Buongiorno a tutti, io sono Gianluca Ceccoli e questa è la mia tesi di laurea «Monitoraggio di flussi e densità pedonale presso aree congestionabili mediante sensori innovativi»

Durante la discussione toccherò i seguenti punti. Partendo da concetti generici arriverò a spiegare come funziona l’architettura proposta e come questa sia stata applicata al caso di studio

Tutto comincia dalla necessità di prevenire situazioni pericolose causate da sovraffollamenti pedonali in luoghi la cui capacità massima è spesso messa a dura prova.

Il grande sviluppo tecnologico che è in atto ogni giorno consente metodi di monitoraggio alternativi rispetto alla classica videosorveglianza. Per questi due motivi si è deciso di sviluppare un sistema di monitoraggio pedonale il cui obiettivo è quello di stimare la densità pedonale per classificare il traffico in tre livelli di viabilità, banalmente poco affollato, affollato e a rischio. Il sistema dovrebbe aiutare quindi la prevenzione e lo smaltimento di situazioni pericolose mediante sensori wifi

I più classici dispositivi impiegati nel monitoraggio sono le videocamere. Registrando immagini rgb o in scala di grigio si può estrarre il foreground con diversi algoritmi come frame differencing o background subtraction. All’interno della Crowd analysis vengono impiegate a livello macroscopico, in particolare per problemi di tipo ROI (Region of interest) ovvero la stima del numero di persone all’interno dell’area catturata da cui si può ricavare la densità.

I problemi principali dell’utilizzo delle telecamere riguardano la diminuzione di precisione con grandi masse e con meteo e condizioni di luce che variano durante la registrazione. Le occlusioni dovute al posizionamento, i vincoli sul posizionamento, l’impatto estetico che comportano e registrando i volti delle persone possono nascere controversie riguardo la privacy

I più classici dispositivi impiegati nel monitoraggio sono le videocamere. Registrando immagini rgb o in scala di grigio si può estrarre il foreground con diversi algoritmi come frame differencing o background subtraction. All’interno della Crowd analysis vengono impiegate a livello macroscopico, in particolare per problemi di tipo ROI (Region of interest) ovvero la stima del numero di persone all’interno dell’area catturata da cui si può ricavare la densità.

I problemi principali dell’utilizzo delle telecamere riguardano la diminuzione di precisione con grandi masse e con meteo e condizioni di luce che variano durante la registrazione. Le occlusioni dovute al posizionamento, i vincoli sul posizionamento, l’impatto estetico che comportano e registrando i volti delle persone possono nascere controversie riguardo la privacy

Le videocamere stereoscopiche sono videocamere che impiegano più di un punto di vista per avere informazioni sulla profondità. Come le videocamere normali registrano immagini e quindi hanno tutti gli svantaggi precedentemente menzionati.

Questi dispositivi però sono impiegati all’interno della Crowd Analysis per risolvere problemi a livello microscopico, cioè sul singolo individuo all’interno della folla. I problemi di tipo LOI (line of interest) hanno come obiettivo quello di ottenere la differenza di persone entranti o uscenti da un varco (che sarebbe appunto la linea di line of interest)

Quindi nasce un altro vincolo sul posizionamento che deve essere effettuato sulla verticale del varco. Inoltre sono poco applicabili all’esterno o in aree che hanno molteplici vie di fuga.

I laser e gli infrarossi sono una buona alternativa alle telecamere stereoscopiche in quanto non necessitando di registrare immagini ad alta risoluzione la complessità del conto è molto alleggerita. Ovviamente sempre per problemi di tipo LOI

Una tecnologia ancora poco affermata, protagonista solo di esperimenti è rappresentata dagli sniffer wifi. Uno sniffer in gergo è un sistema effettua un’intercettazione passiva del traffico sulla rete. Se supponiamo che in questo periodo digitalizzato ogni persona sia rappresentata dal suo smartphone, contando il numero di dispositivi potremmo essere in grado di stimare il numero di persone presenti nel raggio d’azione del sensore. Si ritorna quindi a problemi ROI senza però avere gli svantaggi dovuti al posizionamento di una telecamera. I sensori sono spesso homemade, a basso costo, discreti perché non hanno particolari vincoli di posizionamento e non sono influenzati dall’illuminazione.

La supposizione fatta precedentemente è alquanto forte, perché ogni persona potrebbe avere più cellulari come nessuno rilevabile. Andrebbe calcolato il tasso di rilevazione rispetto alla verità ma si pensa che per discriminare il traffico in tre livelli questo basti.

Lo standard IEEE 802.11 definisce 3 tipi di frame scambiati dai dispositivi wifi: magagement frame, control frame, data frame. Quello che ci interessa approfondire è il tipo management di cui fanno parte altri 5 sottoframe: association, authentication, beacon e probe request/response

Restringendo ancora il campo vediamo come un dispositivo ricerca le reti wireless. Innanzitutto i beacon sono messaggi che gli access point inviano per segnalare la propria presenza e il proprio ssid. Le probe request sono richieste che i dispositivi inviano ad AP specifici o in maniera broadcast allegando informazioni in chiaro su loro stessi. Quindi, tramite passive scanning i dispositivi ricevono i beacon, mentre durante l’active scanning mandano le probe request e aspettano le probe response. Il metodo con cui vengono inviati i frame si può schematizzare con l’immagine a destra. Vengono mandati burst di frame su uno o più canali a intervalli più o meno regolari.

Piccola anticipazione: eseguire lo sniffing delle probe request per contare i mac address contenuti in esse è quello che ci permette di contare i dispositivi

Cos’è il Mac address. È un codice di 6 byte assegnato in modo univoco ad ogni scheda di rete, tuttavia modificabile tramite sofware. IEEE assegna prefissi di 3 byte in cambio di una tassa che prendono il nome di OUI organiztionally unique identifier. I produttori sono poi liberi di assegnare i restanti 3 byte ai propri dispositivi con il vincolo di non usare mai lo stesso indirizzo due volte

C’è un però. Esiste una pratica chiamata randomizzazione dell’indirizzo MAC. È una misura per la protezione della privacy che alcuni sistemi operativi adottano per impedire il tracking dei dispositivi. Non esiste uno standard quindi ogni sistema operativo implementa la propria versione. E questo fa porre domande sulla loro efficacia. Si riconosce per il local bit che è il secondo bit meno significativo del primo ottetto settato a 1.

Analogamente agli OUI IEEE assegna prefissi di 3 byte chiamati CID company identifier. Un indirizzo randomizzato in gergo viene chiamato locally assigned. Un esempio è il CID di google.

La randomizzazione viene effettuata solo quando il dispositivo non è connesso a nessuna rete

L’architettura proposta è costituita da un raspberry pi 3 modello b+ con ambiente linux su cui gira uno script di sniffing in python, una scheda di rete usb impiegata in monitor mode per catturare il traffico wireless e un server sito qui all’università che ospita un database mysql e l’applicazione web per la visualizzazione dei dati

Lo script in python è costituito da due thread: uno per lo sniffing vero e proprio tramite la libreria scapy, l’altro per l’invio periodico dei dati al database. Il suo obiettivo è quello di fornire ad intervalli regolari il numero di dispositivi unici rilevati in quell’istante. Per i mac globali non ci sono problemi, quelli localmente assegnati hanno bisogno di essere aggregati sotto lo stesso dispositivo che li genera per evitare di contare copie multiple. Questo viene fatto mediante una fase di fingerprinting dell’indirizzo e un controllo di aggregazione su indirizzi con la stessa firma. Poi ad ogni indirizzo è assegnato un tempo di decadimento dopo l’ultima rilevazione, trascorso il quale viene rimosso dalla lista di quelli presenti.

Una delle altre informazioni contenute nelle probe request sono gli Information Elements o parametri taggati o tags. Servono per segnalare agli ap le caratteristiche fisiche del dispositivo mittente. Ognuno possiede un id e il relativo valore

Non sono obbligatori ma lo standard definisce che siano inclusi in ordine crescente di id. Questa pratica però non è sempre seguita quindi oltre al valore che i tag hanno, anche l’ordine di comparizione può essere utilizzata come fonte di discriminazione tra i vari modelli dei dispositivi

Dopo aver diviso le richieste in bucket per ogni bucket si controlla se vi siano indirizzi localmente assegnati da dover aggregare. Un’altra informazione contenuta nelle probe request è il sequence number, un contatore intero che si incrementa ad ogni invio di frame durante l’active scanning. Se due indirizzi mac ricadono nello stesso bucket e i loro sequence number sono vicini, allora questi vengono aggregati. In realtà alcuni dispositivi anche le informazioni WPS di cui si può sfruttare l’UUID che è stato dimostrato essere generato direttamente dal mac globale, quindi uuid uguali portano all’aggregazione. Lo stesso discorso vale per gli ssid. Le probe request possono contenere gli ssid delle reti conosciute e liste di ssid uguali portano all’aggregazione

L’output dello sniffer può essere descritto mediante una somma di due numeri, x1 mac globali e x2 mac localmente assegnati già aggregati. L’output è una misura rumorosa in quanto dipende dall’accuratezza di x2, cioè da quanto sia preciso il metodo di aggregazione, dal fatto che non tutti abbiano il wifi acceso, dal fatto che alcuni dispositivi con wifi acceso non siano rilevabili perché «dormienti», dalla portata massima dello strumento, limiti dell’architettura, insomma ci sono parecchie variabili in gioco.

Per stimare quindi il numero di persone si è optato per un modello proporzionale piuttosto che cercare un modello troppo complesso anche perché alla fine il risultato che si vuole raggiungere è la distinzione in tre classi di viabilità.

Prima di passare al caso di studio ancora due parole sullo strumento. È stato eseguito un test per avere un’idea dell’accuratezza sull’aggregazione con 5 laptop che sono stati messi a randomizzare forzatamente emulando quanto più possibile la randomizzazione dei cellulari. Ognuno salvava la sequenza di mac utilizzati e lo script riportava le aggregazioni fatte. Ne è risultata un’accuratezza di quasi l’80% su un migliaio di cambi di mac eseguiti.

Per quanto riguarda la portata massima invece siccome non è ancora stato possibile immergere il dispositivo in una folla di migliaia di persone, è stata fatta una stima teorica. Dato un tempo medio di esecuzione per ciclo di 15.8ms e un tempo di decadimento di 70s, a patto di trovare dispositivi sempre diversi se ne possono raggiungere circa 4400.

Le Cinque Terre sono cinque antichi borghi situati tra levanto e la spezia. Data la situazione geografica impervia, la discesa ai paesi è consentita solo a piedi per cui il mezzo di gran lunga più utilizzato è la ferrovia. Non sono aree adatte al turismo di massa che vedono durante i periodi di alta stagione a causa della mancanza di spazi adeguati, specialmente nelle stazioni ferroviarie. È proprio presso le cinque stazioni, o meglio presso i 5 terre point presso le stazioni che sono stati piazzati i sensori.

Monterosso è il primo paese viaggiando da nord a sud. Questo insieme a Riomaggiore, che è l’ultimo, costituiscono i maggiori punti di scambio dei treni per coloro che vogliono visitare il parco. Come si può vedere il sensore capta sia le persone sui binari, sia sulla passeggiata lungomare sottostante la stazione.

Vernazza è il secondo paese che si incontra. L’ufficio del 5 terre point è proprio in mezzo ai binari e consente il monitoraggio completo della stazione. L’accesso è possibile solo tramite una scala dalla via sottostante ed essendo questa appunto sotto la stazione è monitorata anch’essa.

Il terzo paese è corniglia. Anche in questo caso la stazione ha un’unica via di fuga dove i turisti si incamminano verso i sentieri. La massa è costretta a seguire un vicolo di cui il 5 terre point fa angolo per cui tutto il traffico riesce ad essere monitorato

La penultima stazione è quella di manarola e come per le altre i turisti sono obbligati a seguire un sottopassaggio e transitare presso una piazzetta antistante il 5 terre point, per poi proseguire lungo un tunnel che collega la stazione al paese. Motivo in più per monitorare quest’area

Riomaggiore è l’ultimo borgo che come già detto, assieme a monterosso delimita le cinque terre. Qui l’area è un po’ più grande rispetto alle precedenti, ci sono più vie di fuga e la piazza è decisamente più capiente rispetto a quella di manarola. Il 5 terre point si trova proprio nella piazza, tra la stazione e il tunnel che la collega al paese

L’applicazione web per la visualizzazione dei dati è composta da una mappa con i pulsanti per spostarsi rapidamente da un paese all’altro. Sono presenti i marker in corrispondenza di dove sono piazzati i sensori e cliccandoci sopra viene mostrato all’utente uno storico dell’ultima ora.

L’area coperta da ogni sensore prende il colore a seconda della classificazione di cui abbiamo parlato all’inizio. Verde, giallo, rosso e cambia automaticamente davanti all’utente quando si verifica un passaggio di stato

Una sezione sottostante la mappa consente di visualizzare un intervallo personalizzato di uno tra i sensori disponibili. Su questo grafico si può zoomare, rimpicciolire le parti interessate

I sensori ora come ora sono attivi 24h su 24 e siccome il sistema è online da relativamente poco tempo è stato stimato un parametro proporzionale di 1,35 che permette una stima piuttosto veritiera del livello di traffico. Per quanto riguarda la randomizzazione è vero, è un meccanismo che impedisce il tracking ma ha comunque delle falle. Sarebbe opportuno che il contenuto delle probe request fosse ridotto all’essenziale per impedire il fingerprinting. Sarebbe opportuno anche resettare il sequence number ad ogni cambio indirizzo. La randomizzazione dovrebbe essere adottata da tutti i sistemi operativi perché per esempio nonostante sui samsung giri android, questi non randomizzano.

Le rilevazioni attualmente in corso, assieme a meteo, giorno della settimana, festività e stagione potrebbero essere una base per un dataset su cui sviluppare un modulo previsionale. Le previsioni trasformerebbero così l’applicaizone web in uno strumento per i turisti oltre che per i gestori del parco. Volendo si potrebbe utilizzare l’informazione dei mac globali per vedere quali siano i percorsi più battuti e con quali tempistiche o per fare calcoli all’interno di uno stesso paese avendo a disposizione più sensori per ogni borgo.