicamente. In maniera analoga si risolve quella del terminale esposto. La stazione B manda il segnale RTS, ascoltato anche da C. La stazione A invia il segnale CTS a B, ma viste le distanze relative il segnale non arriva a C, che non ascoltando il segnale deduce che l'eventuale comunicazione che avviene C non è in grado di disturbare, e di conseguenza C si sente ad avviare con altri partner una comunicazione. Per essere un po più precisi abbiamo le macchine a stati semplificate. Mittente da attesa, appena c'è un pacchetto da inviare, viene emesso il segnale di RTS. DA questo stato si esce perché scade un timeout senza aver ricevuto nulla; se scade, la macchina riprova ad inviare il segnale di RTS.

Oppure, caso migliore, fortunato, si riceve il pacchetto di CTS, ed in questo caso la macchina invia il pacchetto dati e si mette in atteso di un ACK. Da questo stato di attesa si può uscire se ricevo l'ACK ritorno allo stato iniziale. Se invece scade un timeout senza ricevere l'ACK o si riceve un ACK negativo, allora si ricomincia la storia.

Lato destinatario di una comunicazione, se sono inattivo nel momento in cui ascolto un messaggio RTS indirizzato a me stesso invio il messaggio di CTS, e rimango in attesa di ricevere il vero e proprio messaggio inviato dal mittente. Mentre sono in questo stato può succedere che mi arrivi un messaggio di richiesta di invio da un'altra stazione, interessata a comunicarmi qualcosa. A questo punto la mia risposta è che sono occupato. Quello che può succedere è che se ricevo i dati non corrotti, invio l'ACK e ritorno allo stato iniziale. Se scade un timeout senza aver ricevuto nulla o se ricevo qualcosa ma è corrotto, mando un ACK negativo. Per completare il discorso ci vorrebbe la macchina a stati di chi non è ne mittente ne destinatario, ma la lascio al vostro ingegno.

Commenti su questo protocollo. E' il protocollo usato all'interno del protocollo WiFi 802.11. Ha un impatto positivo dal punto di vista della risoluzione dei problemi, ma non è esente da problemi. L'invio dei pacchetti RTS avviene in competizione, quindi nel caso dell'invio degli RTS si presentano i problemi che il protocollo vuole risolvere. Chi invia RTS invia con la percezione del canale libero, e se inviano in contemporanea la storia si ripete. Però c'è da dire che la probabilità che questo succeda è piccola, in quanto si tratta di pacchetti molto più piccoli di un pacchetto dati mediamente; se anche questo evento dovesse verificarsi, si tratta di pacchetti di pochi byte. La perdita di capacità trasmissiva di utilizzazione effettiva del canale è relativamente piccola. Altra cosa problematica, sono pacchetti che circolano sulla rete, è un overhead che aggiungo a quella che dovrebbe essere l'utilizzazione ottimale del canale. Ma è piccolo il rapporto alla comunicazione che seguirà. Nel protocollo 802.11 l'utilizzo di MACA è concesso solamente se la dimensione dei pacchetti dati è superiore ad una certa soglia.

Due parole sulle altre tre classi di protocolli di comunicazione. Quelli statici, quelli casuali a contesa e quelli dinamici basati su meccanismi di prenotazione. Questi ultimi abbiamo un access point che fa da master del protocollo, che raccoglie le richieste dei permessi di trasmettere, e poi seguendo una sua politica emette uno ad uno ai vari richiedenti i permessi di trasmettere. Questo è il meccanismo di condivisione del canale wireless usato dai protocolli della famiglia Bluetooth. In questo caso c'è un protocollo di elezione del master, in quanto di base la rete è P2P. A parte questo non c'è altro da dire. Piccolo riassunto di quanto detto ieri. Nel caso di protocolli di accesso casuale non si può fare Collision Detection. Se voglio ridurre le collisioni posso solo inserire un ritardo nella comunicazione se il canale viene percepito come occupato. Solo nel caso di reti che non usano meccanismi di regolamentazione nell'accesso abbiamo il problema del terminale nascosto ed esposto. Il protocollo MACA in qualche modo risolve queste problematiche. Dal punto di vista della versatilità i protocolli con polling sono applicabili solo ad un'infrastruttura con un terminale che fa da master. Gli algoritmi casuali invece sono applicabili in caso ed in assenza di infrastruttura. Dal punto di vista delle tipologie di traffico, protocolli statici o di tipo polling sono adeguati a trasmettere traffico che ha dei vincoli stretti sul ritardo massimo, potendo dare delle garanzie. I protocolli a contesa sono per un traffico meno regolare e più "disordinato". La letteratura di 30 anni fa, quando è

esplosa l'esigenza dei protocolli wireless, ci sono centinaia di lavori che propongono varie tipologie di protocolli wireless.

Piccola nota sulle tecniche di condivisone di tipo spaziale. Si affianca ad una delle altre tre tecniche per aumentare il grado di parallelismo nell'uso di una certa banda di frequenze scelta per realizzare una comunicazione wireless. L'idea è di suddividere lo spazio in regioni continue diminuendo lo spazio che ricopre un segnale, in modo da aumentare il numero di utenti. In assenza di meccanismi adeguati però la situazione è difficilmente accettabile. Se ritaglio il mio spazio in questo modo, limito anche le libertà di movimento in attesa di meccanismi dedicati. Perché questo possa funzionare, al di là del fatto che oltre un certo limite nella suddivisione non si può andare in funzione della velocità di spostamento degli utilizzatori, se non voglio che ponga una limitazione alla libertà di movimento devo prevedere dei protocolli che prevedono lo spostamento tra una regione e l'altra, senza che una connessione che avevo in corso si interrompa. Meccanismi di questo tipo sono stati previsti, e vengono chiamati di handoff tra una regione coperta da un certo canale ed una regione adiacente coperta da un canale diverso.

In una rete omogenea in cui le varie regione dello spazio sono coperte dallo stesso tipo di infrastruttura, il passaggio avviene in base al riconoscimento della qualità del segnale. Nelle zone di confine tra celle è percepibile il segnale di entrambe le stazioni. Muovendomi osservo che la qualità del segnale si attenua da una parte e migliora dall'altra. C'è una zona di confine in cui si riescono a percepire entrambi i segnali, e posso effettuare il passaggio di mano tra vecchio e nuovo access point senza che la connessione crolli. L'ampiezza temporale della zona di confine dipende dalla velocità di spostamento e dalla potenza del segnale. Nella progettazione delle reti bisogna trovare un compromesso adeguato tra potenza del segnale e velocità che si intende supportare per gli utilizzatori della rete. Questo meccanismo pone un limite alla dimensione minima che le celle devono avere, perché se scendo sotto una certa dimensione e la velocità supera una certa soglia, il sistema non riuscirebbe a stare dietro ai movimenti. Giusto per avere un'idea delle entità in gioco e del tempo necessario per realizzare lo scambio tra le due stazioni radio. C'è comunque un gap tra reti locali wireless e reti wireless geografiche. Le varie tipologie di reti cellulari si stanno via via unificando.

Wireless LAN - L05

Abbiamo chiuso il capitolo generale ed apriamo subito un altro capitolo in cui ci dedichiamo ad andare in profondità sul protocollo WLAN su rete locale, che ha copertura del centinaio di metri. Protocolli di questo tipo ne sono stati proposti diversi ma ne emerso uno, di cui ci occuperemo. Rispetto al nostro schemino a blocchi ci muoviamo nell'ambito delle comunicazioni wireless, ma affrontiamo uno standard di fatto adottato universalmente. Quando si definisce uno standard l'oggetto di interesse di questo standard se vediamo la pila è quello che vedete rimarcato qui. Ci si deve occupare della definizione della parte fisica e della parte logica di gestione del canale. La parte fisica si può articolare in livelli ceh dipendono strettamente dal mezzo fisico che può essere utilizzato, e poi uno

strato superiore che deve garantire ai livelli sopra ancora, e ai livelli superiori abbiamo il livello per la condivisone del canale e per l'interfacciamento con il livello superiore.

Di tutto questo, dell'ultima parte non ce ne occuperemo. Lavoriamo con i bit, e come questi si materializzano in onde elettromagnetiche esula dai nostri interessi. Di questo non parliamo. A questo livello rientrano le problematiche relaitve all'uso di infrarossi, radiofrequenze, l'accesso a bande libere o regolamentate ecc. Il livello superiore è quello di cui ci occupiamo. Per restringere il campo parleremo soltanto al sottolivello MAC, quello che definisce le regole per condividere su più richiedenti l'utilizzo del canale. LLC non ne parleremo, è un livello che questo protocollo che fa parte della famiglia 802, è un livello che il protocollo 802.11 ha in comune con tutti gli altri protocolli della stessa famiglia. 802.3, Ethernete, utilizza lo stesso livello LLC. Dal punto di vista di chi sta sopra, non importa chi sta sotto, è invisibile. Una volta deciso che vale la pena imbarcarsi nella realizzazione ed installazione di una rete wifi, ci sono obiettivi di sicurezza in senso sanitario, di salute degli esseri viventi, sia nel senso di protezione dei dati. Questi sono problemi che in una rete wifi si pongono in modo e misura diversa.

Nella prima parte avremo informazioni sulla parte architetturale del protocollo IEEE 802.11. L'ogetto principale di interesse sarà la definizione delle regole di condivisione del protocollo. La sua concezione è nata una 30ina di anni fa, ma la prima standardizzazione si ha nel 1997. Gli obiettivi erano quelli di realizzare una rete wireless di tipo locale che usasse una porzione dello spettro non regolamentata senza richiedere licenze. Quindi la banda in questione inizialmente individuata era in un intorno dei 2.4 Ghz, con la richiesta di supportare comunicazioni con un throughput nominale di 2 Mbps, che all'epoca era una banda adeguata ed in linea con le esigenze del momento. Poi il protocollo si è evoluto nel tempo, avendo varie generazioni, che hanno portato ad una crescita di almeno tre ordini di grandezza. Il requisito iniziale era che il canale wireless venisse utilizzato per la gestione di dati senza vincoli stringenti sul ritardo massimo di trasmissione; in più il protocollo da anche garanzie sul ritardo massimo, utile per segnale vocale o video.

Queste caratteristiche sono realizzate dai protocolli DCF e PCF. Altri aspetti sono quelli di come cercare di fare risparmiare energia ai nodi, di offrire una soluzione al peroblema del terminale nascosto ed esposto. Piccola idea dell'evoluzione nel tempo delle generazioni rispetto a quelle iniziali. Tutti i miglioramenti hanno riguardato la parte fisica del protocollo, mentre la parte logica è rimasta invariata negli anni, fino a pochissimi anni fa quando ci è stato un cambio di requisiti che venivano dall'ambiente circostante che ha richiesto un aggiustamento sostanziale della parte logica, creando una variante solo compatibile con le versioni precedenti da un punto di vista logico.

Questa è una storia che si ripeterà quando definiremo nuovi protocolli. Ogni protocollo definisce un proprio vocabolario. Stesse cose vengono individuate con sigle diverse, giusto per rimanere aderenti al vocabolario dei vari standard. **STA**, station, vuole indicare un'entità, un nodo, che ospita questo protocollo, parte fisica e parte MAC. Con il termine **BSS** si intende un insieme di nodi che condividono un canale per interagire tra di loro realizzato tramite questo protocollo. Questo protocollo può essere utilizzato con infrastruttura, sia in modalità senza infrastruttura, quindi usato anche in modo P2P tra varie entità che concordano nell'usare un certo canale per comunicare tra di loro in

comunicazione diretta. Non viene realizzata comunicazione tra nodi che non sono in contatto diretto. Reti di questo tipo in cui nodi realizzano un canale wireless, solo per parlare tra di loro vengono chiamati **IBSS (Indipendent)**. Più reti di questo tipo possono, più BSS, possono essere connesse per realizzare un sistema più articolato, soltanto nella tipologia con infrastruttura. Le BSS possono essere connesse tra di loro se i vari access point sono connessi tra di loro tramite questa struttura di connessione che permette ad un nodo appartenente ad un BSS di utilizzare il protocollo 802.11 per parlare con un nodo appartenente ad un BSS differente. Questo si dice **ESS**. Potrebbe sembrare ovvio che il protocollo 802.11 definisca anche il protcoollo di realizzazione del sistema di definizione, ed in effetti un tentativo in questo senso c'è stato nella versione 802.11f; versione del protocollo che si preoccupava di definire il meccanismo di colloquio tra gli AP per realizzare il sistema di distribuzione. Per ragioni che non mi sono note il prtocollo è stato abbandonato. Questi sistemi di distribuizione esistono ma di natura non standardizzata. Ogni produttore costruisce il suo sistema di distribuzione.

E' una rete wireless, quindi uno si immagina ch la rete supporti in qualche modo la mobilità dei suoi utilizzatori. Chiaramente la mobilità base, fin quando sono nella portata dell'access point o degli altri partner in P2P, sono libero di cambiare la mia posizione nello spazio. Se le mie esigenze mi portano al di là dei confini di un singolo BSS, se mi trovo in un'architettura RSS entra in gioco la gestione della mobilità tra n BSS all'altra basata su un meccanismo semplice: se il nodo che si sposta percepisce la qualità del segnale che sta degradando della BSS, inizia a fare un processo di esplorazione dell'ambiente circostante per rilevare la presenza di altri BSS, tramite i messaggi beacon inviati da questi ultimi in modo periodico, proprio per consentire ad un ospite che vuole entrare di far conoscere la rete. Una volta rilevata la presenza di una rete di qualità adeguata il nodo itneressato manda una richiesta di associazione alla rete. Questa richiesta viene raccolta, anche da più AP se esistono sulla stessa regione dello spazio. Può arrivare una o più risposte, se ne arriva più di una sceglie in base ad un suo criterio, ed a questo punto sel a cosa va a buon fine si stabilisce la connessione con il nuovo BSS altrimenti il processo continua. NEl momento i n cui la connessione è stat stabilita il nuovo AP manderà al vecchio al comunicazione di presa in caricao del nodo mobile, quindi eventuale rilascio di risorse assegnate a questo ultimo. Questo tipo di mobilità serve a coprire situazioni di questo genere. Tutto questo se mi muovo nell'ambito della sottorete che sta a valle. Se cambio il prefisso di rete che caratterizza la rete di livello 3 a cui sono connesso, a questo punto 802.11 si arrende in quanto non è di sua competenza.

Le estensioni da 20 e passa anni a questa parte non hanno riguardato finora esclusivamente questo livello tranne perla versione H, che introduce delle novità. Un AP se fa da ponte tra una rete wireless ed una rete wirede, su un access point p implementata questa pila protocollare. DA un lato abbiamo il livello 802.11, ma dall'altro avrà l'interfaccia 802.3. MAC realizza il meccanismo di condivisione base. Su questo livello si poggia invece un livello aggiuntivo che è stato concepito per riuscire a dare dei vincoli forti, un upper bound noto sul ritardo massimo che può subire una comunicazione.

L'idea base è che la trasmissione è di tipo affidabile. Si inviano dati e si aspetta di ricevere un ack. In due modalità: quella semplice a due vie, invio il dato ed aspetto l'ack, oppure

protocollo AMAC in cui l'ack è preceduto da RTS e CTS. Dal punto di vista della sicurezza la versione iniziale usava il protocollo WEP, poi si è corso ai ripari. La trasmissione è atomica.

Entriamo nella parte noiosa. Quello che vedete riportato è la versione più generale possibile di un pacchetto, unità di strasmissione gestita dal protocollo. Formata da vari campi, non tutti presenti necessariamente, a seconda della funzione del pacchetto. Sicuramente sempre presenti in tutte le varianti sono i primi quattro byte, i primi due: frame control e duration. Abbiamo tre tipi di pacchetti possibili: controllo, legati ai meccanismi di associazione ad una rete, gestione, come ack, rts, cts, e poi i pacchetti dati. Una cosa che potete notare da questo schema generale è che è prevista i quattro campi indirizzi ognuno di 6 byte. Perché 4 campi indirizzo? E' necessario arrivare a distinguere fino a 4 ruoli diversi. Due vengono tipicamente utilizzati per indicare chi è il mittente logico e chi è il destinatario finale del pacchetto. Accanto a questi due ruoli ce ne sono due che sono il mittente fisico, che sta immettendo il canale wireless, e del ricevitore fisico. Come vedremo questi due ruoli fisici possono cincidere con i ruoli logici, ed in quel caso basta un solo campo per le due situazioni, ma in altre situazioni mittente logico e fisico o destinatario logico e fisico potrebbero non coincidere.

Venendo ai campi evidenziati qui, il primo campo, immaginando che il pacchetto circola sul canale wireless, sono i primi byte che vengono trasmessi e catturati dall'interfaccia wireless di chi ascolta il canale. Servono a dedurre che tipo di pacchetto viene a seguire rispetto a questi primi byte. Questi sono i byte che concretamente servono ad indirizzare la comunicazione di ciò che segue alla macchina a stati che deve decodificare quello che segue. Il secondo è il campo che indica il tempo necessario alla comunicazione di quanto segue, ma può essere anche utilizzato come ID. Il campo dati è quello che, se c'è, porta il carico utile della comunicazione, possiamo arrivare fino a 2300 byte circa, ed il campo sequenze control sono due biti utilizzati per gestire l'eventuale frammentazione. Il protocollo in caso di canale wireless disturbato può decidere di frammentare il pacchetto se supera una certa grandezza, in modo da umentare la probabilità ce almeno uno di questi pacchetti riesca a viaggiare senza danni e riuscire a ridurre la perdita di utilizzazione del canale.

Giusto per chiarire il discorso dei quattro indirizzi. Immaginiamo due BSS, la stazione 2 vuole parlare con la stazione 5. Nel pacchetto che si origina dalla stazione 2 ad AP1, il mittente logico è la stazione 2 che è anche il mittente fisico, in quanto dalla sua interfaccia wireless il pacchetto esce ed arriva ad AP1. Mentre invece il destinatario logico e destinatario fisico, chi nel primo passo riceve il pacchetto, sono identità diverse. Chi deve raccogliere il pacchetto è AP1, mentre il destinatario logico è la stazione 5. In questo caso ne servono 3. Quando mi servono 4 indirizzi? La situazione della comunicazione nel caso in cui il sistema di distribuzione sia realizzato a sua volta tramite una rete WiFi, che non è detto. Potrebbe essere anche basato su cavo, ma nel caso di un DS WiFi mi servono quattro indirizzi. Negli altri scenari ne servono massimo 3.

Per scavare ancora di più nel dettaglio dei singoli cambi, i primi due byte del Frame Control veicolano vari tipi di informazione. I primi due bit dicono al versione del protocollo, e fino alla versione H si era sempre scritto 0. Quando è arrivato H è apparso un 1. Gli altri due bit servono a distinguere i tipi del pacchetto (gestione, controllo o pacchetto dati). All'interno

di questa famiglia, i 4 bit a seguire, servono sui sottotipi. Il secondo byte abbiamo i primi due bit per l'indirizzamento, gli altri bit invece danno informazioni sui frammenti, ritentativo, gestione energetica ecc. Come vengono utilizzti i quattro campi indirizzo, se usati? Se usati, vengono interpretati dai due bit come la tabella disponibile sulle slide.