PresenceChecker
Gestione di Rete 2017/18

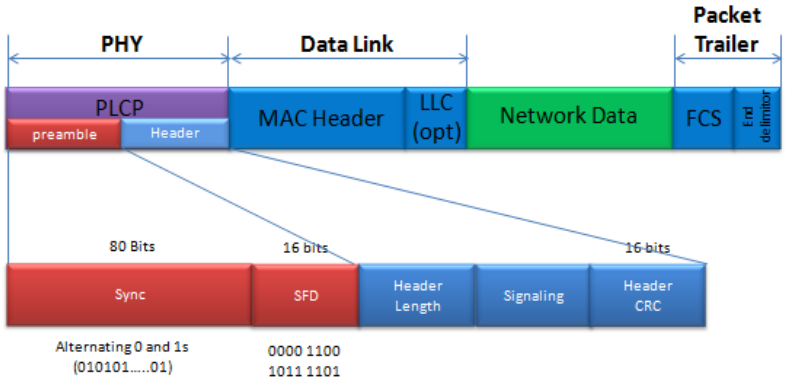
Vatteroni Francesco [468134]

2018/06/05 v0.1

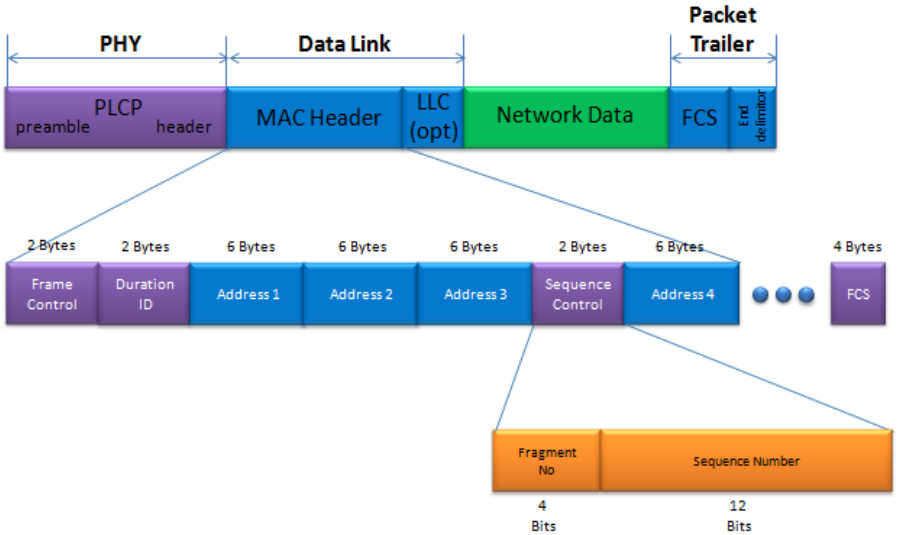
1 Introduzione

PresenceChecker è un software che si pone l'obbiettivo di monitorare la presenza, la prossimità e la permanenza di dispositivi wifi rispetto all' antenna presa in esame. Il tutto è possibile avendo due informazioni:

- Intensità del segnale
- Indirizzo MAC sorgente



L'intensità del segnale la si trova nel Radiotap Header, che stà a livello Fisico, codificata da 1 Byte nella parte Signaling. Più è alto il valore più è vicino il trasmittente.



L'indirizzo MAC sorgente, il quale lo possiamo considerare univoco per ogni dispositivo, si trova invece al livello Collegamento, nel MAC Header e sono i 6 Byte identificati da Address2.

2 Implementazione

Per l'attvità di monitoraggio dei pacchetti, si è scelto di utilizzare il tool airmon-ng, in modo da poter scegliere di settare l'interfaccia di rete in modalità monitor. Ho utlizzato la libreria pcapy per poter catturare i pacchetti Per la cattura dei pacchetti in transito, invece, si è utilizzata la funzione loop, della libreria pcapy. Successivamente, i pacchetti sono stati decodificati utilizzando degli appositi decoder, contenuti nella libreria impacket, in modo da poter leggere le informazioni desiderate (MAC address della sorgente, intensità del segnale). Nello specifico, sono stati utilizzati i decoder:

- RadioTapDecoder;
- Dot11ControlDecoder;
- DataDecoder;

che risultavano adatti allo scopo prefisso nel progetto.

3 Funzionamento

Il diagramma di sequenza in figura illustra il funzionamento, a livello di chiamate di funzione, di PresenceChecker. La struttura del programma è, come si vede, molto semplice: all'avvio del programma il main setta l'interfaccia di rete in modalità monitor. A questo punto, invoca la funzione mysniff, che si occupa di inizializzare tutte le variabili necessarie per la libreria pcapy e invocare, successivamente, la funzione loop. Questa ha al suo interno un ciclo infinito in cui viene invocato l'handler recv_pkts per ogni pacchetto ricevuto ed, ogni 5 secondi, viene chiamato un thread exporter, che esporta i dati ottenuti su un file. All'arrivo di un opportuno segnale di terminazione, il programma esce dal loop e le funzioni ritornano al main, che si occupa di riportare l'interfaccia di rete alla situazione precedente l'avvio.