Università di Pisa

DIPARTIMENTO DI INFORMATICA
Corso di Laurea Triennale in Informatica

Tesi di Laurea Triennale

Rilevazione di disservizi nella connettività di rete

Candidato:
Daniel Casenove

Relatore:
Luca Deri

Anno Accademico 2018/2019

Sommario

Indice

Capitolo 1

Introduzione

Nell'ultimo decennio, con la crescita in popolarità degli smartphone, si é assistito ad un aumento e ad una diversificazione di dispositivi connessi in rete senza precedenti. Una tipica rete non é più composta semplicemente da qualche PC e server, in caso aziendale, ma anche da telefoni, tablet, smart TV, weareables ed elettrodomestici. Inoltre non é poi così raro per un utente possedere più di uno di questi device, aumentando drasticamente il numero di apparecchiature collegate in una singola rete. Secondo previsioni Cisco, il numero di dispositivi connessi a reti IP sarà pari al triplo del numero della popolazione globale entro il 2022[1]. Lo stesso studio riporta un forte cambiamento nel tipo di dispositivi connessi, con dispositivi mobili quali smartphone e tablet, sistemi embedded in TV ed elettrodomestici in costante crescita a discapito dei più tradizionali PC. Viene stimato che, entro il prossimo triennio, il 51% dei dispositivi e connessioni saranno di tipo machine-to-machine, ovvero senza interazione umana, e principalmente costituiti da device IoT. Data la natura dei dispositivi in crescita nelle reti, si osserva anche un cambiamento nel mezzo trasmissivo in favore della connessione senza fili a discapito della connessione cablata.

In contemporanea all'aumento del numero di dispositivi connessi ad Internet si é assistito anche ad un cambio nel paradigma di erogazione di servizi in favore del cloud computing e cloud storage. Ad esempio, servizi come Google Drive e Dropbox permettono di salvare i propri file in remoto ed accederne tramite connessione ad Internet, diminuendo l'uso di memoria nel dispositivo personale a discapito della necessità di connessione performante. Allo stesso modo, servizi di streaming come Netflix e Spotify forniscono cataloghi multimediali pressochè infiniti.

In un mondo sempre più connesso digitalmente diventa quindi fondamentale, per una rete locale, essere in grado di sostenere un traffico di dati elevato ed un numero di dispositivi in costante crescita in modo da poter fornire una

buona connettività per una corretta esperienza d'uso.

Sebbene gran parte del traffico verso questi tipi di servizi venga generato tramite connessioni mobili, quali 3G e 4G, queste non saranno oggetto di discussione. Il motivo principale risiede nel fatto che la qualità della connessione, in questo caso, dipende quasi interamente dalla bontà del segnale ricevuto dalle antenne dell'operatore. Incidono anche fattori metereologici [2], il posizionamento delle apparecchiature sul territorio e la loro rispettiva capillarità. Fattori secondari di qualità del segnale possono essere invece ricondotti alle antenne del dispositivo mobile che usufruisce della connessione ma, anche in questo caso, esse vengono scelte dal fabbricante e quindi sono fuori dal controllo dell'utente. I temi affrontati da questo elaborato riguardano la qualità del servizio offerto da reti locali e dei dispositivi collegati ad esse. Gli sviluppi nel mondo tecnologico precedentemente citati hanno dato vita a diverse sfide per fabbricanti di apparecchiature di rete e personale specializzato del settore. Ad esempio, l'introduzione della connessione senza fili, richiede particolare attenzione per via della natura delle onde radio. Gli access point devono essere posizionati in modo strategico all'interno del locale dove si vuole instaurare la connessione, tenendo conto di problemi come l'attenuazione del segnale attraverso mura [3] e interferenze causate con altri dispositivi attivi sulla stesse frequenze. Una soluzione al primo problema si trova nel posizionare apparecchiature come repeater per estendere il campo di copertura mentre l'utilizzo di software professionale può essere necessario per la scelta corretta di un canale libero da interferenze. L'aumento vertiginoso del numero dei dispositivi connessi alle reti aumenta anche l'importanza di riuscire a capirne il tipo ed eventuali servizi offerti prima di iniziare una fase di monitoraggio riguardante il traffico di rete. Ci sono diverse tecniche in letteratura per questo tipo di analisi, sia di tipo attivo che passivo, che verranno presentate ed approfondite nel prossimo capitolo. Questo tipo di studio, come vedremo, é fondamentale per fornire una corretta analisi dei disservizi di una rete locale poichè é necessario, prima di tutto, avere un'idea della quantità e del tipo dei dispositivi che si andranno a monitorare. In un secondo momento verranno poi presentati alcuni strumenti per il monitoraggio effettivo della rete che, anche in questo caso, possono essere divisi in passivo o attivo. Purtroppo le principali limitazioni di questo tipo di strumenti includono l'implementazione in sole apparecchiature professionali e la difficoltà d'uso per personale non specializzato. Lo studio si é quindi incentrato sulla possibilità di implementare tecniche per la rilevazione di disservizi in reti locali tenendo in mente la facilità d'uso e la possibilità di implementazione su apparecchiature a basso costo per reti di piccole dimensioni.

1.1 Obiettivo

Lo scopo di questo elaborato é quello di fornire uno strumento in grado di rilevare eventuali disservizi nella connettività di piccole reti locali dove le apparecchiature presenti non sono dotate di funzioni di monitoraggio. La crescita non omogenea di questo tipo di reti, il numero spesso imprevedibile di dispositivi connessi e la moltitudine di servizi che questi offrono, rendono, però, necessaria anche una prima analisi di rete finalizzata a determinare la quantità ed il tipo di device connessi. Successivamente, con metriche che verranno introdotte nei prossimi capitoli, si procede al monitoraggio di tutti i dispositivi appartenenti alla rete. In particolare, in caso di malfunzionamenti, si vuole identificare se questi siano dovuti a problematiche interne alla propria Local Area Network (LAN) o alla Wide Area Network (WAN) del provider Internet. Per disservizi interni alla LAN, successivamente alla localizzazione del problema, si procede proponendo soluzioni all'utente e identificando tutti i dispositivi il cui servizio é degradato.

1.2 Contributo originale

Durante lo studio iniziale si é notata la mancanza di strumenti open-source in grado di fornire una visione topologica dei dispositivi Wi-Fi. Si è quindi sviluppata una libreria in grado di monitorare, tramite ispezione di frame 802.11, il traffico Wi-Fi delle reti circostanti per poi fornirne dati relativi alla potenza del segnale dei dispositivi connessi ed una topologia dettagliata. Questo passaggio permette il discovery di dispositivi Wi-Fi nella nostra rete locale ed un monitoraggio nel tempo della bontà del segnale. I dettagli implementativi e la relativa validazione sono lasciati ai corrispettivi capitoli dell'elaborato.

1.3 Struttura della tesi

La tesi é divisa in cinque capitoli di cui si elenca un breve sommario:

- Capitolo 1: **Introduzione**, vengono presentati il problema analizzato e le motivazioni che hanno portato alla stesura di questa tesi.
- Capitolo 2: **Stato dell'arte**, vengono descritte le attuali tecnologie utilizzate per la rilevazione di disservizi nella connettività di rete.
- Capitolo 3: **Soluzione proposta**, vengono esposte la soluzione proposta e la libreria sviluppata.
- Capitolo 4: **Validazione**, vengono mostrati i risultati ottenuti al fine di validare la soluzione proposta.
- Capitolo 5: **Conclusione e lavoro futuro**, presentazione delle conclusioni raggiunte ed alcune ipotesi per lavori futuri.

Capitolo 2

Stato dell'arte

In questo capitolo vengono presentate le motivazioni che hanno portato alla stesura di questo elaborato e le soluzioni per rilevazione di disservizi nella connettività piú utilizzate.

2.1 Motivazione

Come introdotto nel precedente capitolo, lo scopo di questo lavoro é di fornire una soluzione per la rilevazione di disservizi in reti locali domestiche. Lo studio si é focalizzato su questo tipo di infrastrutture poichè esse rappresentano la maggioranza delle reti e, molto spesso, la loro configurazione é lasciata ad un utente finale con poche conoscenze del campo. Questo può portare a prestazioni poco efficienti per quanto riguarda le connessioni Wi-Fi o all'uso di apparecchiature di scarsa qualità che dimuiscono le velocità di download ed upload dei dispositivi. In aggiunta, access point vicini, se sullo stesso canale Wi-Fi,potrebbero interferire sulla connessione locale. Per questo motivo, software come Kismet[4], possono essere utilizzati anche per scegliere un canale non sovrautilizzato oltre a monitorare il traffico Wi-Fi ed i device connessi ad una rete. Negli ultimi tempi, i produttori di router, stanno cercando di implementare in tutti i loro dispositivi metodi di monitoraggio per rilevare disservizi di reti. Questo permette agli Internet Service Providers (ISP) di fornire una diagnostica iniziale che circoscriva il problema all'interno o all'esterno della rete. Nel primo caso, l'utente viene informato della presenza del problema nella sua rete locale e quali dispositivi ne siano affetti, mentre nel secondo caso é il fornitore del servizio Internet a dover intervenire sulla propria rete per rimediare al disservizio. Le soluzioni attuali per il monitoraggio e la gestione di rete presentano infatti diverse problematiche quando applicate a reti piccole locali.

In particolare il software é:

- Ristretto ad apparecchiature di fascia alta.
- Non sempre fornito di interoperabilità con software di altri produttori.
- Difficile da utilizzare per personale non specializzato.

Per questi motivi l'elaborato vuol fornire, dopo aver introdotto le tecniche di rilevazione di disservizi più comuni, una soluzione che possa essere utilizzata in piccole reti da utenti non esperti e su apparecchiature non professionali.

2.2 IEEE 802.11 Distributed Coordination Function

Nel protocollo 802.11 il meccanismo di accesso al mezzo trasmissivo é chiamato distributed coordination function (DCF) [5]. Questo metodo di accesso casuale é basato sul protocollo di accesso multiplo tramite rilevamento della portante con evitamento delle collisioni (CSMA/CA) in cui i terminali tentano di evitare a priori il verificarsi di collisioni durante la trasmissione. La ritrasmissione, in caso di collisione di pacchetti, é gestita tramite un algoritmo di backoff esponenziale binario (BEB) che verrà presentato in dettaglio successivamente. É importante notare che lo standard IEEE 802.11 definisce anche un protocollo opzionale ,chiamato point coordination function (PCF), in cui l'access point ha il compito di coordinare l'accesso al mezzo trasmissivo per evitare collisioni. Questo tipo di meccanismo di accesso non verrà trattato per via del suo poco utilizzo.

DCF descrive due tecniche per la trasmissione di pacchetti:

- Two-way handshake: meccanismo di accesso base.
- Four-way handshake: request to send/clear to send (RTS/CTS).

Il meccanismo di accesso base é ottenuto attraverso la trasmissione immediata di un acknowledgment positivo (ACK) da parte della stazione destinataria dopo aver ricevuto correttamente un pacchetto dal mittente. L'invio esplicito dell'ACK é richiesto poichè in un mezzo trasmissivo senza fili il mittente non può determinare se il pacchetto sia stato ricevuto correttamente ascoltando la sua stessa trasmissione.

Il meccanismo RTS/CTS é opzionale e prevede che una stazione interessata all'invio di un pacchetto riservi il mezzo tramite un pacchetto request to

send. Dopo che il destinatario riconosce questo pacchetto con un frame CTS la comunicazione continua con l'invio del pacchetto desiderato e di relativo ACK.

Questo meccanismo permette l'incremento della performance del sistema grazie alla riduzione della durata di collisione che potrebbe avvenire con l'invio di lunghi pacchetti. Infatti, in questo caso, la collisione può solamente avvenire sul frame RTS e viene riconosciuta dalla mancanza di un frame CTS di risposta del destinatario. In aggiunta il meccanismo RTS/CTS implementato nello standard IEEE 802.11 é sviluppato per contrastare il problema dei terminali nascosti [6] che si presenta quando un paio di stazioni mobili non riescono a rilevarsi.

Si presenta ora il funzionamento di DCF, come standardizzato dal protocollo 802.11.

Una stazione che vuole trasmettere un pacchetto, prima di inviarlo, monitora l'attività presente sul canale. Se il canale risulta inattivo per una durata pari ad un distributed interframe space (DIFS), il mittente procede all'invio del frame. In caso contrario, se il canale é attualmente in uso, la stazione continua a monitorarlo finchè esso non risulta inattivo per un DIFS. A questo punto la stazione attende per un intervallo casuale di backoff per minimizzare la probabilità di collisione di pacchetti con altre stazioni che hanno intenzione di trasmettere. Nello stesso modo, una stazione dovrà attendere un altro intervallo casuale per l'invio di due pacchetti consecutivi, anche se il canale risulta inattivo per un DIFS in modo da non impossessarsi del canale di trasmissione. L'uso del backoff casuale é il meccanismo che questo protocollo implementa per la collision avoidance.

DCF utilizza una scala a tempo discreto di backoff per motivi di efficienza, infatti il tempo immediatamente successivo ad un DIFS viene diviso in slot ed ogni stazione può solo trasmettere all'inizio di ciascuno di questi.

La dimensione dello slot, δ, é pari al tempo che una stazione impiega per rilevare la trasmissione di un pacchetto da parte di una qualsiasi altra stazione. Questo valore dipende dal tipo dal tipo del mezzo trasmissivo e viene raffigurato nella tabella 2.1. Come precedentemente introdotto, DCF, implementa un backoff esponenziale ed il tempo viene scelto in un range (0, ω-1) dove ω é detta contention window. Questo valore dipende dal numero di trasmissioni fallite per un pacchetto, a partire da un valore pari a CW_{min} viene raddoppiata ad ogni trasmissione fallita fino ad un valore massimo pari a $CW_{max}=2^m$ CW_{min}. I valori minimi e massimi della

PHY	δ	CW_{min}	CW_{max}
FHSS	50	16	1024
DSSS	20	32	1024
IR	8	64	1024

Tabella 2.1: Tabella 1

finestra sono specificati, a seconda del tipo di mezzo di trasmissione, nella tabella 2.1. Il contatore del backoff viene decrementato quando il canale si trova in uno stato di idle mentre é mantenuto inalterato quando una trasmissione viene captata sul canale. Infine, la stazione trasmette quando il valore del contatore raggiunge lo 0.

Si presentano ora due esempi di trasmissione usando i due metodi di accesso al metodo trasmissivo presentati.

Considerando due stazioni A e B che condividono lo stesso canale utilizzando il metodo base di accesso, alla fine della trasmissione B attende un DIFS e sceglie un tempo di backoff prima di trasmettere un nuovo pacchetto. Durante questo periodo la stazione A invia un pacchetto sul canale e, di conseguenza, il timer di backoff della stazione B rimane invariato fino a che il canale non verrà percepito come libero per almeno un DIFS. Per quanto riguarda la stazione A, essa riceve un ACK per segnalare la ricezione con successo del pacchetto da parte del destinatario. Il pacchetto di ACK viene inviato immediatamente trasmesso alla fine del messaggio, dopo un periodo di attesa chiamato short interframe space (SIFS). La durata di un SIFS é inferiore a quella di un DIFS, questo rende impossibile alle altre stazioni di rilevare come libero il canale fino a che non venga inviato l'ACK. In caso di mancata ricezione dell'ACK da parte della stazione A entro un tempo specificato ACKTimeout o della trasmissione di altri pacchetti nel canale, questa rischedula l'invio del pacchetto tramite le regole di backoff presentate.

Nel meccanismo RTS/CTS una stazione che vuole trasmettere un pacchetto aspetta fino a che non rileva il canale inattivo per un DIFS, segue le regole di backoff precedentemente introdotte e trasmette un frame speciale chiamato RTS. Quando la stazione ricevente riconosce un frame RTS risponde, dopo un SIFS di attesa, con un frame CTS. Il mittente é autorizzato ad utilizzare il canale solo alla corretta ricezione di un CTS. I frame RTS e CTS contengono inoltre la lunghezza del pacchetto da trasmettere, permettendo a tutte le stazioni in ascolto di aggiornare un network allocation vector (NAV) contenente il periodo di tempo per il quale il canale sarà occupato. Questo meccanismo fornisce, quindi, una soluzione al problema dei terminali nascosti oltre a ridurre la lunghezza dei frame coinvolti nella contesa del canale.

Figura 2.1: DCF con metodo accesso base (sinistra) e RTS/CTS (destra)

2.3 Analisi della performance IEEE 802.11 DCF

Uno dei primi e più rilevanti studi sulle prestazioni del meccanismo DCF é quello svolto da Bianchi [7] che propone la valutazione analitica del saturation throughput, ovvero il limite del throughput di sistema raggiunto all'aumentare del carico sul sistema stesso. L'analisi é stata effettuata con un numero fissato di stazioni ed uno stato di saturazione, ovvero assumendo che ogni stazione abbia sempre un pacchetto disponibile ad essere trasmesso. Diviso in due parti, lo studio improntato da Bianchi si concentra prima nel fornire una rappresentazione in catena di Markov del comportamento della singola stazione per ottenere la probabilità stazionaria τ che essa trasmetta un pacchetto in uno slot di tempo casuale. L'approccio utilizzato fornisce una probabilità indipendente dal tipo di meccanismo di accesso (base o RTS/CTS). Dopo aver trovato questo valore, analizzando i possibili eventi che possono accadere in un determinato slot temporale, lo studio si conclude esprimendo il throughput dei due possibili metodi di accesso al mezzo trasmissivo in funzione del valore τ.

$$\begin{cases} P\{i,k|i,k+1\} = 1 & k \in (0, W_i - 2)\ i \in (0,m) \\ P\{0,k|i,0\} = (1-p)/W_0 & k \in (0, W_0 - 1)\ i \in (0,m) \\ P\{i,k|i-1,0\} = p/W_i & k \in (0, W_i - 1)\ i \in (1,m) \\ P\{m,k|m,0\} = p/W_m & k \in (0, W_m - 1) \end{cases}$$

La prima equazione tiene conto del decremento del tempo di backoff all'inizio di ogni slot di tempo mentre la seconda equazione del fatto che un nuovo pacchetto in seguito ad una trasmissione con successo inizia con un backoff stage pari a 0. I restanti due casi esprimono il sistema in caso di fallimento nella trasmissione. In particolare la terza equazione esprime come avvenga un aumento del backoff stage e la scelta di un nuovo valore di backoff iniziale nel range $(0,W_i)$. Infine, l'ultima equazione, modella il massimo

valore m che il tempo di backoff può assumere. Dopo aver trovato la formula chiusa della catena di Markov si può esprimere la probabilità τ che una stazione trasmetta in uno slot di tempo casuale. Poichè la trasmissione avviene quando il timer di backoff raggiunge lo 0, a prescindere dal backoff stage il valore di tau é pari a:

$$\tau = \frac{2(1-2p)}{(1-2p)(W+1)+pW(1-(2p)^m)} \tag{2.1}$$

Il valore di p, ovvero della probabilità di collisione, é pari alla probabilità che una delle restanti n-1 stazioni decida di trasmettere un pacchetto.

$$1-(1-\tau)^{n-1} \tag{2.2}$$

Possiamo quindi dire che

$$\tau(p) = \frac{2}{1+W+pW\sum_{i=0}^{m-1}(2p)^i} \tag{2.3}$$

Per calcolare quindi S, il throughput normalizzato, ovvero il periodo di tempo in cui il canale é utilizzato per trasmettere correttamente pacchetti, Bianchi ha poi definito le probabilità degli eventi che possono accadere in uno slot di tempo. In particolare, viene identificata con P_{tr} la probabilità che ci sia almeno una trasmissione nello slot di tempo e, poichè ogni stazione trasmette sul canale con probabilità τ, si ha:

$$P_{tr} = 1-(1-\tau)^n \tag{2.4}$$

La probabilità P_s che una trasmissione avvenga correttamente é quindi data dalla probabilità che esattamente una stazione trasmetta condizionata dalla probabilità che almeno una stazione trasmetta.

$$P_s = \frac{n\tau(1-\tau)^{n-1}}{P_{tr}} = \frac{n\tau(1-\tau)^{n-1}}{1-(1-\tau)^n} \tag{2.5}$$

Si può ora descrivere S come il rapporto

$$S = \frac{E[payload\ trasmesso\ in\ uno\ slot\ di\ tempo]}{E[lunghezza\ dello\ slot\ di\ tempo]} \tag{2.6}$$

Dato che E[P] e' la dimensione media di un pacchetto, la media di informazione trasmessa correttamente in uno slot di tempo e' pari a $P_{tr}P_sE[P]$, poichè una trasmissione corretta avviene in uno slot con probabilità $P_{tr}P_s$.

Con probabilità $1-P_{tr}$ lo slot di tempo é vuoto, con probabilità $P_{tr}Ps$ contiene una trasmissione con successo e con probabilità $P_{tr}(1-P_s)$ una collisione. L'equazione per ottenere S diventa quindi

$$S = \frac{P_s P_{tr} E[P]}{(1-P_{tr})\sigma + P_{tr} P_s T_s + P_{tr}(1-P_s)T_c} \tag{2.7}$$

In questa equazione si identifica il tempo medio in cui il canale viene visto come occupato per via di una trasmissione avvenuta con successo con T_s ed il tempo medio in cui il canale viene visto come occupato per via di una trasmissione con collisione con T_c. Questi valori, necessari per il calcolo del throughput, dipendono dal tipo di meccanismo di accesso utilizzato. Per quanto riguarda il meccanismo di accesso base, identificando con H=PHY_{hdr} + MAC_{hdr}, δ il ritardo di propagazione e E[P*] la lunghezza media del più grande pacchetto coinvolto in una collisione:

$$\begin{cases} T_s^{bas} & = H + E[P] + SIFS + \delta + ACK + DIFS + \delta \\ T_c^{bas} & = H + E[P*] + DIFS + \delta \end{cases}$$

Per il meccanismo di accesso basato su RTS/CTS i valori sono invece

$$\begin{cases} T_s^{rts} = RTS + SIFS + \delta + CTS + SIFS + \delta + H + E[P] \\ \qquad\quad + SIFS + \delta + ACK + DIFS + \delta \\ T_c^{rts} = RTS + DIFS + \delta \end{cases}$$

Il modello presentato da Bianchi si é rivelato, dopo validazione tramite simulazione, efficace per rappresentare i diversi schemi di accesso utilizzati da DCF: in particolare quello base, RTS/CTS ed una combinazione dei due che non é stata riportata. I risultati ottenuti dal modello mostrano che la performance del metodo di accesso base dipende fortemente sui parametri del sistema, principalmente il numero di stazioni connessi ed i parametri minimi della finestra di contesa. Questi ultimi sono però meno influenti sul metodo RTS/CTS che si presenta come la migliore opzione di accesso al metodo per reti di grandi dimensioni per via della possibilità di arginare il problema dei terminali nascosti ed un minore tempo impiegato durante la collisione quando più stazioni trasmettono contemporaneamente.

2.4 TCP e DCF, analisi della performance

Lo studio condotto da Wu et al [8] propone un modello basato su quello di Bianchi che tiene però conto del limite di tentativi di ritrasmissione di un frame. In aggiunta, viene proposto un miglioramento allo standard 802.11 con l'introduzione di DCF+. Questo meccanismo di accesso al metodo di trasmessione é introdotto per cercare di sopperire alle problematiche di performance di cui protocolli di livello trasporto soffrono in reti wireless [9]. In particolare, lo studio si concentra sul risolvere la contesa per il canale di trasmissione che avviene durante lo scambio di dati ed ACK TCP, meccanismo che potrebbe causare collisioni e un degrado delle prestazioni. La soluzione proposta é inoltre compatibile con DCF definito dallo standard 802.11, questo vuol dire che in una stessa rete possono coesistere e comunicare stazioni che supportano due metodi di accesso al mezzo trasmissivo diversi.

Il principale cambiamento che DCF+ apporta é quello di utilizzare il MAC ACK specificato nello standard 802.11 come un RTS. Questo é in linea con l'implementazione di DCF che prevede l'invio di un ACK in caso di una trasmissione ricevuta con succeso e permette una retrocompatibilità con stazioni che non implementano DCF+.

In figura si mostra un esempio del funzionamento di DCF+ assumendo che la stazione destinatario debba, oltre a ricevere un frame dal mittente, anche inviargli un pacchetto dati. Successivamente alla corretta ricezione del frame dati il destinatario procede ad inviare un ACK al mittente che, come già introdotto, viene considerato come un RTS ed utilizzato per inizializzare anche il NAV delle altre stazioni in ascolto. Come da implementazione del DCF il mittente risponde a questo frame con un CTS ed inizializza i valori del NAV pari alla lunghezza del frame di dati che deve ricevere. L'operazione si conclude con l'invio del pacchetto ed un normale ACK di riscontro. Per quanto riguarda il metodo di accesso RTS/CTS la procedura differisce solo per l'aggiunta dei due pacchetti iniziali che permettono alle stazioni di impossessarsi del mezzo trasmissivo.

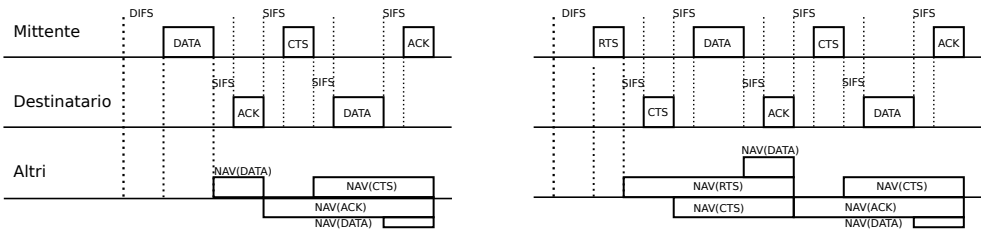

Figura 2.2: DCF+ con metodo accesso base (sinistra) e RTS/CTS (destra)

Il funzionamento di DCF+ come presentato si basa, però, su due assunzioni:

- La stazione mittente che riceve l'ACK sia in grado di determinare, in base al campo della durata presente nel frame, se il destinatario ha un pacchetto dati pronto per l'invio.
- Le stazioni, tramite campi nel frame dati e record locali, siano in grado di determinare se il destinatario supporti DCF+.

Il modello utilizzato da Wu et al per l'analisi di questo metodo di accesso si basa su una estensione del modello proposto da Bianchi. In particolare, a parità di assunzioni, viene proposta una catena di Markov in cui vengono considerati gli effetti del limite di ritrasmissioni di frame:

$$\begin{cases} P\{i,k|i,k+1\} = 1 & k \in (0, W_i - 2)\ i \in (0,m) \\ P\{0,k|i,0\} = (1-p)/W_0 & k \in (0, W_0 - 1)\ i \in (0,m) \\ P\{i,k|i-1,0\} = p/W_i & k \in (0, W_i - 1)\ i \in (1,m) \\ P\{0,k|m,0\} = p/W_0 & k \in (0, W_m - 1) \end{cases}$$

Questa differenza si ripercuote anche sui valori di τ e p. In aggiunta, poichè viene considerato anche l'effetto timeout dell'ACK, il modello differirà da quello proposto da Bianchi anche nei valori di T^{bas} e T^{rts} che saranno, rispettivamente:

$$\begin{cases} T_s^{bas} & = H + E[P] + SIFS + \delta + ACK + DIFS + \delta \\ T_c^{bas} & = DIFS + H + E[P*] + SIFS + ACK \end{cases}$$

$$\begin{cases} T_s^{rts} = RTS + SIFS + \delta + CTS + SIFS + \delta + H + E[P] \\ \qquad\quad + SIFS + \delta + ACK + DIFS + \delta \\ T_c^{rts} = DIFS + RTS + SIFS + CTS \end{cases}$$

Il modello analitico sviluppato da questo studio si é dimostrato più accurato rispetto a quello proposto da [7] in seguito alle simulazioni svolte. Quest ultimo infatti sovrastima il throughput poichè non considera il limite di ritrasmissioni ed il timeout dovuto all'ACK. Le prestazioni di DCF+ sono poi state comparate a quelle di DCF utilizzando il modello presentato, evidenziando un miglioramento in metriche quali: goodput, fairness nell'utilizzo del mezzo trasmissivo e delay a livello MAC.

2.5 IEEE 802.11E EDCF

Fino allo standard IEEE 802.11e [10] il modello della WLAN può essere visto come una versione wireless di Ethernet che supporta un servizio best effort. L'aumento dei servizi offerti in streaming e VoIP ha però reso necessaria l'implementazione di meccanismi per il supporto quality of service (QoS), ovvero la possibilitdi fornire una diversa priorità a diverse applicazioni o utenti. Nel principio 802.11 non fornisce questo supporto di differenziare frame in base a priorità, tutto ciò che fornisce DCF é un accesso al canale in contesa con uguale probabilità per tutte le stazioni. Lo standard 802.11e definisce due miglioramenti al fine di supportare QoS mediamente l'introduzione di Enhanced Distributed Coordination Function (EDCF) e Hybrid Coordination Function (HCF). In EDCF vengono implementate delle categorie di traffico (TC) a cui vengono associate diverse priorità come mostrato nella tabella 2.2.

Priorità	802.1D	Categoria	Descrizione
Bassa	1	AC_BK	Background
	2	AC_BK	Background
	0	AC_BE	Best Effort
	3	AC_BK	Best Effort
	4	AC_VI	Video
	5	AC_VI	Video
	6	AC_VO	Voce
Alta	7	AC_VO	Voce

Tabella 2.2: Tabella categorie accesso

I frame delle stazioni vengono quindi divisi in diverse istanze di backoff, ognuna con dei parametri specifici alla categoria di traffico 2.3. Nel periodo di contesa per il mezzo trasmissivo, ogni categoria di traffico cerca di accedere ad una transmission opportunity (TXOP) ed inizia un periodo di backoff indipendente dopo che il canale é inattivo per almeno un Arbitration Interframe Space (AIFS). Se durante il periodo di backoff il canale torna ad essere utilizzato, come per DCF, EDCF aspetta che il canale torni ad essere libero prima di diminuire il valore di backoff. Per via delle categorie di traffico, una singola stazione può implementare fino ad otto code interne realizzate come stazioni virtuali. Se più di una stazione raggiunge il valore 0 nel backoff, uno scheduler ha il compito di evitare una collisione tra le due stazioni virtuali dando la TXOP alla stazione con priorità più alta.

Durante l'intervallo TXOP, definito da un tempo di inizio ed una massima durata, una stazione ha il diritto di trasmettere sul canale. L'intervallo

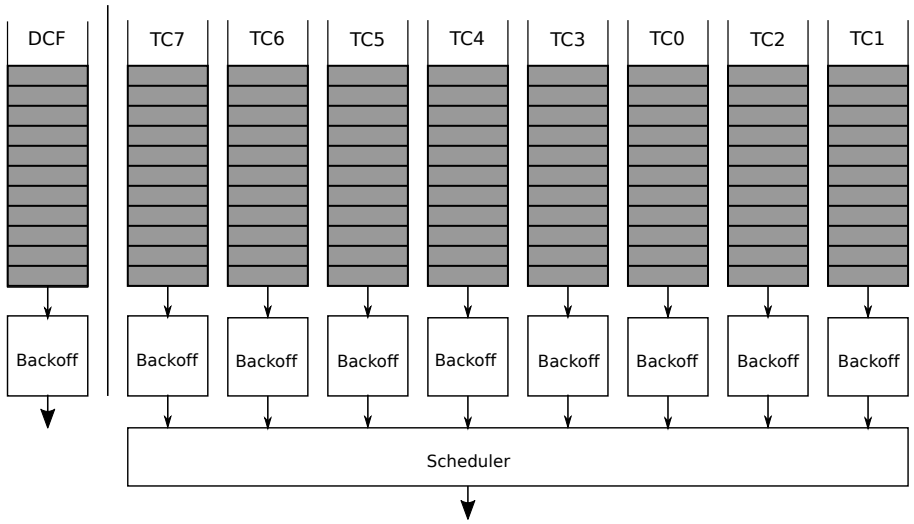

Figura 2.3: DCF (sinistra) e EDCF con otto backoff virtuali (destra)

TXOP viene allocato tramite una contesa (EDCF-TXOP) o assegnato attraverso HCF (polled-TXOP). La durata dell'intervallo é definita dai beacon frames dell'AP per quanto riguarda EDCF-TXOP e specificato nel frame del poll per quanto riguarda HCF.

Diversi studi sono stati improntati sulla performance di EDCF, in particolare [11] dopo aver simulato l'uso di EDCF ne evidenzia una soluzione efficiente per l'implementazione QoS su reti WLAN e la retrocompatibilità con stazioni che non implementano questo metodo di accesso. Con l'opportuna scelta di parametri, stazioni EDCF riescono infatti ad avere priorità sul canale rispetto a stazioni che implementano DCF.

Xiao [12] ha successivamente fornito un modello analitico, seguendo le orme di Bianchi, di EDCF. Utilizzando metriche di backoff quali: dimensione iniziale della finestra, limite di ritrasmissioni e il fattore di incremento della finestra di backoff i risultati ottenuti dallo studio mostrano come una categoria di traffico possa rubare banda ad un altra categoria in caso questa aumenti il valore delle suddette metriche. In aggiunta, viene suggerita una ridimensione del limite di ritrasmissioni per traffico di tipo video per aumentare throughput e migliorare il delay.

2.6 IEEE 802.11N e 802.11AC

Attualmente la maggior parte dei router in commercio ed utilizzati in reti locali sono conformi allo standard 802.11n ed, in particolare, a quello 802.11ac. Il primo, con l'obiettivo di aumentare il throughput degli standard precedenti, fornisce supporto per frame aggregation e multiple-input and multiple-output (MIMO). Come suggerisce il nome, il frame aggregation permette ad un trasmettitore di inviare più di un frame in una singola trasmissione. Questa funzionalita, come studiato da [13], si rivela molto efficace per l'aumento del throughput della rete e per la riduzione del ritardo di trasmissione. La tecnologia MIMO fa utilizzo di una moltitudine di antenne in ricezione ed invio per trasmettere simultaneamente più stream di dati utilizzando propagazione a più vie. Il successivo standard 802.11ac, utilizzato maggiormente nella realizzazione del tirocinio, estende MIMO per permettere un uso multi utente, chiamato MU-MIMO.

2.7 Radiotap

Un header radiotap é un meccanismo che viene utilizzato per aggiungere informazioni ad un frame 802.11 al momento della sua cattura. Pur non facendo parte in alcun modo di pacchetti 802.11 l'importanza delle metriche fornite ed il supporto ai più utilizzati sistemi operativi lo rendono uno standard per la ricezione di frame 802.11. L'header radiotap viene aggiunto al frame catturato dal device di rete, o dal suo driver, e contiene quindi informazioni fornite dalla particolare stazione che riceve e non di quella che trasmette.

Si elencano ora alcuni dei campi presenti nel radiotap header, in particolare quelli utilizzati per lo sviluppo della soluzione proposta dal tirocinio:

- Antenna: antenna in ricezione o tramissione utilizzata per il pacchetto.
- Channel: frequenza del canale utilizzato per trasmettere il pacchetto.
- Antenna Signal: potenza del segnale in ricezione all'antenna.
- Antenna Noise: rumore di sottofondo in ricezione all'antenna.
- Timestamp: l'istante di tempo in cui é stato ricevuto il pacchetto.

In particolare con l'uso di queste metriche, oltre ad identificare su quale canale un AP stia utilizzando per le proprie trasmissioni, si può fornire un valore riguardante la bontà del segnale Wi-Fi.

La differenza tra antenna signal ed antenna noise fornisce, infatti, un parametro chiamato Signal-to-Noise-Ratio (SNR) che viene per classificare la qualità del segnale. In generale i valori del SNR si possono così catalogare:

- >40dB: segnale eccellente, massima velocità.
- 25db-40db: segnale molto buono, ottima velocità.
- 15db-25db: segnale basso, buona velocità.
- 10db-15db: segnale molto basso, bassa velocità.
- 5db-10db: nessun segnale.

Avere un SNR accettabile per ogni dispositivo connesso alla rete é fondamentale per la performance generale, poichè uno scarso segnale contribuisce fortemente all'aumentare del numero di ritrasmissioni e quindi una diminuzione del throughput del sistema Wi-Fi.

2.8 Software di monitoraggio Wi-Fi

I metodi di accesso al mezzo trasmissivo e le metriche per misurare la bontà del segnale presentati in questo capitolo sono alla base del funzionamento dei software più utilizzati per il monitoraggio di reti Wi-Fi. La soluzione open-source più utilizzata e sviluppata é sicuramente la già menzionata Kismet, che tra le tante funzionalità permette, tramite API, la visualizzazione di tutti i dispositivi connessi ad un access point e ne fornisce eventuali valori del segnale. Questo tipo di approccio non permette però una visione di insieme della topologia Wi-Fi poichè, ad esempio, l'individuazione di eventuali repeater non é automatizzata.

Funzioni simili a quelle di Kismet si possono trovare nel prodotto UniFi [14] di Ubiquity che fornisce una panoramica dettagliata dell'attività di rete e degli indici di connessione dei dispositivi. Purtroppo, software di questo tipo sono generalmente proprietari e limitati ad un utilizzo con dispositivi specifici del produttore. Questo tipo di soluzione non é quindi ottimale per la gestione di una rete locale domestica dove i dispositivi connessi sono generalmente di diversi produttori e non di livello professionale.

Più comuni sono software come NetSpot [15], Kismac e inSSIder [16] che forniscono invece una visione della rete Wi-Fi limitata agli access point presenti nelle vicinanze. In questo modo é possibile identificare eventuali problemi di connessione Wi-Fi dovuti alla sovrapposizione di più reti WLAN sullo stesso canale.

Capitolo 3

Soluzione proposta

In questo capitolo viene presentata la soluzione proposta per la rilevazione di disservizi nella connettività di reti locali. Si analizza brevemente l'architettura del software sviluppato per poi fornirne una descrizione dettagliata della sua implementazione e del software utilizzato nello sviluppo.

3.1 Architettura

L'architettura della soluzione proposta é principalmente suddivisa in due parti come mostrato in figura:

- una libreria che implementa un'operazione di ARP [17] scan, utilizzata per fornire una metrica del round-trip time (RTT) ed associare ad indirizzi IPv4 nella rete locale i rispettivi indirizzi MAC. Benchè l'utilizzo di questa libreria sia facoltativo, nei capitoli successivi si mostrerà come i risultati ottenuti dall'operazione di ARP scan migliorino l'accuratezza della ricostruzione della topologia Wi-Fi.

- una libreria che, dopo aver catturato pacchetti di traffico di rete ed ottenuto i risultati dell' ARP scan, analizza i frame ricevuti e li utilizza per ricostruire una topologia della rete Wi-Fi fornendo valori di bontà del segnale. Questa libreria é in grado di ricostruire topologie di reti sia in modalità di cattura attiva o da file di cattura.

Le operazioni di cattura di pacchetti in entrambe le librerie sviluppate sono effettuate utilizzando l'API Pcap [18]. In particolare, nella libreria di ARP scanning vengono catturati frame di tipo Ethernet II mentre nella libreria per la ricostruzione della topologia di una rete i frame catturati sono di tipo 802.11.

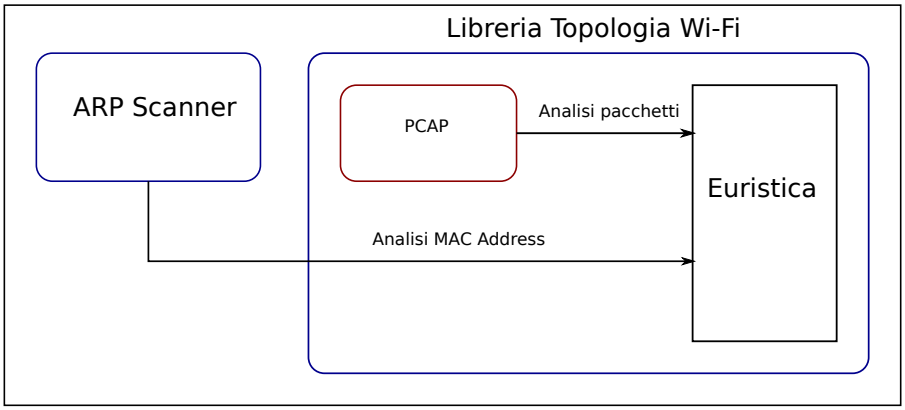

Figura 3.1: Architettura soluzione proposta

3.2 Implementazione

Si presentano brevemente, prima dei dettagli implementativi della libreria per la ricostruzione topologica della rete, il funzionamento della libreria utilizzata per la cattura dei pacchetti Pcap e quella implementata per effettuare ARP scanning.

3.2.1 Pcap

Sviluppata da Tcpdump, libpcap é una libreria scritta in linguaggio C che permette la cattura ed il filtraggio di pacchetti di rete. La scelta di questa libreria si é basata su tre principali aspetti:

- Facilità d'uso: libpcap offre astrazioni ad alto livello per la cattura ed il filtraggio di pacchetti di rete.
- Filtraggio dei pacchetti: mediante la compilazione di un filter, é possibile catturare solo i pacchetti di rete di interesse per l'applicazione.
- Compatibilità: la libreria, oltre ad essere disponibile per la maggior parte dei sistemi operativi moderni, presenta numerosi wrapper per essere integrata in linguaggi di programmazione diversi dal C.

Di seguito si descrivono i passi necessari ad effettuare una cattura utilizzando libpcap:

1. Scelta dell'interfaccia da utilizzare per la cattura.
2. Inizializzazione dell'interfaccia e dei parametri della sessione.

3. Creazione e compilazione del filtro da utilizzare per catturare i pacchetti desiderati.

4. Ciclo di ascolto in cui vengono analizzati, uno ad uno, i pacchetti catturati.

5. Chiusura della sessione di cattura.

3.2.2 ARP Scan

La libreria di ARP scan sviluppata permette la scoperta di tutti i dispositivi all'interno della rete locale. Questa operazione viene effettuata inviando un numero di pacchetti ARP ad ogni possibile indirizzo IPv4 presente nella sottorete per poi, utilizzando libpcap, riceverne eventuali riscontri.

Il risultato ottenuto é un'associazione tra indirizzo IP ed indirizzo media access control (MAC), un indirizzo fisico univoco assegnato ad ogni scheda di rete dal proprio produttore. L'indirizzo MAC così ottenuto verrà poi utilizzato per fornire una maggiore accuratezza nella ricostruzione della topologia Wi-Fi della rete locale in esame.

Sebbene questo sia il motivo principale di implementazione della libreria, é inoltre possibile ricavare una misura del round-trip time verso ogni dispositivo connesso alla rete, in modo analogo al ping attraverso richieste ICMP. A differenza di quest ultimo che può essere ignorato da alcuni tipi di dispositivi, utilizzando l'ARP ping con un numero di pacchetti appropriato é possibile ricevere riscontro da tutti i dispositivi attualmente connessi alla rete locale. In particolare, i dispositivi che tendono ad ignorare questo tipo di richieste sono quelli di tipo mobile come smartphone e tablet nei momenti di non utilizzo da parte dell'utente.

Benchè ci siano già diverse implementazioni funzionanti per i sistemi operativi più utilizzati, si é deciso di sviluppare una libreria basilare che svolga solo le operazioni necessarie per la ricostruzione topologica della rete. Si é cercato in questo modo di limitare l'utilizzo di risorse e fornire una soluzione la cui implementazione é indipendente dal sistema operativo e basata solamente sull'uso di libpcap.

3.2.3 WiFi-Topology

Dopo aver introdotto nelle sezioni precedenti una vista dell'architettura, purchè basilare, e le librerie fondamentali per il funzionamento della soluzione proposta si discute ora l'implementazione della principale libreria sviluppata durante il tirocinio.

La ricostruzione della topologia Wi-Fi delle reti viene effettuata attraverso l'analisi del traffico originato dalle stazioni presenti nelle vicinanze del dispositivo su cui il software é in esecuzione.

Questo tipo di cattura, come descritto precedemente, é effettuata utilizzando la libreria libpcap che permette di utilizzare un'interfaccia di tipo Wi-Fi in una particolare modalità, chiamata monitor mode, di cui si espone di seguito il funzionamento.

Monitor mode

La cattura in monitor mode, o RFMON (Radio Frequency MONitor), permette ad una interfaccia di rete wireless di catturare tutto il traffico passante per un canale Wi-Fi.

In questa modalità una scheda di rete non é associata ad alcun access point o rete ad-hoc e si pone in uno stato di ascolto in maniera completamente trasparente ad altri dispositivi wireless presenti nelle vicinanze. Per effettuare ciò non vengono rispettati i normali comportamenti di una stazione operante con il protocollo 802.11, come ad esempio l'invio di ACK come descritto nel secondo capitolo. Di conseguenza, in questa modalità, il dispositivo perde la possibilità di trasmettere dati ed il suo utilizzo é ristretto ad un singolo canale wireless. Un'altra limitazione in questo tipo di cattura riguarda il mancato controllo di errori nei pacchetti catturati, effettuato normalmente con un controllo di ridondanza ciclico (CRC).

Nonostante gli svantaggi elencati, questo tipo di modalità trova molto utilizzo nella progrettazione di reti wireless, ad esempio per la scelta di un canale poco utilizzato al fine di diminuire interferenze tra stazioni, o nel cracking di reti protette con WEP .

Nello sviluppo della libreria questa modalità é stata utilizzata per catturare diversi tipi di frame 802.11 trasmessi dai dispositivi nelle vicinanze. Analizzando questo tipo di dati ed i valori di potenze di segnale forniti dal radiotap header é stato poi sviluppato un algoritmo per la ricostruzione della topologia delle reti Wi-Fi. Per fornire una corretta analisi il controllo di ridondanza ciclico per i frame ricevuti é stato integrato nella libreria sviluppata, in modo da poter evitare eventuali incoerenze tra la topologia ricostruita e quella effettiva. In aggiunta, poichè la modalità monitor dissocia la scheda

di rete da un access point e cattura tutto il traffico passante per un canale, la libreria sviluppata non si limita a ricostruire una particolare rete di cui si é interessati ma fornisce una visione di tutte quelle nelle vicinanze. Per sopperire all'impossibilità di ascoltare su più di un canale si é fatto uso di uno script per effettuare channel hopping, in modo da poter catturare traffico per qualche secondo su ciascun canale.

Il compromesso principale dell'uso della monitor mode resta quello di dover dedicare completamente un'interfaccia Wi-Fi alla cattura dei frame dissociandola dalla rete locale che si vuole monitorare. Per questo motivo, su dispositivi dotati di una sola scheda di rete, non é possibile mantenere costantemente attiva la cattura perdendo quindi la possibilità di assistere a cambi nella topologia di rete in tempo reale. Un recente studio [19] ha evidenziato come sia possibile virtualizzare, senza perdita di prestazioni, interfacce per la cattura di traffico in modalità promiscua o, come in questo caso, in monitor mode.

Nella prossime sezioni vengono introdotti in dettaglio i frame catturati in questa modalità e come essi sono utilizzati per la ricostruzione della topologia della rete.

MAC Frame

Prima di mostrare come avviene l'analisi del traffico si introduce la struttura generale dei frame catturati tramite monitor mode ed i tipi rilevanti al funzionamento della libreria. Nei protocolli di rete wireless 802.11 un MAC frame, rappresentato in figura 3.2, é composto da campi comuni a tutti i tipi di frame e da campi specifici ad alcuni di essi.

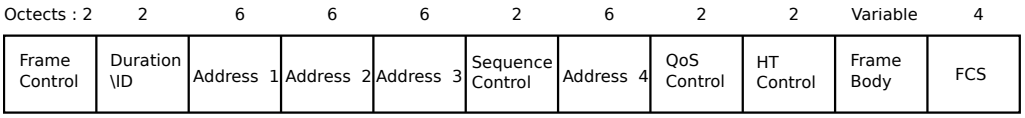

Figura 3.2: MAC frame

Un frame 802.11 contiene quindi un MAC header di lunghezza pari a 34 byte, un body di lunghezza variabile in base al tipo di frame catturato ed infine un campo di 4 byte per il controllo degli errori.

Di seguito si fornisce una breve descrizione di tutti i campi presenti nel MAC header, in particolare di quelli utilizzati durante l'implementazione della libreria:

- Frame Control: 2 byte che forniscono informazioni sul tipo del frame.
- Duration/ID: 2 byte che indicano alle stazioni la durata della trasmessione e viene usato per inizializzare il valore del NAV introdotto nel secondo capitolo.
- Address 1-2-3-4: 6 ottetti che identificano unicamente un dispositivo tramite indirizzo MAC.
- Sequence Control: diviso in due campi di 12 e 4 bit che indicano, rispettivamente, il numero di sequenza ed il numero del frammento del pacchetto.
- QoS Control: 2 byte che identificano i parametri QoS in un frame di dati.
- HT Control: 2 byte aggiunti dallo standard 802.11n.
- Frame Body: campo di lunghezza e tipo variabile, payload del frame.
- FCS: 4 byte di frame check sequence, un codice di rilevazione di errore.

I campi interessanti per la ricostruzione della topologia di una rete includono il frame control, gli indirizzi MAC, il body del frame ed il FCS. In particolare, nella figura 3.3, possiamo osservare come il frame control sia suddiviso in 11 sottocampi.

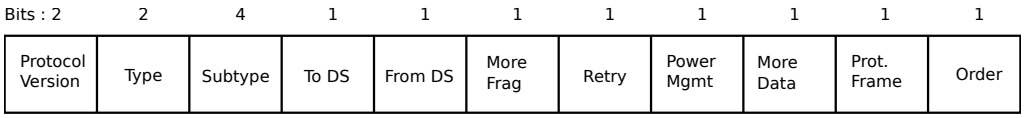

Figura 3.3: Frame Control Fields

Il primo campo, protocol version, indica la versione del protocollo 802.11 in uso dal frame ed é sempre pari a 0 poichè attualmente esiste una sola versione di questo protocollo.

Il secondo e terzo campo del frame control indicano invece il tipo e sottotipo del frame ricevuto.Questo tipo di informazione é fondamentale per una corretta analisi poichè a diversi tipi e sottotipi di frame corrispondono diversi campi nel frame body.

Data la lunghezza pari a 2 bit, un frame nello standard 802.11 può essere suddiviso in quattro categorie di tipo diverse, che a loro volta possono contenere sedici sottocategorie codificate con 4 bit:

- 00- Management Frame: forniscono informazioni sullo stato della rete e sono utilizzati per la connessione e disconnessione di dispositivi.
- 01- Control Frame: assistono la trasmissione di data frame e per amministrare l'accesso al mezzo al mezzo trasmissivo.
- 10- Data Frame: contengono dati di protocolli di livello superiore all'interno del loro body.
- 11- Reserved: tipo di frame riservato e non utilizzato nello standard 802.11.

L'utilizzo e il tipo di analisi effettuata su questi tipi di frame ed i loro sottotipi verrà introdotto in apposite sezioni.

I successivi due campi del frame control, To DS e From DS, sono di particolare importanza per lo studio effettuato sulla ricostruzione della topologia di rete. Questi due bit possono essere utilizzati per determinare quando un frame é immesso nel mezzo trasmissivo wireless e quando, invece, ne esce.

Di seguito si evidenziano i possibili valori di verità dei due campi:

- To DS=0, From DS=0 : il frame non deve lasciare il mezzo trasmissivo, valore generalmente associato a tipi di frame come: management e control.
- To DS=0, From DS=1 : il frame proviene da un access point e sta entrando nel mezzo trasmissivo wireless.
- To DS=1, From DS=0 : il frame proviene da un client e sta uscendo dal mezzo trasmissivo wireless.
- To DS=1, From DS=1 : il frame é destinato ad un'altra rete wireless.

Accoppiando questo tipo di analisi del mezzo trasmissivo con i valori di segnale ottenuti tramite Radiotap é possibile rilevare anche eventuali dispositivi connessi ad un access point via cavo, purchè il traffico analizzato contenga un cambio di mezzo trasmissivo.

Un esempio, che sarà discusso anche nel prossimo capitolo, potrebbe essere quello di un router collegato via cavo ad un access point ed un numero di dispositivi connessi in Wi-Fi a quest'ultimo.

MAC Address

Un MAC address é un identificatore unico associato ad un'interfaccia di rete dal proprio costruttore e viene utilizzato nel protocollo 802.11 per l'instradamento dei frame. L'indirizzo é formato da una struttura di 48 bit divisa in 6 ottetti, come mostrato in figura 3.4. Per mantenere l'unicittà tra tutte le schede di rete prodotte é stato introdotto uno standard, chiamato EUI-48 e gestito dalla IEEE, che divide l'indirizzo MAC in due parti:

- Organisationally Unique Identifier (OUI): identifica unicamente un produttore di schede di rete ed assegnato dalla IEEE.
- Network Interface Controller (NIC): identifica unicamente una determinata scheda di rete e viene assegnata dal prodottore.

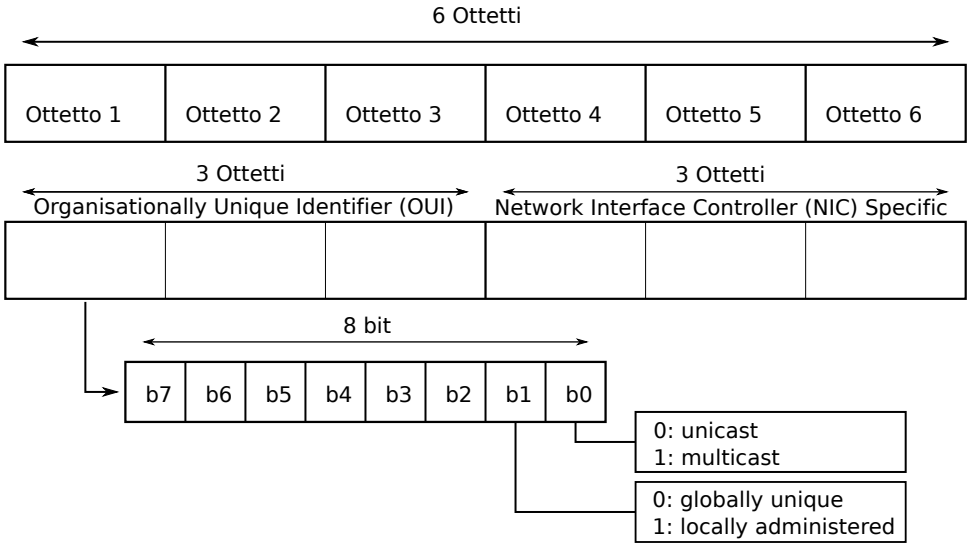

Figura 3.4: Mac Address

In aggiunta, un indirizzo MAC può essere universalmente (UAA) o localmente (LAA) assegnato. Questa diversificazione viene effettuata attraverso il valore del secondo bit meno signficativo del primo ottetto. Per quanto riguarda gli indirizzi UAA, questo bit viene posto a 0 ed il valore del primo ottetto é pari a quello del OUI. Al contrario, un valore del bit pari ad 1 identifica un indirizzo LAA che viene generalmente assegnato da eventuali amministratori di rete.

La differenziazione del tipo di trasmissione in unicast e multicast avviene in maniera simile, in questo caso l'identificazione avviene mediante il bit meno significativo del primo ottetto.

Un valore pari a 0 equivale ad una trasmissione unicast mentre un valore pari ad 1 una trasmissione di tipo multicast. Infine, l'indirizzo di broadcast é ottenuto ponendo un valore pari ad 1 ad ogni bit dell'indirizzo MAC.

Come visto precedentemente, un MAC header é costituito da quattro indirizzi MAC il cui valore e significato varia in base al tipo di frame ed ai valori To DS e From DS. Gli indirizzi possono essere dei seguenti tipi:

- Receiver Address (RA): indirizzo della stazione che riceve il frame.
- Transmitter Address (TA): indirizzo della stazione che trasmette il frame.
- Basic Service Set Identifier (BSSID): indirizzo dell'access point della rete.
- Destination Address (DA): indirizzo di destinazione finale del frame.
- Source Address (SA): indirizzo sorgente del frame.

Nella figura 3.1 si mostrano le varie combinazioni che gli indirizzi MAC possono rappresentare in base ai valori presenti nel frame control.

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA=DA	TA=SA	BSSID	N/A
0	1	RA=DA	TA=BSSID	SA	N/A
1	0	RA=BSSID	TA=SA	DA	N/A
1	1	RA	TA	DA	SA

Tabella 3.1: Tabella uso indirizzi MAC

Management Frame

I frame di tipo management vengono utilizzati dalle stazioni e dall'access point per regolare l'accesso e disconnessione alla rete WLAN. Questo tipo di frame permette, durante la parte di analisi del traffico, di identificare gli access point attivi ed eventuali dispositivi che stiano cercando di accedervi.

Benchè i sottotipi definiti per questo tipo di frame siano 16 si elencano, in tabella 3.2, solo quelli effettivamente utilizzati dalla libreria per la costruzione topologica della rete.

Subtype	Descrizione
0001	Association Response
0100	Probe Request
1000	Beacon
1010	Disassociation
1100	Deauthentication

Tabella 3.2: Sottotipi Mgmt Frame

Il sottotipo di frame più interessante per questa operazione é quello di Beacon, che viene utilizzato dagli access point per annunciare la presenza di una rete WLAN alle stazioni vicine.

Nel frame body sono presenti 5 campi obbligatori:

- Timestamp: 8 byte che indicano il tempo di attività dell'access point.
- Beacon Interval: 2 byte che indicano la frequenza di invio di un beacon frame.
- Capability Information: 2 byte utilizzati per specificare funzionalità aggiuntive dell'access point.
- SSID: lunghezza variabile, identifica il nome logico di una rete WLAN.
- Supported Rates: specifica la velocità in Mbps che la stazione offre.

La libreria utilizza il Beacon frame per determinare se il MAC address del mittente sia un access point che avrà, eventualmente, una serie di dispositivi a lui connesso. In aggiunta, analizzando il radiotap header di un Beacon frame é possibile fornire un quadro completo sui dettagli della rete che viene annunciata, in particolare: canale in uso, potenza del segnale.

Come intuibile dalla descrizione, i frame di Association Response, Disassociation e Deauthentication indicano connessioni e disconnessioni di dispositivi alla rete wireless. In particolare i tipi di frame riguardanti le disconnessioni sono fondamentali per evitare di fornire una topologia della rete in cui vengano identificati come collegati dispositivi che non sono più appartenenti alla rete. Nonostante la loro importanza, la frequenza con cui questi

frame vengono analizzati dipende fortemente dal tipo di monitoraggio che si effettua: costante o ad istanti di tempo.

A differenza dei frame precedenti il Probe Request viene inviato da un dispositivo che si pone in cerca di reti WLAN a cui accedere e la sua analisi avviene solo per misurare parametri di bontà del segnale poichè il dispositivo non é connesso a nessuna rete.

Control Frame

I frame di tipo control assistono l'invio di frame management e data, amministrando l'accesso al mezzo trasmissivo wireless.

Come evidente dalla tabella 3.3 i principali frame che vengono analizzati corrispondono a quelli introdotti nella presentazione di DCF nel secondo capitolo.

Subtype	Descrizione
1001	Block Ack
1011	RTS
1100	CTS
1101	ACK

Tabella 3.3: Sottotipi Control Frame

In questo tipo di frame, come specificato da DCF, non é presente un frame body. Per questo motivo l'analisi dei control frame da parte della libreria é in grado di fornire solamente una relazione di connessione tra due indirizzi MAC e quindi due dispositivi.

Data Frame

I Data frame vengono utilizzati nel protocollo 802.11 per la trasmissione di dati provenienti da livelli superiori.

In tabella 3.4 si evidenziano i sottotipi di questo frame che vengono analizzati per la ricostruzione della topologia della rete WLAN.

La cattura e l'analisi di questi tipi di frame permette l'identificazione dei dispositivi su cui la trasmissione wireless termina o inizia.

Subtype	Descrizione
0000	Null No Data
0100	Data
1000	QoS Data
1100	QoS Null No Data

Tabella 3.4: Sottotipi Data Frame

Sfruttando questa informazione é quindi possibile identificare per ogni stazione che trasmette un frame il dispositivo a cui esso é collegato.

Come verrà esposto nella sezione successiva questo procedimento é fondamentale per la corretta rappresentazione della topologia di rete e permette di identificare il percorso dei frame inviati da un dispositivo anche in presenza di ripetitori Wi-Fi.

Analisi ed euristica

Il funzionamento della libreria può essere diviso in tre principali fasi delle quali si spiega, nel dettaglio, il funzionamento:

1. Cattura ed analisi dei frame 802.11.
2. Ispezione degli indirizzi MAC dei dispositivi presenti e di eventuali access point.
3. Topologia risultante.

La cattura dei frame 802.11, come precedentemente introdotto, viene effettuata mediante la libreria libpcap e impostando la scheda di rete Wi-Fi in modalità monitor. Durante questa procedura, per ogni frame ricevuto dalla scheda di rete, vengono analizzati il radiotap header ed il MAC header. In particolare, utilizzando il radiotap header, vengono estratte informazioni riguardanti la potenza del segnale della stazione che trasmette il frame ed il canale utilizzato per l'invio.

L'analisi del MAC header é cruciale per fornire una corretta ricostruzione della topologia di rete e comprende diversi controlli di correttezza. In primis viene effettuato un controllo sul FCS per poter scartare tutti i frame corrotti che vengono catturati. Se il pacchetto ricevuto é esente da errori, vengono successivamente analizzati gli indirizzi MAC in base al tipo e sottotipo di frame ricevuto. In questo controllo vengono scartati tutti pacchetti di tipo data e control i cui indirizzi destinatari sono di tipo broadcast, poichè questi tipi di frame non forniscono informazioni su alcun dispositivo connesso.

Soddisfatti questi requisiti gli indirizzi MAC presenti nel frame vengono considerati dispositivi Wi-Fi di interesse e memorizzati per poi poter esser nuovamente ispezionati al termine del procedimento di cattura.

Nel caso in cui il dispositivo analizzato abbia trasmesso almeno un frame di tipo beacon, questo viene considerato come un access point.

Per ogni dispositivo, in questo stadio dell'esecuzione, sono quindi noti i seguenti valori:

- Canale, potenza e rumore dell'antenna.
- Indirizzo MAC.
- Lista di indirizzi MAC con cui il dispositivo interagisce.
- Nome della rete annunciata (se AP).

La fase successiva necessaria per la ricostruzione della topologia di rete consiste nell'associare eventuali indirizzi MAC virtuali e multicast ai rispettivi indirizzi globalmente assegnati. Questo procedimento é necessario per evitare di includere nella topologia Wi-Fi indirizzi MAC che, in realtà, non appartengono a nessun dispositivo. Non é affatto raro, infatti, l'utilizzo di indirizzi virtuali da parte di repeater ed access point per la trasmissione in rete o l'uso di multicast da parte di router per l'invio di frame a singoli dispositivi. Il risultato ottenuto é un diretto collegamento tra un indirizzo virtuale al suo indirizzo globalmente assegnato, sia esso ottenuto mediante una precedente ARP scan o dalla cattura di frame 802.11.

Il passo successivo effettuato dalla libreria é quello di applicare un'euristica in grado di determinare se un dispositivo di rete abbia più di una antenna Wi-Fi ed in che modo queste vengano utilizzate. Gli attuali access point presenti in commercio aderiscono allo standard 802.11AC e sono quindi provvisti di una moltitudine di antenne wireless. Dopo lo studio di numerosi dispositivi di questo tipo si é formulata una euristica coerente con i comportamenti osservati, basata sulla divisione dell'indirizzo MAC in due sezioni:la prima comprendente i primi cinque ottetti e la seconda il restante ottetto. Infatti, gli indirizzi MAC delle varie antenne presente in questo tipo di dispositivi sembrano essere sempre maggiori in valore rispetto all'indirizzo fornito dal produttore. Considerando quindi tutti gli indirizzi MAC ottenuti dalla cattura di frame ed, eventualmente, anche dall'ARP scan si seleziona quello che presenta un valore minore nell'ultimo ottetto come l'indirizzo effettivo del dispositivo.

L'euristica presentata, in aggiunta a quella implementata per assegnare un indirizzo MAC globale ad uno localmente assegnato, risolve inoltre un altro problema emerso durante lo sviluppo della libreria riguardante l'utilizzo di indirizzi MAC da parte di repeater Wi-Fi. Durante lo studio approntato sono stati infatti individuati due metodi di funzionamento dei repeater, anche in dispositivi la cui unica differenza risiedeva nel firmware installato.

Uno dei metodi in cui i repeater trattano il traffico é quello intuitivo in cui i frame inviati e ricevuti dai dispositivi associati vengono trasmessi in

modo trasparente dal repeater stesso. In questo caso l'indirizzo MAC del repeater viene incluso nel frame 802.11 come TA.

Il secondo metodo osservato consiste nell'uso da parte del repeater di diversi indirizzi MAC per ogni dispositivo ad esso connesso. In particolare il MAC risultante é così definito: i primi tre ottetti corrispondono al LAA del repeater mentre gli ultimi tre ottetti corrispondono al NIC del dispositivo a lui connesso. La validazione di questi tipi di euristiche é rimandata al successivo capitolo.

L'ultimo passo effettuato dalla libreria é quello di creare due strutture facili da interpretare che rappresentino la topologia di ogni rete Wi-Fi nelle vicinanze.

Una struttura contiene una lista di tutte le reti wireless, in particolare:

- Indirizzo MAC dell'access point, canale della rete Wi-Fi, potenza segnale e rumore.
- Lista di indirizzi MAC dei dispositivi connessi alla rete, indicando se questi siano connessi direttamente all'access point o meno.

La seconda struttura contiene invece una lista di indirizzi tutti i dispositivi attivi nelle vicinanze ed un indirizzo a cui essi sono collegati, sia esso un access point o repeater, ed i valori di potenza segnale e rumore.

Capitolo 4

Validazione

In questo capitolo viene validato il lavoro svolto e vengono presentati i risultati ottenuti.

Capitolo 5

Conclusione

Bibliografia

[1] Cisco. *Cisco Visual Networking Index: Forecast and Trends, 2017–2022*. Rapp. tecn. Technical report, Cisco Systems Inc, 2019. URL: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html.

[2] Abdul Jabbar et al. «Performance Comparison of Weather Disruption-Tolerant Cross-Layer Routing Algorithms». In: apr. 2009, pp. 1143–1151. DOI: 10.1109/INFCOM.2009.5062027.

[3] D. Micheli et al. «Measurement of Electromagnetic Field Attenuation by Building Walls in the Mobile Phone and Satellite Navigation Frequency Bands». In: *IEEE Antennas and Wireless Propagation Letters* 14 (2015), pp. 698–702. ISSN: 1536-1225. DOI: 10.1109/LAWP.2014.2376811.

[4] Kismet Wireless. *Kismet*. URL: https://www.kismetwireless.net.

[5] IEEE. «IEEE standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications». In: (ago. 1999).

[6] Fouad Tobagi e Leonard Kleinrock. «Packet switching in radio channels: Part II-The hidden terminal problem in carrier sense multiple-access and the busy-tone solution». In: *IEEE Transactions on communications* 23.12 (1975), pp. 1417–1433.

[7] Giuseppe Bianchi. «Performance analysis of the IEEE 802.11 distributed coordination function». In: *IEEE Journal on selected areas in communications* 18.3 (2000), pp. 535–547.

[8] Haitao Wu et al. «Performance of reliable transport protocol over IEEE 802.11 wireless LAN: analysis and enhancement». In: *Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*. Vol. 2. IEEE. 2002, pp. 599–607.

[9] George Xylomenos e George C Polyzos. «TCP and UDP performance over a wireless LAN». In: *IEEE INFOCOM'99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No. 99CH36320)*. Vol. 2. IEEE. 1999, pp. 439–446.

[10] IEEE. «Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements». In: (nov. 2005).

[11] Stefan Mangold et al. «IEEE 802.11 e Wireless LAN for Quality of Service». In: *Proc. European Wireless*. Vol. 2. 2002, pp. 32–39.

[12] Yang Xiao. «Performance analysis of IEEE 802.11 e EDCF under saturation condition». In: *2004 IEEE International Conference on Communications (IEEE Cat. No. 04CH37577)*. Vol. 1. IEEE. 2004, pp. 170–174.

[13] Dionysios Skordoulis et al. «IEEE 802.11 n MAC frame aggregation mechanisms for next-generation high-throughput WLANs». In: *IEEE Wireless Communications* 15.1 (2008), pp. 40–47.

[14] Ubiquity. *UniFi*. URL: `https://www.ui.com`.

[15] *NetSpot*. URL: `https://www.netspotapp.com`.

[16] *inSSIDer*. URL: `https://www.metageek.com/products/inssider/`.

[17] David C. Plummer. *An Ethernet Address Resolution Protocol)*. RFC 826. Nov. 1982. URL: `https://tools.ietf.org/html/rfc826`.

[18] *Pcap*. URL: `https://www.tcpdump.org`.

[19] Guido Piero Zanetti e Claudio Enrico Palazzi. «Non-invasive node detection in IEEE 802.11 wireless networks». In: *2010 IFIP Wireless Days*. IEEE. 2010, pp. 1–5.