Università degli studi di Pisa

Facoltà di scienze Matematiche, Fisiche e Naturali

CORSO DI LAUREA TRIENNALE IN INFORMATICA

GESTIONE DI RETE

Sistema di monitoraggio WI-FI

Studente: Ligorio Francesco

Matricola: 477000

Anno Accademico 2015/2016

Indice

Introduzione

Il tool rappresenta uno scanner di rete in grado di intercettare pacchetti relativi al protocollo IEEE 802.11 con lo scopo di analizzarli per estrapolare informazioni riguardanti gli access points (AP) nei paraggi.

L'IEEE ha definito le specifiche per le LAN wireless, chiamate IEEE 802.11, che copre i livelli fisico e di collegamento.

Lo standard IEEE 802.11 definisce due tipi di architetture, la BSS (Basic Service Set) e la ESS (Extended Service Set). La BSS è costituita da una o più stazioni wireless e da un AP facoltativo (nel nostro caso consideriamo architetture caratterizzate da AP). La ESS è invece caratterizzata da due o più BSS con infrastruttura (ovvero dall'access point e dal collegamento di questo con il router). In quest'ultimo caso i BSS sono collegati tra loro attraverso un sistema di distribuzione, che provvede proprio al collegamento tra gli AP dei diversi BSS.

L'architettura IEEE 802.11 prevede che una stazione wireless si associ ad un AP per poter accedere a internet. Avremo dunque il problema di capire in un determinato momento quali AP sono disponibili. Lo standard prevede che un AP possa pubblicizzarsi attraverso l'invio in broadcast di opportuni frame chiamati beacon. Tali beacon contengono informazioni di utilità relative all'AP e rappresentano uno dei due tipi di frame che lo scanner andrà ad intercettare ed analizzare. Uno dei concetti più importanti risulta dunque essere l'invio di questi beacon frame da parte degli access point, in quanto ci consentono appunto di individuarli e di associare loro un profilo identificativo. Considerando la necessità di elencare inoltre tutte le stazioni associate ad un certo AP avremo allora bisogno di intercettare anche un'altra tipologia di frame prevista dallo standard e chiamata data frame.

In particolare verrano estratte le seguenti informazioni relative ai vari AP:

- ESSID, una stringa che rappresenta il nome identificativo della rete;
- BSSID, ovvero il mac address associato all'AP;
- Channel (espresso in MHz), parametro che indica la frequenza di lavoro di un certo AP, in particolare ad ogni AP possono essere associate diverse frequenze;
- Signal (espresso in dBm), che rappresenta la potenza del segnale su una determinata frequenza;
- Stations, ovvero la lista di stazioni attualmente connesse a quel particolare AP. Ogni frequenza di lavoro dell'AP sarà dunque caratterizzata da una lista

L'applicazione è composta da tre file:

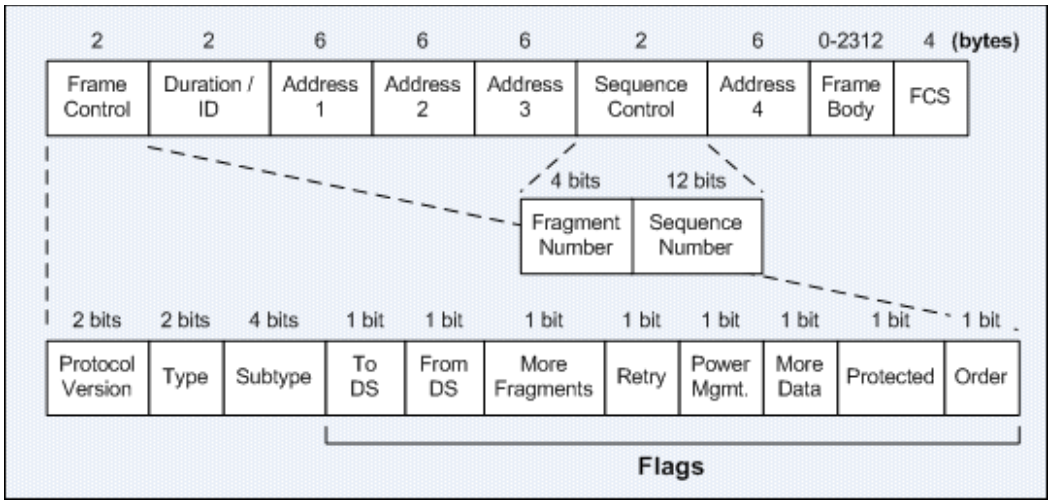
- sonda.c, rappresenta la parte fondamentale dello scanner, ovvero dove viene effettuata la cattura dei pacchetti interessanti e dove questi vengono analizzati per recuperare l'informazione ;

- support.c, contenente un insieme di funzioni di utilità utilizzate dal file precedente. In particolare in tale file vengono definite tutte le strutture dati utilizzate per il mantenimento dell'informazione recuperata;
- support.h, header relativo al file support.c contenente i prototipi di tutte le funzioni messe a disposizione dello scanner.

1. Dettagli implementazione

1.1 Formato dei frame e filtri di cattura

Un generico frame associabile allo standard IEEE 802.11 è caratterizzato dalla struttura seguente:



Il campo Frame Control consente di individuare i frame interessanti, che in questo caso risultano essere i beacon frame ed i data frame.

Per individuare i beacon frame è stato sufficiente applicare filtri sui campi Type e Subtype (il beacon frame è un particolare frame di tipo gestione dello standard che stiamo analizzando). Per quanto riguarda invece i data frame è stato scelto di applicare un filtro, oltre che sul campo Type (che appunto individua i frame dati), anche sui due campi da un bit "To DS" e "From DS" in modo da individuare specifici pacchetti di dati (ne esistono diversi). In particolare si vogliono analizzare i soli frame dati aventi come valori di "To DS" e "From DS" rispettivamente 1 e 0 in quanto questi pacchetti sono quelli che vanno da una stazione verso un access point; verranno individuate dunque solo le stazioni che generano traffico dati (tramite un'opportuna interpretazione dei campi "Address").

Un altro controllo significativo effettuato sul pacchetto è legato all'intestazione del livello collegamento in quanto l'unica gestita è la "Radiotap".

1.2 Strutture dati di supporto e consistenza dell’informazione

Per quanto riguarda le strutture dati utilizzate per il mantenimento dell’informazione si tratta di semplici liste, in particolare avremo un tipo di lista per contenere tutti gli AP ed un tipo di lista per contenere le stazioni associate agli AP.

La struttura dati è stata implementata per essere sempre in uno stato consistente, di conseguenza ci sarà un controllo (eseguito ogni volta che viene completata la scansione su tutte le 13 frequenze) che aggiorna la struttura “eliminando” di volta in volta le stazioni e gli AP che non vengono intercettati da un certo tempo (il timeout limite di validità è fisso ed è impostato a 20 secondi) e che dunque possono essere considerati non validi (ogni AP ed ogni stazione sarà quindi caratterizzata da un flag di validità). In realtà ogni elemento invalidato non verrà direttamente eliminato dalla struttura ma sarà unicamente marcato come non valido e dunque escluso dalla rappresentazione per l’utente finale; la ragione di questa scelta è legata alla possibilità per gli elementi di tornare ad essere validi, cosa che comporterebbe il reinserimento all’interno della struttura. Tutta la memoria allocata dinamicamente dal programma per consentire il salvataggio dell’informazione raccolta verrà dunque liberata solo al momento della terminazione dell’esecuzione.

Un’osservazione importante è quella relativa all’invalidazione di un generico AP. In particolare è stato scelto di effettuare il controllo sull’access point solo nel momento in cui una delle sue stazioni viene invalidata; questo evento infatti viene considerato sintomo di malfunzionamento in quanto se tutte le stazioni continuano a generare traffico verso un generico AP allora vuol dire che molto probabilmente questo è ancora attivo e dunque valido.

1.3 Output

Il tool è stato realizzato in modo tale da fornire istante per istante delle notifiche relative ai pacchetti che vengono catturati, inoltre, considerando che vengono scandite tutte le tredici frequenze disponibili, viene fornito un output aggiuntivo in formato JSON relativo a tutta l’informazione recuperata ogni volta che viene esaminato l’ultimo canale. La visualizzazione dell’output è legata alla presenza di un’opzione che verrà specificata nella sezione opportuna.

1.4 Gestione dei segnali

È stata prevista una gestione particolare per il segnale SIGINT. In particolare tale segnale esegue compiti di pulizia, infatti uno degli obiettivi principali è quello di liberare la memoria allocata dinamicamente dal processo per il mantenimento dell’informazione. Un ulteriore compito di questo gestore è quello di chiudere tutti i descrittori di file rimasti aperti e necessari al programma fino a quel momento (descrittore utilizzato per il cambio di frequenza ed handle di cattura dei pacchetti). Prima di terminare dunque l’esecuzione del programma stampa ancora una volta l’informazione presente nella struttura dati in formato JSON.

1.5 Utilizzo del tool

Risulta prima di tutto necessario eseguire il set per la modalità monitor della scheda di rete, procedura essenziale per essere in grado di intercettare i frame appartenenti allo standard di rete IEEE 802.11.

Una volta fatto bisognerà dunque lanciare il programma con due opzioni, di cui una obbligatoria:

- opzione “-i”, consente di specificare l’interfaccia di rete che dovrà essere utilizzata per la cattura dei pacchetti. Questa opzione deve necessariamente essere presente e deve essere seguita da un argomento che specifica appunto il nome di tale interfaccia;
- opzione “-v”, ovvero l’opzione che consente di visualizzare maggiori informazioni relative alla cattura in corso. In particolare consente di ottenere informazioni sui pacchetti catturati nell’istante corrente ed ogni volta che viene scandita l’ultima frequenza, prima dell’esposizione in JSON, vengono fornite informazioni aggiuntive riguardanti gli istanti di tempo degli ultimi aggiornamenti delle stazioni e degli AP a cui sono connesse. Questo consente dunque di rendersi conto dell’evoluzione della struttura col passare del tempo.