

UNIVERSITÀ DEGLI STUDI DI GENOVA

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

*Monitoraggio di flussi e densità pedonale nelle località turistiche delle “Cinque Terre“ mediante sniffer Wi-Fi*

TESI DI LAUREA MAGISTRALE

Gianluca Ceccoli

Relatore:

Prof. Roberto Sacile

ANNO ACCADEMICO 2018/2019

Sommario

[Sommario 2](#_Toc13056339)

[1. Introduzione 3](#_Toc13056340)

[2. Le Cinque Terre 4](#_Toc13056341)

[3. Stato dell’arte 5](#_Toc13056342)

[3.1. Dispositivi 6](#_Toc13056343)

[3.1.1. Videocamere 6](#_Toc13056344)

[3.1.2. Infrarossi e laser 7](#_Toc13056345)

[3.1.3. Sniffer 8](#_Toc13056346)

[3.2. Progetti di monitoraggio 9](#_Toc13056347)

[3.2.1. SAIL Amsterdam (2015) 9](#_Toc13056348)

[3.2.2. Europride (2016) 10](#_Toc13056349)

[3.2.3. Pellegrinaggio Hajj (2016) 10](#_Toc13056350)

[3.2.4. Il caso Venezia (2018) 11](#_Toc13056351)

[3.3. Tecnologia preesistente in loco 12](#_Toc13056352)

[4. Caso di studio: Wi-Fi 13](#_Toc13056353)

[4.1. MAC Address 13](#_Toc13056354)

[4.2. Sniffer Wi-Fi 14](#_Toc13056355)

[5. Bibliografia 17](#_Toc13056356)

1. Introduzione

La crescita sempre più rapida della popolazione nel mondo e la conseguente urbanizzazione hanno portato a un incremento nel numero di attività come eventi sportivi, raduni politici, dimostrazioni pubbliche ecc. che risultano in più frequenti raduni di folle. In questi scenari, la Crowd Analysis sta ricevendo crescente attenzione per poter assicurare miglior gestione della folla o riconoscimento automatico di situazioni potenzialmente pericolose. Il rilevamento di situazioni anormali può migliorare significativamente l’efficienza della sorveglianza, risparmiando l’attenzione umana per i casi più importanti, previa segnalazione di un sistema.

Il costo sempre più accessibile dei sistemi di videosorveglianza, ha come conseguenza che i metodi tradizionali per il monitoraggio del traffico pedonale facciano affidamento su tecnologie basate su acquisizione video o contapersone (fotocellule o barriere laser) che tuttavia sollevano questioni estetiche o di sicurezza per i dispositivi stessi, oltre a quelle legate alla privacy delle immagini registrate. Come ogni altro problema di Computer Vision, la Crowd Analysis comporta molte sfide da affrontare come occlusioni, distribuzione non uniforme delle persone, illuminazione variabile o prospettive sfavorevoli che rendono l’analisi particolarmente difficile.

D’altra parte, l’ammodernamento dei dispositivi mobili e la propensione dell’uomo a possederne uno, ha permesso che il monitoraggio dei cellulari possa competere nel campo della stima dei movimenti del traffico pedonale. Se il sistema di rilevazione è dotato di ricevitori Wi-Fi, è possibile catturare l’origine-destinazione (O-D) di un pedone, il suo travel time, wait time ricavando informazioni sul flusso di un sottoinsieme di pedoni, possessori di devices con modulo Wi-Fi acceso.

Lo scopo principale di questo elaborato è quello di studiare la fattibilità di implementazione di un sistema di monitoraggio di flussi impiegando degli sniffer Wi-Fi i cui dati saranno integrati con quelli disponibili da altri mezzi di monitoraggio preesistenti, che consenta, in tempo reale o semi-reale, di stimare l’afflusso pedonale in aree particolarmente predisposte a congestionamenti come i borghi delle Cinque Terre. L’idea è quella di installare più stazioni Wi-Fi, inizialmente in posizioni strategiche nella sola zona di Manarola per poi valutare una possibile espansione ai restanti 4 paesi. Una prima fase consiste nella definizione del network di sensori atti al monitoraggio dei flussi turistici. Una seconda fase prevede la progettazione e realizzazione di una base di dati per gestire in modo centralizzato i dati provenienti dalla rete di sensori. Come ultimo passo, sarà necessario rendere i dati disponibili in forma grafica agli utenti accreditati mediante un ambiente WebGIS.

Nel secondo capitolo verrà fornita una breve panoramica delle Cinque Terre e della loro topografia. Nel terzo capitolo verrà discusso lo stato dell’arte riguardo i dispositivi di monitoraggio, i passati esperimenti di stima del flusso pedonale in grandi eventi e le risorse già esistenti in loco, disponibili ad essere integrate nel sistema di monitoraggio alle Cinque Terre. Nel quarto capitolo mi concentrerò più nel dettaglio sul caso di studio preso in considerazione, riportando i dettagli tecnici di come sono realizzati e impiegati i sensori Wi-Fi.

1. Le Cinque Terre

Immagine che contiene testo, mappa

Descrizione generata con affidabilità molto elevata

Figura 1 Overview del Parco Nazionale delle Cinque Terre

Il Parco Nazionale delle Cinque Terre è un frastagliato tratto di costa della [Riviera ligure](https://it.wikipedia.org/wiki/Riviera_ligure) [di levante](https://it.wikipedia.org/wiki/Riviera_di_levante) situato nel territorio della [provincia di La Spezia](https://it.wikipedia.org/wiki/Provincia_della_Spezia) tra Punta Mesco e Punta di Montenero, nel quale si trovano cinque borghi, da [ovest](https://it.wikipedia.org/wiki/Ovest) verso [est](https://it.wikipedia.org/wiki/Est): [Monterosso al Mare](https://it.wikipedia.org/wiki/Monterosso_al_Mare), [Vernazza](https://it.wikipedia.org/wiki/Vernazza), [Corniglia](https://it.wikipedia.org/wiki/Corniglia), [Manarola](https://it.wikipedia.org/wiki/Manarola) e [Riomaggiore](https://it.wikipedia.org/wiki/Riomaggiore). Nel 1997 l'UNESCO ha inserito le [Cinque Terre nella lista del Patrimonio Mondiale dell'Umanità](http://whc.unesco.org/en/list/826) come "paesaggio culturale".

Gran parte dei parcheggi sono riservati ai residenti e in ragione della mancanza di spazi adeguati, la discesa ai borghi è possibile solo a piedi. Esiste tuttavia un servizio di bus elettrici gestito dal Parco Nazionale che nei periodi di maggior afflusso turistico garantisce i collegamenti. Nella stagione turistica un servizio di battelli di linea collega tutti i borghi ad eccezione di Corniglia (che non è situata sulla costa) con Porto Venere, a sua volta collegata con La Spezia, [Lerici](https://it.wikipedia.org/wiki/Lerici) e con gli altri paesi della riviera di Levante. Data la situazione geografica piuttosto impervia dei borghi, il mezzo di trasporto di gran lunga più utilizzato per raggiungerli è la ferrovia che fa tappa in tutte le terre e vede una notevole frequenza di transiti. Una volta nei pressi dei paesi, esistono due sentieri principali che i turisti percorrono per visitare il Parco. Il primo (sentiero numero 1) è conosciuto come Alta via delle Cinque Terre e collega Levanto con Portovenere. Permette di percorrere un tragitto più elevato e nell’entroterra rispetto al secondo ma è attraversato da molti sentieri trasversali che consentono di raggiungere la costa. Il secondo sentiero (sentiero numero 2), meglio conosciuto come Sentiero Azzurro, è quello più apprezzato dai turisti. Collega le Cinque Terre con un percorso sul litorale e regala parecchi scorci panoramici. Visto il suo successo, l’accesso è regolato tramite l’acquisto della Cinque Terre Card.

A causa della storicità dei sentieri e per motivi di sicurezza, alcuni tratti vengono spesso chiusi/manutenuti secondo le necessità più o meno impreviste. [1]

1. Stato dell’arte

La Crowd Analysis può essere effettuata su due livelli: quello microscopico e quello macroscopico. Il primo si focalizza sul singolo individuo all’interno di una folla e come per esempio questo interagisca con gli altri pedoni o con l’ambiente in cui è immerso con modelli che sono computazionalmente più onerosi rispetto a quelli macroscopici. Per contro, i modelli macroscopici tendono a considerare la folla come se fosse un fluido [2] e pertanto forniscono misure più approssimate. Ai diversi punti di vista corrispondono due facce della stessa medaglia per ogni problema che si considera. Quelli a cui siamo interessati sono il conteggio di persone e il tracking dei loro movimenti, che secondo l’interpretazione microscopica assumono il significato rispettivamente di LOI (line-of-interest counting), che conta il numero di persone che passano attraverso una data linea virtuale, e del tracking individuale di ogni pedone registrando la sua velocità istantanea e la sua direzione. Se invece consideriamo la prospettiva macroscopica questi due problemi si identificano con ROI (region-of-interest counting), che conta il numero di persone in una data regione, e con il tracciamento generico della folla, registrando la sua velocità media e direzione del flusso.

Un importante aspetto delle folle è la loro densità ed è naturale pensare che folle di diverse densità dovrebbero ricevere diversi livelli di attenzione. Gli studi effettuati prima da Fruin [3] e poi ripresi da Polus et al. [4] ci forniscono una chiara idea del problema del *livello del servizio* per il traffico pedonale definito come: flusso libero, flusso limitato, flusso denso e flusso interrotto in accordo con una misura della densità definita come il numero di pedoni per unità di area. Weidmann inoltre dimostrò empiricamente che lo scopo dello spostamento influisce sulla velocità di moto [5] che per il traffico turistico o ricreativo stimò essere 0.99 m/s. Le stime sulla densità e sul movimento della folla ci possono aiutare a stabilire se siano in atto o meno comportamenti anormali o allarmanti [6] e a gestire situazioni potenzialmente pericolose.

Le soluzioni a LOI condividono tre step fondamentali: rilevazione del foreground per discriminare i pixel in movimento rispetto a quelli statici dello sfondo, riconoscimento di ogni singola persona nella scena e tracciamento della sua traiettoria per aumentare il contatore nel momento in cui questa interseca la linea virtuale d’interesse. Le differenze tra i vari metodi ricadono nell’approccio utilizzato per ogni step e nel tipo di dispositivo utilizzato. I primi tentativi nel conteggio delle persone sono progettati per processare i video catturati da telecamere RGB. Molti di questi metodi utilizzano combinazioni di rilevazione del foreground come frame differencing o background subtraction.

|  |  |
| --- | --- |
| Figura 2 Frame originale | Figura 3 Estrazione foreground |

Il problema principale di queste soluzioni è che presentano diverse difficoltà in scenari molto affollati e soggetti a cambiamenti di luce. Per limitare l’impatto di questi problemi, hanno cominciato a sorgere studi su come svolgere un’analisi 3D per sfruttare l’informazione riguardo la profondità. I primi metodi che seguono questa linea di pensiero erano basati sull’utilizzo di telecamere stereoscopiche anche se con l’uscita di Microsoft Kinect, che utilizza la luce strutturata, nuove opportunità si sono aperte proprio con l’utilizzo di questo device [7], [8].

In questo capitolo verrà presentata una panoramica dei dispositivi esistenti da impiegare nel monitoraggio del traffico pedonale e delle esperienze di significativa importanza in cui sono stati utilizzati.

* 1. Dispositivi

Esistono diversi tipi di dispositivi che vengono quotidianamente utilizzati in questo campo: dispositivi che acquisiscono immagini, laser, fotocellule e sniffer. Le prime tre categorie riescono a gestire più o meno bene l’informazione riguardo il numero di ingressi/uscite da un varco, quindi problemi di tipo LOI. Le telecamere, inoltre, possono essere impiegate anche per la stima della densità pedonale nelle immagini catturate (ROI). Gli sniffer, in particolare WiFi, si distinguono per la loro versatilità, specialmente se utilizzati in sinergia con molteplici esemplari.

* + 1. Videocamere

I metodi convenzionali si approcciano al problema della Crowd Analysis utilizzando generiche telecamere a colori o in scala di grigio e si possono dividere in tre categorie: rilevamento e tracking dei pedoni, regressione sulla base di feature e clustering delle traiettorie. I fotogrammi possono anche essere utilizzati per rilevare comportamenti anomali nella folla [6] o, grazie a metodi recenti basati su deep learning, per fornire una stima della densità di questa [9], [10], [11].

Nonostante siano stati fatti grandi progressi, i problemi menzionati sono ben lontani dall’essere risolti a causa di svariate sfide che includono cambiamenti nell’illuminazione, ombre, occlusioni e diversità nell’aspetto dei pedoni. Inoltre, molte delle soluzioni si basano su immagini ad alta risoluzione e modelli complessi che rendono difficile l’applicabilità real-time. Per migliorare le performance del conteggio e per ridurre la complessità computazionale, sono stati proposti diversi metodi che sfruttano sensori di profondità differenti (Kinect, telecamere a tempo di volo, telecamere stereoscopiche ecc) in sinergia o in sostituzione alle telecamere RGB [7], [12], [13].

Sul mercato vi sono molteplici soluzioni, relativamente a basso costo, molte delle quali sfruttano appunto telecamere stereoscopiche [14], [15].

|  |  |
| --- | --- |
| Figura 4 Telecamera stereoscopica Hikvision iDS-2CD6810F/C | Figura 5 Frame tratto dalla telecamera a sinistra [16] |

Da tenere in considerazione l’impatto estetico non indifferente che l’installazione comporta e il fatto che in generale, per grandi masse, l’accuratezza dell’analisi cala. Trattando immagini, se il software non considera il problema, possono sorgere controversie riguardo la privacy e per conteggiare il numero di ingressi/uscite da un varco vi è il vincolo del posizionamento presso la verticale dello stesso.

* + 1. Infrarossi e laser

Infrarossi e laser forniscono un’alternativa efficiente ai problemi sopra menzionati. In studi passati, telecamere ad infrarossi, scanner laser o una combinazione dei due sono stati impiegati in questo campo. Grazie all’abilità di acquisire immagini tramite radiazioni di calore, le camere IR forniscono caratteristiche uniche mentre grazie agli scanner laser si possono ottenere informazioni sulla profondità. In aggiunta, con device laser, immagini ad alta risoluzione non sono necessari, riducendo di molto la complessità computazionale e rendendo le operazioni idonee ad un ambiente real-time. Wu et al. [17] mostrano un approccio innovativo basato su un laser ad infrarossi multipunto per ricavare l’informazione sulla profondità e costruire un modello spaziale dello sfondo per l’individuazione delle persone senza il bisogno di immagini ad alta risoluzione.

STMicroelectronics [18] ci dimostra come la ricerca in questo campo stia dando vita a soluzioni sempre più convenienti e minimali [19]. LZR-SIGMA, per esempio, è un dispositivo laser ad infrarossi con misura a tempo di volo [20] facilmente reperibile sul mercato europeo.

|  |  |
| --- | --- |
| Immagine che contiene oggetto  Descrizione generata con affidabilità elevata  Figura 6 LZR®-SIGMA. Soluzione contapersone laser con campo di rilevazione ad alta risoluzione (250 punti per battente) | Immagine che contiene edificio, esterni, strada, terra  Descrizione generata con affidabilità molto elevata  Figura 7 SIGMA possiede un sistema di conteggio affidabile che offre una misurazione accurata del flusso di adulti, bambini e gruppi di persone. |

* + 1. Sniffer

Considerata la notevole importanza che gli smartphone stanno a mano a mano acquisendo per via della loro capacità di accedere al web utilizzando dati mobili e reti Wi-Fi, rispecchiando talvolta in scenari distopici la figura di estensione del nostro corpo, l’analisi del traffico wireless si è rivelata un’ottima alternativa ai metodi convenzionali sopracitati. Si definisce sniffing (eavesdropping) l’attività di intercettazione passiva dei dati che transitano in una rete. I software che sono in grado di captare i singoli pacchetti del traffico Internet prendono il nome di sniffer e quelli Wi-Fi necessitano di un modulo wireless che stia in ascolto del traffico. Laddove i metodi di videosorveglianza o quelli basati su laser e IR si applicano molto bene ad analisi di tipo LOI, facendo leva sull’attaccamento che l’uomo ha per il proprio dispositivo mobile, gli sniffer Wi-Fi trovano efficace impiego nella stima delle densità, flussi e tempo di viaggio. Recenti studi vedono impiegati molteplici sniffer che in sinergia rendono possibile la stima della posizione di un dispositivo mobile all’interno di un’area schematizzabile in celle grazie a tecniche di machine learning [21], la stima della densità di persone all’interno di un centro commerciale [22], la stima del flusso e dei percorsi pedonali [23], [24], [25] o il monitoraggio di grandi eventi come il pellegrinaggio Hajj verso la Mecca [26].

Esistono alcuni prodotti specializzati [27] ma la maggior parte degli scienziati, che in questi anni hanno cercato di sfruttare questo metodo di monitoraggio emergente, si affida ancora a soluzioni “casalinghe”, spesso costituite da una o più stazioni composte da un single-board computer (come Raspberry Pi [28]) con un modulo Wi-Fi usb esterno. Il motivo di questa scelta risiede nell’installazione di un sistema che, a differenza di quelli di videosorveglianza, risulta economico, semplice e senza la necessità di hardware aggiuntivo.

L’ottenimento di informazioni tramite lo sniffing Wi-Fi di per sé non è un processo complicato anche perché una delle caratteristiche delle reti wireless è proprio quella di essere broadcast. I dispositivi con il modulo Wi-Fi acceso, infatti, sono regolarmente in cerca di connettività. Mandano continuamente richieste per cercare reti a cui hanno già effettuato un accesso in passato. Queste richieste contengono tra le altre cose, informazioni che consentono l’identificazione del dispositivo inviante. Lo scopo però che in questo caso si vuole raggiungere tramite lo sniffing, ovvero la Crowd Analysis, comporta uno studio non banale, dovuto a varie ragioni. In primo luogo, i dati ottenuti sono quelli di un sottoinsieme del traffico reale, in cui il penetration rate dei dispositivi con Wi-Fi attivato gioca un ruolo fondamentale. In secondo luogo, la rilevazione di un dispositivo dipende in primis da esso stesso poiché, nonostante il corretto funzionamento del Wi-Fi, può risultare comunque momentaneamente invisibile. Infine, a seconda dei casi, i dispositivi potrebbero non lasciare un’impronta univoca e quindi il conteggio andrebbe a considerare dei doppioni o peggio triple, quadruple e via dicendo copie come entità separate.

Nel capitolo 4 verrà fornita una spiegazione tecnica di come sia possibile eseguire lo sniffing dei dispositivi mobili e di come sia stato sviluppato il nostro sistema di sniffer Wi-Fi.

* 1. Progetti di monitoraggio

Oggigiorno, molti eventi di larga scala sono ospitati in aree urbane che non sono progettate per ricevere questo grande afflusso di spettatori. Oltre al numero di visitatori fuori misura, il comportamento di queste folle è spesso imprevedibile e non contemplato. Mai come in questo periodo sono necessari sistemi di monitoraggio delle folle che forniscano informazioni real-time riguardo lo stato del traffico pedonale sull’area dell’evento per garantire la sicurezza dei visitatori prevenendo situazioni di pericolo e colli di bottiglia o identificandole tempestivamente.

Di seguito sono riportati alcuni tentativi di monitoraggio effettuati in passato durante eventi di larga scala i quali hanno utilizzato più tecnologie contemporaneamente per avere una visione il più completa possibile della situazione.

* + 1. SAIL Amsterdam (2015)

Immagine che contiene esterni, cielo

Descrizione generata con affidabilità molto elevataSAIL è un evento marittimo quinquennale che si tiene ad Amsterdam, in Olanda [29]. Ha il vanto di essere una delle più grandi (se non la più grande) manifestazione nautica al mondo e senz’altro il più grande evento pubblico Olandese. Ogni cinque anni più di 600 navi tra velieri, fregate, natanti, navi moderne, militari e repliche di imbarcazioni storiche navigano lungo il canale del mare del Nord per poi ormeggiare al porto di Ijhaven ad Amsterdam. Il legame tra Amsterdam e il mare è profondo e SAIL non è solo un’esibizione di grandi navi. In poche parole, comprende “qualsiasi cosa che galleggi” e durante l’edizione del 2000 si raggiunse l’impressionante numero di 8000 imbarcazioni. Accanto alle attività in acqua ci sono molte attrazioni anche a terra come musica, arte, cultura e tante attività per bambini.

SAIL fu organizzato per la prima volta nel 1975 e visto il grande successo, si è deciso di ripetere l’evento in forma quinquennale, riunendo nelle recenti edizioni circa 2 milioni di persone sul territorio.

Figura 8 La Amerigo Vespucci italiana

Durante SAIL 2015, una combinazione di sistemi di conteggio video, tracciatori GPS e sensori Wi-Fi fu impiegata per determinare lo stato del traffico pedonale [30], [31]. I dati vennero raccolti utilizzando 8 telecamere per conteggio, 20 sensori Wi-Fi e 324 tracciatori GPS furono distribuiti ai visitatori per registrare le loro traiettorie. Il problema fondamentale dello studio però fu che non c’era una vera e propria conoscenza assoluta (in termini tecnici ground-truth) del traffico reale a cui fare riferimento, ma i calcoli vennero comparati alle immagini registrate da altre telecamere aeree. Le 8 telecamere ebbero il compito di calcolare il numero di pedoni che attraversano una sezione trasversale. In teoria, i dispositivi impiegati avevano un’accuratezza del 98% decrescente a 92% in situazioni di alta densità ma nessuna considerazione su velocità o percorsi può essere fatta con questi dati.

I sensori Wi-Fi invece ebbero lo scopo di derivare i flussi e il tempo di percorrenza, acquisendo informazioni riguardo i pedoni dotati di un qualsiasi dispositivo mobile (es. smartphone) all’interno del loro raggio d’azione. I dati contenenti i gli indirizzi MAC dei dispositivi, l’ID del sensore e il primo e ultimo timestamp di rilevamento di ogni dispositivo rendono possibile il calcolo cumulativo dei singoli dispositivi e dei tempi di attraversamento da sensore a sensore (supponendo che ad un dispositivo corrispondesse un pedone).

Confrontando i dati ottenuti dai sensori Wi-Fi e dalle telecamere, si nota che i sensori percepirono circa un terzo dei pedoni conteggiati dalle telecamere e la metà di questi (quindi 1/6) corrispondono a dispositivi unici. Nonostante un penetration rate così basso, i calcoli eseguiti su approssimativamente 2.3 milioni di visitatori sono sufficienti per avere un’idea dei percorsi effettuati e sui tempi di tragitto per alcune tratte. Per impiegare i sensori Wi-Fi nella stima della densità tuttavia, sono necessarie stime accurate sul penetration rate (rapporto tra pedoni totali e numero di dispositivi mobili rilevati) in modo da poter stimare in maniera più accurata il traffico reale.

Nello studio citato vengono illustrati nel dettaglio 3 algoritmi di stima dello stato per stimare travel time, densità e flussi [31].

* + 1. Europride (2016)
    2. Pellegrinaggio Hajj (2016)

Hajj è il tradizionale pellegrinaggio annuale verso la Mecca. Essendo il quinto pilastro dell’Islam e momento di purificazione per i fedeli, l’Hajj è considerato il pellegrinaggio più grande al mondo in cui si riuniscono 2-3 milioni di musulmani provenienti da tutto il globo. L’Hajj è una sequenza di riti praticati in tempi e luoghi prestabiliti e questi vincoli spazio-temporali rendono la gestione dell’Hajj un processo complesso. È con lo studio di come si comportano i pellegrini, dei loro pattern, delle interazioni, delle necessità e domande che si può fornire un livello di servizio soddisfacente. Con questo pensiero, A. Basalamah [26] installò un sistema composto da 8 sniffer Wi-Fi autoalimentati a energia solare in una delle aree destinate ad ospitare i pellegrini per un giorno, Arafat, 12 km a sudest della Sacra Città della Mecca. Arafat è un’area deserta per tutto il resto dell’anno in cui durante il pellegrinaggio vengono allestite delle tende per i fedeli e nel 2016 furono stimate 185.000 persone. La collezione dei dati cominciò due giorni prima del picco stimato e continuò per i successivi tre giorni. I risultati ottenuti mostrarono che il sistema fu in grado di rilevare circa il 37.5% della folla, corrispondente a 69.467 dispositivi unici. Dalla rete di sensori, Basalamah fu in grado di identificare le aree più affollate, stabilire gli orari dei picchi di mobilità, estrapolare informazione riguardo lo stato economico dei pellegrini avendo a disposizione le marche delle case produttrici dei dispositivi e diverse altre statistiche.

Figura 9 Dispositivi unici per giorno

Figura 10 Dispositivi unici per ora (giorno di picco)

* + 1. Il caso Venezia (2018)

**VENIS - Venezia Informatica e Sistemi S.p.A.** è l'azienda di servizi ICT e l’operatore locale di comunicazioni elettroniche del Comune di Venezia. Nei primi mesi del 2018, VENIS ha aperto un bando rivolto a soggetti privati ad offrirsi per una sperimentazione gratuita di impianti atti al conteggio dei flussi pedonali nelle aree limitrofe alla Stazione Santa Lucia ed in Piazza San Marco. Le sperimentazioni hanno visto come oggetto l’installazione gratuita e il test di impianti tecnologici e/o sensoristica e/o videorilevazione nelle aree del Centro Storico di Venezia. In sei mesi, i prodotti di sei ditte sono stati messi a confronto e per ognuno è stato stilato un resoconto riguardo tipologia del sensore, attendibilità, flessibilità, installazione, estetica e disponibilità dei dati. I dispositivi presi in analisi si riferiscono a laser, telecamere steroscopiche, sniffer Wi-Fi, telecamere ad infrarossi e telecamere con annesso software per il riconoscimento di transiti. Di seguito viene riportata una tabella riassuntiva, ma è disponibile alla lettura il report completo [32].

Immagine che contiene screenshot

Descrizione generata con affidabilità molto elevata

Figura 11 Sintesi dei risultati

* 1. Tecnologia preesistente in loco

1. Caso di studio: Wi-Fi

Lo standard IEEE 802.11 definisce tre tipi di frame che vengono scambiati dai dispositivi Wi-Fi: Management frames, Control frames e Data frames. I sistemi sniffer in esame fanno leva sulle informazioni contenute nei Management frames per cui gli altri due tipi di non verranno menzionati oltre. Per quanto riguarda i Management frames, esistono quattro principali categorie di frame: Beacons, Probes, Association e Authentication a loro volta divisi in altri sottotipi.

I Beacon frames (sottotipo 0x08) sono messaggi che gli AP (access point) inviano periodicamente in modalità broadcast per segnalare ai dispositivi nei dintorni la propria esistenza e il proprio SSID. Le Probe requests (sottotipo 0x04) sono dei frame speciali inviati da una stazione client che richiede informazioni da un particolare AP specificato da un SSID o da tutti quelli nei dintorni con un SSID broadcast. L’invio di una Probe request avviene quando la scheda wireless del dispositivo sta eseguendo il cosiddetto active scanning, cioè la ricerca attiva di AP che secondo risultati empirici dovrebbe avvenire almeno una volta ogni due minuti [x], mentre il semplice ascolto dei frame Beacon è denominato passive scanning. In seguito ad una Probe request, gli AP emettono una Probe response (sottotipo 0x05) contenente le informazioni necessarie a stabilire una connessione.

Ogni dispositivo elettronico porta con sé un’informazione univoca, un indirizzo MAC (media access control) che può essere intercettato quando esso tenta di collegarsi ad una rete wireless o il collegamento è già stato effettuato perché è contenuto in chiaro nelle Probe requests. È quindi mediante lo sniffing di queste richieste, durante la fase di active scanning, che si possono collezionare informazioni riguardo i client (nel nostro caso gli smartphone dei turisti) come indirizzo MAC, potenza del segnale (RSSI), timestamp, sequence number della richiesta e svariati altri dati. Come intuibile, le Probe requests sono più frequenti quando il dispositivo non è connesso a nessuna rete e la loro frequenza diminuisce drasticamente quando esso si connette.

In risposta alla possibilità di ottenere facilmente informazioni dalle Probe requests, molti dei sistemi operativi per smartphone stanno via via implementando sistemi di randomizzazione dell’indirizzo MAC in modo da proteggere la privacy degli utenti e impedire il tracking dei loro spostamenti. In particolare, come constatato empiricamente in un precedente progetto del sottoscritto [33], i dispositivi iOS sono quelli che effettuano la randomizzazione in modo più ostico per quello che riguarda l’attribuzione di indirizzi randomici allo stesso dispositivo.

* 1. MAC Address

L’indirizzo MAC (Media Access Control) è un codice di 48 [bit](https://it.wikipedia.org/wiki/Bit_(informatica)) (6 [byte](https://it.wikipedia.org/wiki/Byte)) assegnato in modo univoco dal produttore ad ogni [scheda di rete](https://it.wikipedia.org/wiki/Scheda_di_rete) [ethernet](https://it.wikipedia.org/wiki/Ethernet) o [wireless](https://it.wikipedia.org/wiki/Wireless) prodotta al mondo, tuttavia modificabile a livello [software](https://it.wikipedia.org/wiki/Software). Al fine di garantire l’univocità dell’indirizzo MAC tra i dispositivi, l’IEEE assegna blocchi di indirizzi alle organizzazioni in cambio di una tassa. Questi blocchi, conosciuti più comunemente come OUI (Organizationally Unique Identifier), possono essere comprati e registrati tramite l’IEEE che da all’organizzazione il controllo e la responsabilità per tutti gli indirizzi con un dato prefisso a tre byte. I produttori a questo punto sono liberi di assegnare i rimanenti tre byte a qualsiasi valore essi vogliano con l’unica accortezza di non utilizzare lo stesso indirizzo due volte.

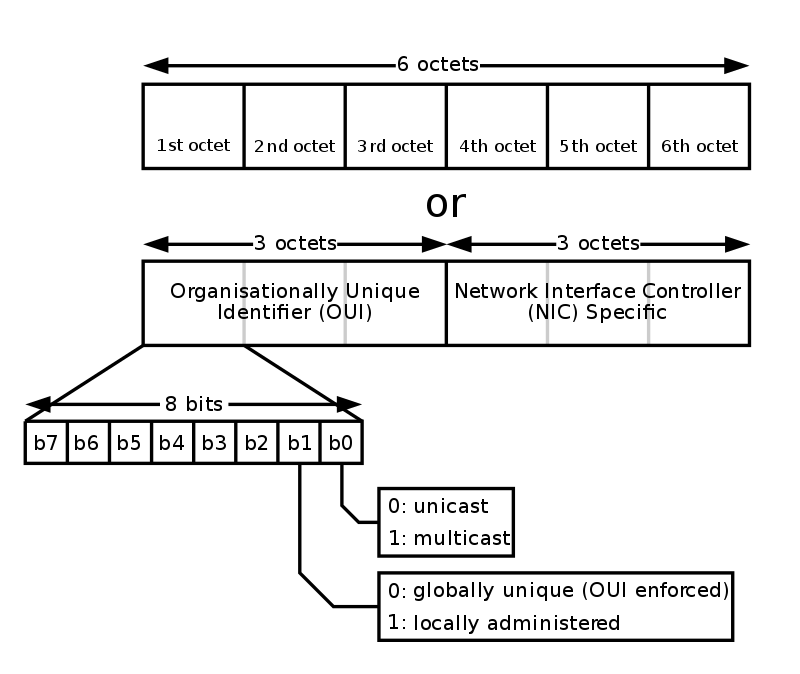


Figura 12 Diagramma che mostra la struttura di un indirizzo MAC-48, con indicate esplicitamente le posizioni del multicast/unicast bit e OUI/local bit

Oltre all’indirizzo MAC globale del produttore e di dominio pubblico, i dispositivi moderni utilizzano frequentemente un indirizzo localmente assegnato che è contraddistinto da un local bit nel byte più significativo dell’indirizzo. Gli indirizzi localmente assegnati non danno la garanzia di univocità e generalmente non sono utilizzati in una maniera persistente. Questi infatti, possono essere utilizzati per generare indirizzi MAC randomici come misura aggiuntiva per la privacy. Poiché in fase di active scanning i dispositivi comunicano la loro presenza agli AP nelle vicinanze e le Probe request richiedono l’indirizzo MAC della sorgente, se un device utilizza il suo indirizzo globale allora sta effettivamente facendo broadcast della sua identità. Analogamente agli OUI, i produttori possono acquistare da IEEE dei prefissi CID (Company Identifier) con la promessa di non utilizzarli in forma globale per i dispositivi. Di conseguenza, i CID hanno sempre il local bit asserito. Un esempio di questo tipo è dato dal prefisso DA:A1:19 posseduto da Google. Con l’impiego di MAC address randomizzati che cambiano nel corso del tempo, il tracking dei dispositivi risulta non più banale [34]. Nel momento in cui un device però si connette ad un AP smette di randomizzare ed utilizza il suo MAC reale. Per contro, come già accennato, l’evento che ci interessa sniffare, ovvero la fase di active scanning, si verifica con frequenza nettamente inferiore.

* 1. Sniffer Wi-Fi

Un primo prototipo di sniffer Wi-Fi è stato realizzato durante l'anno accademico 2017/2018 dal sottoscritto con la collaborazione dei due colleghi Chiara Leoni e Ulisse Quartucci. Il progetto prevedeva lo sviluppo di uno script Python che permettesse lo sniffing del traffico Wi-Fi. Con l'aiuto di [34] e [35] abbiamo stabilito un criterio che ci consentisse di attribuire ad un unico dispositivo i MAC address randomici che questo aveva generato, con il fine di ottenere in output ad intervalli regolari il numero di MAC address unici e quindi il numero di dispositivi con il modulo Wi-Fi acceso e tracciabili nel raggio d'azione dell'antenna wireless. Il software era pensato per girare su una stazione indipendente composta da un Raspberry Pi 3 B+ dotato di modulo Wi-Fi esterno che tramite ethernet rendesse disponibili i risultati su un database mySql.

Immagine che contiene elettronico

Descrizione generata con affidabilità elevata

Figura 13 Schema operativo dello sniffer Wi-Fi

Il sistema si metteva in ascolto dei pacchetti in transito e recuperava le informazioni in essi contenute al fine di costruire una signature che andava a delineare una prima distinzione tra marche e modelli di dispositivi. A questa veniva poi associato il MAC address contenuto nel pacchetto da cui era stata generata. La signature può essere considerata come una chiave derivata dalle caratteristiche fisiche di ciascun dispositivo [35], che vengono trasmesse come informazioni del pacchetto. Questo comporta che dispositivi appartenenti allo stesso modello abbiano signature uguali. All’interno delle Probe requests, ad accompagnare ogni MAC, vi sono informazioni utili alla derandomizzazione come timestamp, RSSI e sequence number della richiesta che venivano collezionate dallo script in un log da associare all’indirizzo MAC. L’esecuzione del processo portava ad avere una struttura dati in cui ad una signature potevano essere associati più indirizzi MAC e ad un indirizzo MAC uno storico di log. Se una signature conteneva molteplici MAC randomici, allora tramite uno studio sui log si cercava di capire se questi fossero stati generati dallo stesso dispositivo o meno.

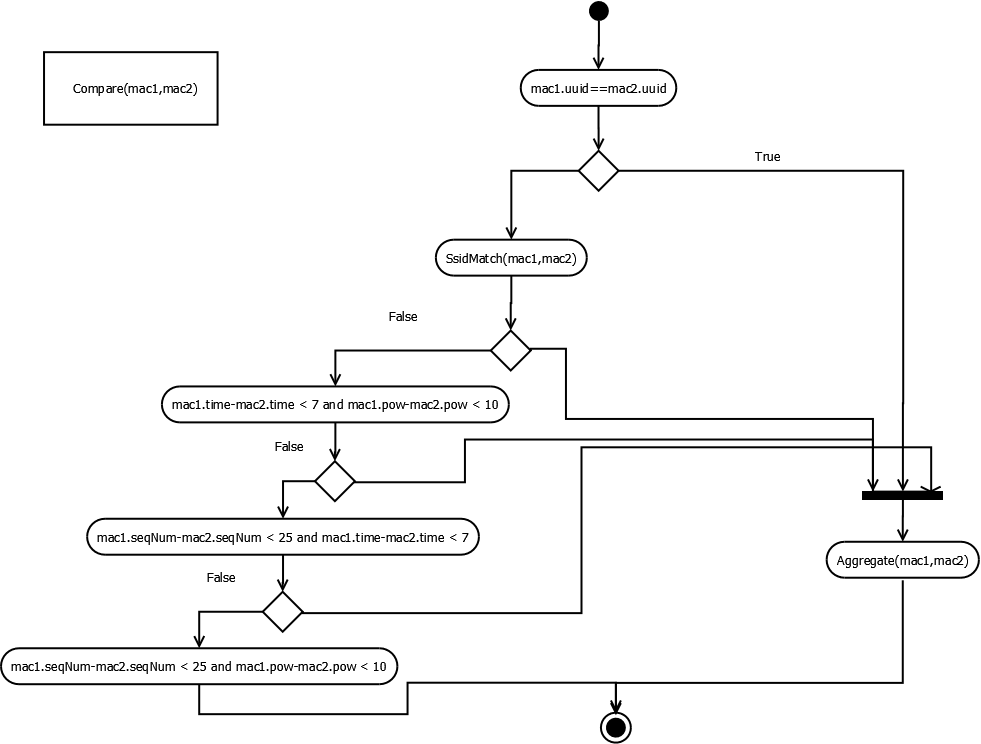


Figura 14 Activity diagram della funzione Compare(). Questa funzione veniva usata per stabilire se due indirizzi MAC randomici fossero stati generati dallo stesso dispositivo.

I criteri per l’aggregazione erano basati sulle differenze tra i log di due MAC differenti per i valori sopracitati, considerati tra loro a coppie:

1. piccole variazioni di timestamp e potenza;
2. piccole variazioni di sequence number e timestamp;
3. piccole variazioni di sequence number e potenza.

Seppur rari, vi sono casi in cui un dispositivo può trasmettere le informazioni WPS (Wi-Fi Protected Setup), protocollo supportato da alcuni dispositivi che permette una connessione sicura con un AP anche a dispositivi non autenticati, da cui si ricava l’UUID (Universally Unique Identifier) che, come scoperto in alcuni studi [36], viene generato direttamente dal MAC globale. In questi casi è sufficiente confrontare gli UUID per stabilire se i due MAC randomici provengano dallo stesso dispositivo. Un altro caso particolare si ha quando le richieste inviate dai dispositivi non sono di tipo broadcast ma indirizzate a specifici AP, quindi contenenti gli SSID degli hotspot con cui vorrebbero stabilire una connessione, conosciuti in precedenza. In una situazione del genere, liste di AP uguali portano all’aggregazione dei due MAC random. Una volta trovate le condizioni per cui era possibile l’aggregazione, al MAC con il log più recente venivano aggiunti i log dell’altro, che veniva etichettato come “da cancellare”.

1. Bibliografia

|  |  |
| --- | --- |
| [1] | Consorzio Turistico Cinque Terre, «Benvenuto su 5terre | 5terre,» [Online]. Available: https://www.cinqueterre.it/. |
| [2] | D. Helbing, «Models for Pedestrian Behavior,» 1998. |
| [3] | J. J. Fruin, «Designing for pedestrians: a level of service concept,» *Highway Research Board,* pp. 1-15, 1971. |
| [4] | A. Polus, J. L. Schofer e A. Ushpiz, «Pedestrian Flow and Level of Service,» *Journal of Transportation Engineering,* vol. 109, n. 1, pp. 46-56, 30 12 2008. |
| [5] | U. Weidmann, «Transporttechnik der Fussgänger Transporttechnische Eigenschaften des Fussgängerverkehrs, Literaturauswertung,» 1992. |
| [6] | G. Xiong, J. Cheng, X. Wu, Y. L. Chen, Y. Ou e Y. Xu, «An energy model approach to people counting for abnormal crowd behavior detection,» *Neurocomputing,* vol. 83, pp. 121-135, 15 4 2012. |
| [7] | P. Vera, S. Monjaraz e J. Salas, «Counting pedestrians with a zenithal arrangement of depth cameras,» *Machine Vision and Applications,* vol. 27, n. 2, pp. 303-315, 1 2 2016. |
| [8] | X. Zhang, J. Yan, S. Feng, Z. Lei, D. Yi e S. Z. Li, «Water filling: Unsupervised people counting via vertical kinect sensor,» in *Proceedings - 2012 IEEE 9th International Conference on Advanced Video and Signal-Based Surveillance, AVSS 2012*, 2012. |
| [9] | V. A. Sindagi e V. M. Patel, «A survey of recent advances in CNN-based single image crowd counting and density estimation,» *Pattern Recognition Letters,* vol. 107, pp. 3-16, 1 5 2018. |
| [10] | Q. Chang, Y. Qi, W. Zhou e J. Liu, «An Auto-adaptive CNN for Crowd Counting in Monitor Image,» in *Proceedings of 2018 6th IEEE International Conference on Network Infrastructure and Digital Content, IC-NIDC 2018*, 2018. |
| [11] | Y. Zhang, D. Zhou, S. Chen, S. Gao e Y. Ma, «Single-image crowd counting via multi-column convolutional neural network,» in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2016. |
| [12] | L. Del Pizzo, P. Foggia, A. Greco, G. Percannella e M. Vento, «Counting people by RGB or depth overhead cameras,» *Pattern Recognition Letters,* vol. 81, pp. 41-50, 1 10 2016. |
| [13] | Terabee, «Time-of-Flight principle: Technologies and advantages - Terabee,» [Online]. Available: https://www.terabee.com/time-of-flight-principle/. |
| [14] | L. Hikvision Digital Technology Co, «IP Camera | Network Camera - Hikvision,» [Online]. Available: https://www.hikvision.com/en/Products/Network-Camera. |
| [15] | VIVOTEK Inc., «People Counting :: VIVOTEK ::,» [Online]. Available: https://www.vivotek.com/solutions/people-counting. |
| [16] | DVSLTD, «Hikvision People Counting Camera Set Up - YouTube,» [Online]. Available: https://www.youtube.com/watch?v=zAK90GxVn5s. |
| [17] | H. Wu, C. Gao, Y. Cui e R. Wang, «Multipoint infrared laser-based detection and tracking for people counting,» *Neural Computing and Applications,* vol. 29, n. 5, pp. 1405-1416, 1 3 2018. |
| [18] | STMicroelectronics, «Time of Flight (ToF) Sensors - STMicroelectronics,» [Online]. Available: https://www.st.com/en/imaging-and-photonics-solutions/proximity-sensors.html?querycriteria=productId=SC1934#. |
| [19] | STMicroelectronics, «People Counting Using a Single ST Time-of-Flight Sensor - YouTube,» [Online]. Available: https://www.youtube.com/watch?v=c91Ve-g0J2U. |
| [20] | BEA, «LZR®-SIGMA | BEA Europe,» [Online]. Available: https://www.bea-sensors.com/it/prodotto/lzr-sigma/. |
| [21] | A. E. Redondi e M. Cesana, «Building up knowledge through passive WiFi probes,» *Computer Communications,* vol. 117, pp. 1-12, 1 2 2018. |
| [22] | X. Tang, B. Xiao e K. Li, «Indoor Crowd Density Estimation Through Mobile Smartphone Wi-Fi Probes,» *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* 25 4 2018. |
| [23] | Y. Fukuzaki, N. Nishio, M. Mochizuki e K. Murao, «A pedestrian flow analysis system using Wi-Fi packet sensors to a real environment,» 2014. |
| [24] | J. Weppner, B. Bischke e P. Lukowicz, «Monitoring crowd condition in public spaces by tracking mobile consumer devices with wifi interface,» 2016. |
| [25] | A. Kurkcu e K. Ozbay, «Estimating Pedestrian Densities, Wait Times, and Flows with Wi-Fi and Bluetooth Sensors,» *Transportation Research Record: Journal of the Transportation Research Board,* vol. 2644, n. 1, pp. 72-82, 7 7 2017. |
| [26] | A. Basalamah, «Crowd Mobility Analysis using WiFi Sniffers,» *International Journal of Advanced Computer Science and Applications,* vol. 7, n. 12, 4 1 2017. |
| [27] | Hak5, «WiFi Pineapple - Hak5,» [Online]. Available: https://shop.hak5.org/products/wifi-pineapple. |
| [28] | Raspberry Pi Foundation, «Buy a Pi – Raspberry Pi,» [Online]. Available: https://www.raspberrypi.org/products/. |
| [29] | «Home | Sail Amsterdam,» [Online]. Available: https://www.sail.nl/?lang=en. |
| [30] | W. Daamen, Y. Yuan, D. Duives e S. Hoogendoorn, «Comparing three types of real-time data collection techniques: Counting cameras, Wi-Fi sensors and GPS trackers,» *Proceedings of Pedestrian and Evacuation Dynamics ,* pp. 568-574, 2016. |
| [31] | Y. Yuan, W. Daamen, D. Duives e S. Hoogendoorn, «Comparison of three algorithms for real-Time pedestrian state estimation - Supporting a monitoring dashboard for large-scale events,» in *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC*, 2016. |
| [32] | E. Boni e E. Piccin, «Risultati della sperimentazione dei sistemi di monitoraggio dei flussi pedonali,» 14 Settembre 2018. [Online]. Available: https://www.venis.it/sites/www.venis.it/files/redazione/Trasparenza/762\_AT\_180925\_all1.pdf. |
| [33] | G. Ceccoli, C. Leoni e U. Quartucci, «Relazione progetto Wi-Fi sniffing Cinque Terre,» Luglio 2018. [Online]. Available: https://drive.google.com/file/d/1uJ-T7iVB9G1NUSr3NJQTa27\_o4kqaklH/view. |
| [34] | J. Martin, T. Mayberry, C. Donahue, L. Foppe, L. Brown, C. Riggins, E. C. Rye e D. Brown, «A Study of MAC Address Randomization in Mobile Devices and When it Fails,» 2017. |
| [35] | D. Gentry e A. Pennarun, «Passive Taxonomy of Wifi Clients using MLME Frame Contents». |
| [36] | M. Vanhoef, C. Matte, M. Cunche, L. Cardoso, F. Piessens, L. S. Cardoso, †. Iminds-Distrinet e K. U. Leuven, «Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms An Analysis of Wi-Fi Network Discovery Mechanisms,» 2016. |