AirWatch - Analisi del traffico WiFi in monitor mode

Nome: Giovanni
Cognome: D'Alessandro
E-mail: g.dalessandro9@studenti.unipi.it

Indice:

1. Descrizione del Progetto

Il presente progetto si propone di configurare la scheda di rete in modalità monitor al fine di condurre un'analisi del traffico WiFi circostante, supportando sia la cattura in tempo reale dei pacchetti che l'analisi offline mediante l'utilizzo di file .pcap.

Tale analisi, comprende l'approfondimento dei pacchetti *beacon* e dei pacchetti *dati* conformi al protocollo 802.11, al fine di raccogliere informazioni essenziali sui punti di accesso WiFi nelle immediate vicinanze. I pacchetti beacon rappresentano i segnali periodici trasmessi dai punti di accesso per annunciare la propria presenza e le relative caratteristiche di rete, mentre i pacchetti dati includono le trasmissioni effettive di dati tra i dispositivi connessi alla rete.

Attraverso l'analisi di tali pacchetti, si mira ad identificare l'SSID, la frequenza operativa, l'antenna utilizzata, il canale di trasmissione, la potenza del segnale e il data rate di ciascun punto di accesso. Si intende, altresì, individuare e registrare gli indirizzi MAC dei dispositivi connessi a specifici punti di accesso.

1.1 Implementazione della monitor mode

La monitor mode è stata implementata mediante la funzione `set_monitor_mode__(),` in quanto l'uso diretto di `pcap_set_rfmon__()` non ha prodotto i risultati desiderati, nonostante il dispositivo supportasse nativamente la monitor mode, come confermato dall'output del comando `iw list`, tuttavia la sua abilitazione non avveniva correttamente.

Per risolvere questa problematica, è stata sviluppata la funzione `set_monitor_mode()` che si avvale dell'utilizzo di *airmon-ng*. Essenzialmente, airmon-ng fornisce una serie di funzionalità per la manipolazione delle interfacce wireless, consentendo operazioni come il cambio di modalità e la cattura del traffico.

La funzione `set_monitor_mode()` opera in due fasi:

- utilizza airmon-ng per interrompere tutti i processi in esecuzione che possono interferire con l'utilizzo della scheda di rete;
- una volta liberata da eventuali processi in conflitto, la modalità monitor viene abilitata manualmente.

1.2 Analisi dei pacchetti

Dopo aver impostato la modalità monitor, sia durante la cattura live che nell'analisi offline di un file .pcap; la funzione `process_packet()` è responsabile dell'analisi dei pacchetti. In particolare, questa funzione esamina il

byte 36 del pacchetto per determinare il frame type, distinguendo tra pacchetti beacon (0x80) e pacchetti dati (0x08).

Pacchetto Beacon:
L'analisi del pacchetto beacon è gestita dalla funzione `beacon_handler()`. Questa funzione si avvale dell'header RadioTap come struttura d'appoggio. RadioTap è un'intestazione utilizzata nei pacchetti WiFi che fornisce metadati relativi alla trasmissione radio, inclusi informazioni sul canale, la potenza del segnale, ecc…

La funzione `beacon_handler` estrae i seguenti campi dal pacchetto beacon:

- **Frequenza** I byte 27-26 contengono le informazioni sulla frequenza del canale WiFi.
- **Canale**: Utilizzando le informazioni sulla frequenza, viene calcolato il canale corrispondente.
- **RSSI** Il byte 30 contiene il valore del segnale ricevuto.
- **Numero antenna:** Il byte 35 fornisce il numero di antenna utilizzato per la trasmissione.
- **Data rate:** Il byte 25 indica il tasso di trasmissione dei dati.

Successivamente, la funzione determina l'offset dal quale inizia la parte dati del pacchetto utilizzando le informazioni fornite da RadioTap. Questo offset consente di estrarre ulteriori informazioni utili, come l'**SSID** e l'indirizzo **MAC** dell'access point..

Pacchetti Dati:
La funzione responsabile dell'analisi dei pacchetti dati è `data_handler()`. Questa funzione estrae le stesse informazioni presenti nei pacchetti beacon (anch'essa utilizza RadioTap), come la frequenza, il canale, il RSSI, il numero di antenna e il tasso di trasmissione dei dati. Tuttavia, il suo obiettivo principale è quello di ottenere il MAC Address del dispositivo associato a un determinato MAC Address dell'access point.

L'associazione tra il MAC Address del dispositivo e l'SSID dell'access point avviene utilizzando le informazioni precedentemente raccolte dai pacchetti beacon. In questo modo, è possibile ottenere una panoramica completa delle reti WiFi circostanti, inclusi i dispositivi connessi a ciascun access point e le relative informazioni di rete.

1.3 Strutture Dati Utilizzate

Per memorizzare i dati provenienti dai pacchetti beacon e pacchetti dati, è stata adottata un'organizzazione basata su una tabella hash.

1.3.1 Tabella Hash principale
La tabella hash principale utilizza:

- il MAC Address dell'access point come chiave;
- un puntatore a una struttura dati chiamata `WifiDevice`, che contiene le informazioni rilevanti dei pacchetti beacon;
- un'altra tabella hash chiamata HashDeviceTable, contenente i MAC Address collegati all'access point.

1.3.2 Struttura WifiDevice:
La struttura `WifiDevice` memorizza le informazioni dei pacchetti beacon relativi a un singolo access point. Tra i dati memorizzati vi sono l'SSID, la frequenza, il canale, il RSSI e altre informazioni rilevanti.

1.3.3 HashDeviceTable:
Ogni elemento della tabella hash principale contiene anche un puntatore a un'altra tabella hash, chiamata `HashDeviceTable`. Questa tabella hash contiene i vari MAC Address che hanno trasmesso pacchetti dati. Per ciascun MAC Address, viene mantenuto un contatore che tiene traccia di quanti pacchetti sono stati inviati da quel dispositivo.

1.4 Terminazione del Programma

1.4.1 Modalità Live:
Per terminare il programma in modalità live, è sufficiente premere CTRL+C. Questo interrompe l'esecuzione del programma in modo sicuro e controllato.

1.4.2 Modalità Offline:
In modalità offline, il programma termina automaticamente una volta completata l'analisi del file .pcap. Non è pertanto necessaria alcuna azione da parte dell'utente.

Una volta che il programma è terminato, viene fornita un'overview dei pacchetti analizzati. Questo include informazioni sulla rete nell'ultimo pacchetto beacon analizzato, come l'SSID, la frequenza e il canale. Successivamente, viene mostrato il numero dei dispositivi MAC che hanno trasmesso pacchetti dati per quella data connessione, oppure viene fornito un elenco dei MAC Address e il numero di pacchetti inviati da ciascun dispositivo.

Infine, una volta completata l'analisi e mostrate le informazioni pertinenti, la memoria allocata per le tabelle hash viene deallocata. Questo assicura una gestione efficiente delle risorse e previene eventuali perdite di memoria.

2. Prerequisiti ed Istruzioni per l'Esecuzione

Prima di utilizzare AirWatch, assicurati di soddisfare i seguenti prerequisiti:

- Installare `libpcap`:

```
sudo apt-get install libpcap-dev
```

- Installare `airmon-ng`:

```
sudo apt-get install aircrack-ng
```

Nota: assicurati di eseguire il programma come super utente.
Nota Bene: Dopo aver ripristinato la managed mode, AirWatch richiede l'avvio manuale del Network Manager. Si precisa che il programma è stato testato esclusivamente su Ubuntu, pertanto non sono note eventuali differenze di comportamento su altre distribuzioni Linux.

2.1 Istruzioni

1. Compilazione: utilizza il Makefile fornito per compilare il progetto digitando il comando

```
make
```

2. Esecuzione: per avviare il programma, esegui il seguente comando, dove `-i` indica l'interfaccia di rete o il path del file, mentre `-v` indica la modalità verbose, ossia se stampare gli indirizzi del MAC Address dei dispositivi che trasmettono pacchetti dati, oppure il solo numero.

```
sudo ./AirWatch_v1 -i <device|path> -v <1 | 2>
```

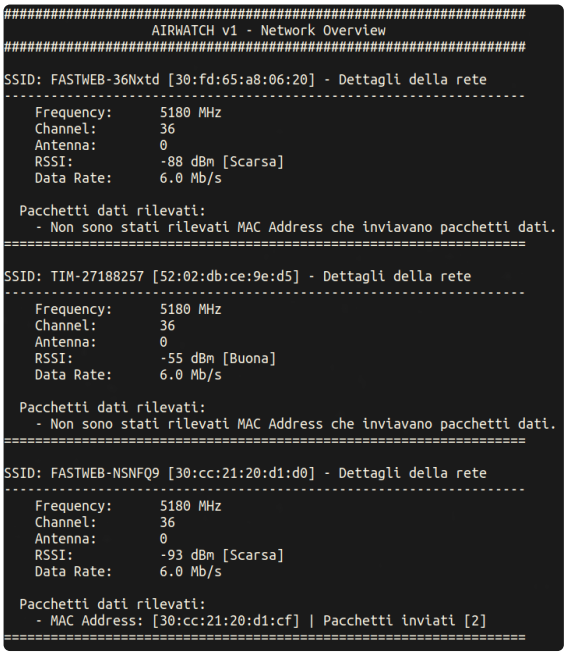
3. Aiuto: per visualizzare l'help, utilizza il comando:

```
sudo ./AirWatch_v1 -h
```

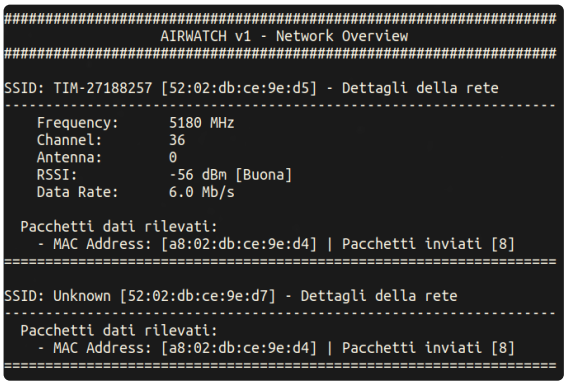
3. Test effettuati

Nel Makefile sono inclusi diversi test per valutare il funzionamento e le prestazioni del programma AirWatch. Di seguito sono elencati i test disponibili:

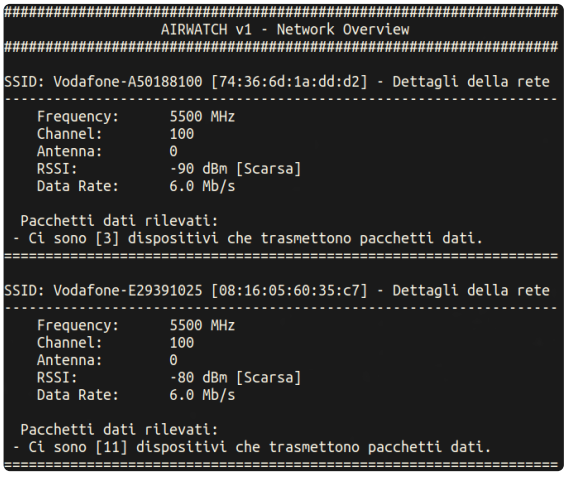
- `make test1`: File .pcap catturato in un ambiente domestico.



- `make test2`: File .pcap catturato in un ambiente domestico con un solo dispositivo collegato alla rete.



- `make test3`: File .pcap catturato mentre ci si sposta con il programma in funzione.



```
SSID: Wind3 HUB-EFA589 [d4:3d:f3:ef:a5:8a] - Dettagli della rete
---------------------------------------------------------------------
    Frequency:      5500 MHz
    Channel:        100
    Antenna:        0
    RSSI:           -90 dBm [Scarsa]
    Data Rate:      6.0 Mb/s

  Pacchetti dati rilevati:
 - Ci sono [7] dispositivi che trasmettono pacchetti dati.
=====================================================================

SSID: Unknown [62:3d:f3:ef:a5:8f] - Dettagli della rete
---------------------------------------------------------------------
  Pacchetti dati rilevati:
 - Ci sono [6] dispositivi che trasmettono pacchetti dati.
=====================================================================

SSID: Vodafone-C01600064 [08:16:05:be:91:fc] - Dettagli della rete
---------------------------------------------------------------------
    Frequency:      5500 MHz
    Channel:        100
    Antenna:        0
    RSSI:           -74 dBm [Debole]
    Data Rate:      6.0 Mb/s

  Pacchetti dati rilevati:
 - Ci sono [4] dispositivi che trasmettono pacchetti dati.
```

- `make test4`: File .pcap catturato presso un dipartimento dell'università.

```
#####################################################################
                    AIRWATCH v1 - Network Overview
#####################################################################

SSID: FASTWEB-2P5MT2 [7c:13:1d:d8:63:47] - Dettagli della rete
---------------------------------------------------------------------
    Frequency:      5520 MHz
    Channel:        104
    Antenna:        0
    RSSI:           -89 dBm [Scarsa]
    Data Rate:      6.0 Mb/s

  Pacchetti dati rilevati:
 - Ci sono [0] dispositivi che trasmettono pacchetti dati.
=====================================================================

SSID: UniPisa [30:86:2d:60:53:a0] - Dettagli della rete
---------------------------------------------------------------------
    Frequency:      5520 MHz
    Channel:        104
    Antenna:        0
    RSSI:           -84 dBm [Scarsa]
    Data Rate:      6.0 Mb/s

  Pacchetti dati rilevati:
 - Ci sono [565] dispositivi che trasmettono pacchetti dati.
=====================================================================

SSID: Teaching [30:86:2d:60:53:a1] - Dettagli della rete
---------------------------------------------------------------------
    Frequency:      5520 MHz
    Channel:        104
    Antenna:        0
    RSSI:           -83 dBm [Scarsa]
    Data Rate:      6.0 Mb/s

  Pacchetti dati rilevati:
 - Ci sono [0] dispositivi che trasmettono pacchetti dati.
=====================================================================
```

```
SSID: GuestUnipi [30:86:2d:60:53:a2] - Dettagli della rete
---------------------------------------------------------------------
    Frequency:      5520 MHz
    Channel:        104
    Antenna:        0
    RSSI:           -85 dBm [Scarsa]
    Data Rate:      6.0 Mb/s

  Pacchetti dati rilevati:
 - Ci sono [8] dispositivi che trasmettono pacchetti dati.
=====================================================================

SSID: eduroam [30:86:2d:60:53:a3] - Dettagli della rete
---------------------------------------------------------------------
    Frequency:      5520 MHz
    Channel:        104
    Antenna:        0
    RSSI:           -85 dBm [Scarsa]
    Data Rate:      6.0 Mb/s

  Pacchetti dati rilevati:
 - Ci sono [631] dispositivi che trasmettono pacchetti dati.
=====================================================================
```