Progetto del corso

Anno accademico 2017-18

Una delle caratteristiche degli smartphone è la loro capacità di riconnettersi rapidamente a una rete WiFi cui sono stati precedentemente associati, non appena si vengono a trovare all'interno della sua area di copertura. Tale comportamento è reso possibile dalla cosiddetta modalità di scansione attiva, per la quale, invece di attendere passivamente la ricezione di un pacchetto di tipo BEACON proveniente dall'access point, essi inviano, ad intervalli regolari, pacchetti broadcast di tipo PROBE REQUEST, eventualmente indicando il nome della rete a cui essi provano a connettersi.
Tale comportamento può essere utilizzato per realizzare un rilevatore di presenza, che determini, in una data area, una stima del numero di smartphone presenti.

Il dispositivo ESP32 possiede un'implementazione firmware dello stack WiFi che permette di registrare una callback che viene invocata ogniqualvolta venga ricevuto un pacchetto di tipo CONTROL, offrendo così la possibilità di rilevare sia la presenza di BEACON che di PROBE REQUEST.
Tale callback riceve come parametro una struttura dati che fornisce, oltre al pacchetto stesso ricevuto, anche altri metadati, tra cui la potenza del segnale ricevuto (RSSI – Received Signal Strenght Indicator). In condizioni ideali, tale valore decresce esponenzialmente al crescere della distanza ed è pertanto espresso in forma logaritmica (dB). Valori tipici variano tra -35/-40 (molto vicino) fino a -95/-105 (molto lontano, ai limiti della possibilità di ricezione). Nella realtà, vari fattori possono condizionare tale valore, tra cui la presenza di riflessioni multiple dovute al terreno, ai muri e agli altri ostacoli alla propagazione o le interferenze con altri segnali presenti nell'ambiente. In ogni caso, esso fornisce una stima approssimata della distanza.

Requisiti del sistema

Si realizzi un sistema di rilevazione a due (o più) punti, formato da dispositivi ESP32 disposti all'interno di un ambiente a opportuna distanza (in modo tale da sentirsi reciprocamente) e da un PC che agisca da collettore delle informazioni raccolte e ne permetta la elaborazione e la visualizzazione.

1. Ciascuno dei dispositivi ESP32 si mette in ascolto, per un periodo dell'ordine di un minuto, su un dato canale WiFi (da 1 a 13, in Europa), raccogliendo una lista di record riportanti come minimo l'indirizzo MAC del mittente, l'SSID richiesto (se presente), una marca temporale, l'hash del pacchetto, il livello del segnale ricevuto. Al termine del periodo, interrompono momentaneamente l'ascolto, si connettono al PC e inviano i dati raccolti, poi tornano ad ascoltare.
2. Le stazioni di ascolto devono avere la stessa base dei tempi, così che le marche da esse apposte siano compatibili. A tale scopo, nelle fasi iniziali di avvio del sistema e periodicamente durante il suo funzionamento, devono scambiare dati con il PC volti a allineare i propri orologi ed a mantenere la sincronizzazione.
3. Il software presente sul PC raccoglie ed archivia i dati ricevuti e determina se un determinato pacchetto (identificato dal suo hash) sia stato o meno ricevuto da tutti i dispositivi in ascolto e, nel caso, cerca di determinarne la posizione in funzione della potenza relativa riportata dalle stazioni di ascolto.

4. I dati così filtrati e arricchiti sono utilizzati per eseguire una stima del numero di dispositivi distinti rilevati continuativamente in un dato intervallo (5 minuti) all'interno dell'intersezione delle aree di copertura delle stazioni di ascolto; tale informazione è visualizzata sotto forma di grafico temporale;
5. La posizione stimata più di recente degli smartphone identificati è visualizzata dinamicamente sullo schermo del PC.
6. Il numero e la posizione nello spazio delle stazioni di ascolto deve essere un parametro di configurazione del sistema e una sua variazione non deve richiedere modifiche al software.

Possibili estensioni al sistema sono di seguito espresse.

Statistica di lungo periodo

I dati raccolti possono essere utilizzati per determinare quali indirizzi MAC siano stati ricevuti più di frequente in una data finestra temporale (anche di più giorni) e mostrarne una visualizzazione grafica sintetica, riportante, in quali intervalli tali dispositivi siano stati rilevati.

Riconoscimento di dispositivi con indirizzi nascosti

Alcuni dispositivi mobili (tipicamente quelli basati sulle versioni più recenti del sistema operativo iOS, ma anche alcuni Android), allo scopo di impedire il tracciamento, inviano i pacchetti di tipo PROBE REQUEST utilizzando, al posto del proprio indirizzo MAC globale, indirizzi locali (riconoscibili perché il secondo bit del primo byte è posto a 1) i cui bit restanti sono scelti casualmente, con variazioni anche molto frequenti (un nuovo indirizzo può essere generato ogni qualche secondo). Analizzando i restanti dati presenti nel pacchetto trasmesso, e la posizione stimata della stazione, è possibile trovare delle correlazioni che indicano come tale pacchetto possa essere riconducibile ad altri pacchetti precedentemente ricevuti. Si perfezioni l'analisi base con i dati ottenuti da tali correlazioni, indicando il margine di errore stimato.

Visualizzazione del movimento

Utilizzando i dati raccolti, il sistema visualizza, sotto forma di animazione controllabile, la successione delle posizioni dei singoli dispositivi all'interno dell'area per un dato intervallo temporale a scelta dell'utente del sistema.

Riferimenti

- Guida alla configurazione dell'ambiente esp-idf:
  https://esp-idf.readthedocs.io/en/latest/get-started/index.html
- Guida alla configurazione di Eclipse CDT
  https://esp-idf.readthedocs.io/en/latest/get-started/eclipse-setup.html (macOS e linux)
  https://esp-idf.readthedocs.io/en/latest/get-started/eclipse-setup-windows.html (windows)
- Dettagli sui pacchetti di tipo PROBE REQUEST
  https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/
- Presentazione di un sistema simile sviluppato presso l'INIRIA
  http://confiance-numerique.clermont-universite.fr/Slides/M-Cunche-2014.pdf