

Estudi de la privacitat de dades

David Matos Xancó

1 INTRODUCCIÓ

EN l'actualitat, per a poder fer ús de les tecnologies actuals ja sigui en estudis mèdics, en investigacions demogràfiques, etc., necessitem acceptar obligatòriament l'entrega de les nostres dades personals a diferents empreses o organitzacions. Aquestes, ja sigui per interès mutu o per regulacions que ho exigeixen, es veuen en la obligació de publicar i compartir les dades que recullen. Això pot tenir efectes positius sobre els mateixos usuaris que ofereixen les dades personals ja que molts cops se'n treu profit, però en ocasions pot arribar a posar en risc la privacitat dels mateixos. Recentment s'han vist casos relacionats amb el tractament incorrecte d'aquestes bases de dades, en els quals degut a la seva publicació ha estat possible el reconeixement directe de diferents usuaris, i per tant, s'ha trencat la privacitat d'aquestes persones. Arran d'aquest problema i possibles atacs a la intimitat dels usuaris, sorgeix la necessitat de trobar un mètode d'anonimitzar aquestes dades sensibles per tal que aquests no puguin ser reconeguts. Així doncs, les empreses que tracten aquest tipus de dades es veuen en la obligació de protegir els usuaris davant possibles atacs dirigits a l'extracció d'informació útil a partir de les dades personals, fent ús de diferents tècniques i mètodes.

2 OBJECTIUS

Tenint en compte la importància de l'anonimització d'aquestes dades de cara a la preservació de la privacitat dels usuaris, es plantegen els següents objectius.

- En primer lloc, serà necessari estudiar a quins àmbits aplica, això és molt important ja que l'ús de les nostres dades està present en moltes situacions i per tant primer cal comprendre el problema que hi ha. Un cop realitzat un primer estudi s'aprofundirà en dos dels casos, dels quals es definirà el risc existent i quins són els models que s'apliquen per tal de cobrir aquest perill.
- Així doncs, un cop estudiat l'estat de l'art coneixent les tècniques i models d'atacs més populars, s'escullirà un per a implementar-lo.
- S'implementa el mètode escollit a petita escala i s'observen els resultats. S'extrapola a un servidor amb capacitat per a processar un volum major de dades i

es fa un anàlisi comparatiu entre les dades abans de anonimitzar i després, per tal de poder treure conclusions sobre la utilitat del mètode de cara a posteriors tractaments de les dades.

3 METODOLOGIA

Aquest projecte és un projecte d'enfoc teòric, però aquesta es basa en la generació de uns resultats a partir de un model ja existent. És per això que la metodologia emprada en aquest treball ha de ser una metodologia en la que els passos del projecte estiguin prou definits, una metodologia basada sobretot en l'estudi de l'estat actual del tema, és per això que s'ha decidit basar el projecte en la metodologia en cascada. Aquesta metodologia permetrà en primer lloc realitzar l'estat de l'art, entenent de forma complerta la necessitat i tots els camps als que aplica aquest projecte. La següent serà una fase de recopilació i enteniment de dades preses com a exemple, de forma que es podrà veure quins són els individus més afectats i s'aplicarà la tècnica estudiada a aquestes. Com s'ha dit, aquesta metodologia es basa en la definició de un cicle a complir, en el qual no es podrà passar a la següent tasca fins que no s'hagi finalitzat per complet la actual en la que s'estigui treballant. Això facilitarà el fet de recopilar tota la informació necessària en un primer moment per tal de poder desarrelar la resta del projecte que depèn d'aquesta.

4 PLANIFICACIÓ

Per tal de poder dur a terme el projecte dins els terminis que s'estableixen, s'haurà de fer una prèvia planificació que es seguirà exhaustivament.

- Primera fase - Inici: En la primera fase es farà una planificació del desenvolupament del treball i una descripció del problema juntament amb la descripció dels objectiu i metodologia.
- Segona fase - Documentació: Es fa un estudi de l'estat de l'art per a conèixer els diferents mètodes existents que posen a en dubte la privacitat de les dades de trajectòria així com les tècniques per a protegir els usuaris d'aquests mateixos.
- Tercera fase - Implementació del model: S'escull un model dels anteriors i s'implementa per tal de veure el seu funcionament amb un conjunt de dades simulades.
- Última fase - Tancament: Realització de la memòria escrita i de la presentació final.

• E-mail de contacte: davidignacio.matos@e-campus.uab.cat
 • Menció realitzada: Tecnologies de la Informació
 • Treball tutoritzat per: Jordi Casas Roma
 • Curs 2019/20

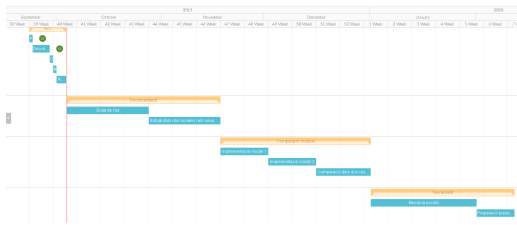


Fig. 1: Diagrama de Gantt

5 DEFINICIÓ DEL PROBLEMA

Les nostres vides cada cop es veuen més envoltades amb components on la tecnologia de la comunicació és omnipresent. Desde trucar algú per telèfon, anunciar qualsevol event o navegar per la xarxa fins a fer servir un sistema de navegació per a automòbils o pagar amb una tarjeta de crèdit són exemples de situacions en les que sense ser conscients, els usuaris deixen enregistrades a una base de dades tot un conjunt d'activitats del seu dia a dia. Aquestes dades podran ser extretes més endavant per a diferents propòsits, ja sigui per a la publicitat dirigida basada en l'ubicació, l'anàlisi dels transports que els usuaris fan servir o un perfil de la conducta. Una de les característiques que es destaca de les noves tecnologies, i que s'estudiarà en profunditat, és que sovint depenen d'una base de dades que es compona, i inclou microdades sobre trajectories. Aquestes microdades contenen informació personal sobre els individus i els seus moviments, les quals descriuen trajectories en un espai i temps, és a dir, posicions geogràfiques dels usuaris. A continuació s'exposen 5 exemples de microdades basades de trajectories per tal d'explicar una mica més la situació:

- **Serveis basats en ubicació:** Són aplicacions executades en dispositius mòbils que carreguen les dades sobre la posició d'un usuari segons sigui necessari per a complir amb el servei. Exemples d'aplicacions serien Google Maps o Instagram.
- **Operadors de xarxes de telèfon:** Fan un monitoreig passiu a les seves xarxes per a recopilar dades sobre l'activitat dels seus usuaris amb fins que inclouen facturació, trànsit de dades o desenvolupament de serveis en els que s'hagi d'afegir valor. Podem trobar rastres de la ubicació en l'antena del telèfon, el registre de trucades o el registre del servei a la xarxa del propi usuari.
- **Dispositius mòbils equipats amb interfícies Wi-Fi:** Aquests estan constantment enviant missatges mitjançant ones per tal de descobrir punts d'accés propers. Aquests punts coneguts com AC, registren l'adreça MAC dels dispositius que emeten aquestes ones. L'accés Wi-Fi pot rastrejar els usuaris dins la cobertura de la seva xarxa. Alguns exemples els trobem als nostres dispositius mòbils els quals poden seguir en gran mesura els moviments dels usuaris.
- **Sistemes moderns de navegació:** Aquest servei de navegació proveeix als usuaris d'informació en temps reals sobre l'estat de les carreteres i les seves condicions, però també permet recopilar dades sobre el posicionament del vehicle. Aquestes dades són usades pels proveïdors de sistemes de navegació i per compa-

nyies de assegurances per tal de poder perfilar perfils de conducció i nivells de riscos associats.

- **Pagaments electrònics:** Aquest tipus de pagament està prenent més importància que el pagament en efectiu. Aquesta transacció queda enregistrada a la direcció de la persona que accepta el pagament. Que permet a les empreses del sector bancari monitoritzar els moviments dels clients a mesura que usen les tarjetes de crèdit.

Aquests són exemples on es pot veure com les tecnologies permeten la recopilació de microdades de trajectòries a gran escala. Aquesta informació porta a la construcció de grans bases de dades que emmagatzemaran aquestes trajectòries. És per això que s'obté un gran interès en explotar aquestes microdades de totes les formes possibles, i poder així créixer en un mercat multimilionari emergent. Es crea així, una necessitat totalment nova de recopilar, emmagatzemar, fer circular i comercialitzar microdades de trajectòria. Aquest tràfic de dades, si no es fa amb les dades totalment protegides crea paral·lelament interès per part de terceres persones en atacar aquestes dades posant en risc la privacitat dels usuaris existents en la base de dades. Aquest concepte és conegut com mineria de dades i tracta d'extreure informació útil i desconeguda fins el moment d'un conjunt de dades emmagatzemades, i pel qual surgeixen una sèrie de mètodes i eines que es responsabilitzen de la seguretat de les dades. Aquests mètodes modificaran el contingut de les dades inicials per tal que els atacants no puguin reidentificar els usuaris en un futur, no obstant aquestes modificacions fan que la utilitat d'aquestes dades en processos o estudis posteriors sigui menor, pel que s'ha de trobar un equilibri entre l'anonimització i usabilitat de les dades. És per aquest motiu que aquests mètodes s'encarregaran de la manipulació, tramitació i publicació de les dades de forma que aquestes mantinguin la seva utilitat al mateix temps que preserven la privacitat dels usuaris que apareixen en elles.

S'ha d'entendre el risc que es presenta, ja que un atacant podria recopilar informació suficient per a reidentificar un usuari dins una base de dades que conté atributs sensibles com la ubicació del lloc de treball, habitatge, o llocs freqüentats durant rangs determinats d'horaris, entre altres. Per tant, si l'atacant tingués èxit podria saber informació privada sobre els llocs que els usuaris freqüenten com llocs de culta que revelin les preferències religioses, locals de caràcter eròtic o sexual, etc.

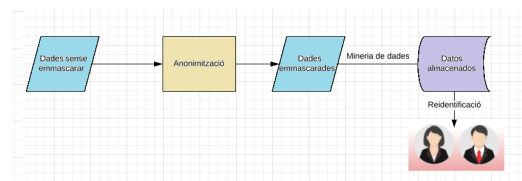


Fig. 2: Minería de datos

6 MODELS TEÒRICS DE PRIVACITAT

Existeixen dos grans models per a limitar el risc de divulgació en els processos de publicació de les dades. Els podem classificar de la següent manera:

- **Protecció no interactiva:** Es genera i publica una versió protegida d'un conjunt de dades original. Es fa servir majoritàriament quan es vol fer un anàlisi de dades que són desconegudes en el moment de la publicació.
- **Protecció interactiva:** Genera una versió protegida que es retorna en el moment que un usuari faci una consulta de dades definides a una base de dades amb una finalitat analítica. Normalment es fa servir en els anàlisis en les que les dades són prèviament conegudes.

Dins aquests grans blocs, trobem els següents mètodes destacables.

1. **Pseudonimització:** aquest model de protecció no interactiu va ser el primer model pensat per tal de protegir d'alguna manera les dades dels usuaris, consisteix principalment en eliminar els identificadors personals de la base de dades i substituir-los per algun identificador pseudoaleatori. Modificant aquests identificadors i no cap altre atribut com els quasi-identificadors fa que per a un atacant sigui probable, o poc difícil la reidentificació d'usuaris dins la base de dades. Un atacant no podrà saber de forma exacta si l'informació que obté al entrar a la base de dades és l'original o ha estat alterada. Es troba alguna dificultat seguint aquest mètode, i és que el fet d'afegir massa soroll a les dades originals podria anular la seva pròpia utilitat, i per tant s'estableixen dos principis que el soroll ha de complir:

- Que sigui suficient per a que un atacant no pugui saber si les dades han estat modificades o no.
- L'informació general del conjunt s'ha de preservar per a que possibles anàlisis futurs s'aproximin el màxim possible als fets amb dades originals.

2. **k-anonimitat:** aquest és un altre model teòric de protecció no interactiu. És una propietat de les dades que ens assegura que un individu no podrà ser identificat de la resta de $k-1$ individus existents a la base de dades. La principal avantatge que experimenta aquest model és que un atacant no podrà identificar la seva víctima amb una probabilitat superior a $\frac{1}{k}$. És per això que s'ha de tindre en compte que com més alt sigui el valor de k més augmentarem la privacitat, i per contrapartida més reduïrem la utilitat de les dades.

3. **Privacitat diferencial:** el model de privacitat diferencial està fet per a la protecció interactiva enfocada a bases de dades estadístiques, és a dir, consultes a bases de dades. En aquest context el mecanisme d'anonimització es troba entre l'usuari i la base de dades. Per tal d'assegurar que els usuaris estaran totalment protegits, aquest model defensa que el fet d'afegir o eliminar un individu d'un cert conjunt de dades no ha de suposar una alteració en els resultats d'un anàlisi a la base de dades. Aquesta afirmació és recolzada pel fet que si al afegir un conjunt de dades d'un usuari en concret a una base de dades aquesta pateix una alteració suficients com per ser apreciada per un atacant, aquest usuari seria fàcilment identificable i per tant estaria en risc la seva privacitat. Per exemple, suposem que es

té un conjunt de dades que es diferencia en només un element d'un altre conjunt de dades, i que per un altre banda, tenim un algoritme randomitzat del tipus ϵ -diferencial. Aquest element és el que regula directament la quantitat de diversitat que es pot trobar en el resultat d'una consulta a la base de dades quan s'elimina o afegeix un individu. Per tant, la privacitat diferencial assegura que el coneixement que un atacant pot adquirir addicionalment estarà limitat segons aquest paràmetre. És per això que la privacitat diferencial és una condició que es troba en el mecanisme de publicació i no en el conjunt de dades en sí.

7 ANONIMITZACIÓ DE LOCALITZACIONS I DADES TEMPORALS

Per a preservar la privacitat dels usuaris es recullen diferents tècniques en dos grans grups:

- **Tècniques d'anonimització de punts espai-temporals,** que tenen en compte únicament la localització del moment actual.
- **Tècniques d'anonimització de trajectòries:** Que tenen en compte una successió de punts al llarg del temps

En el cas de les tècniques d'anonimització de punts espai-temporals, cal destacar que redueixen la precisió amb la que s'envia la localització exacta d'un usuari en un moment determinat. Hi ha tres participants:

- Servidor LBS: ofereix un servei als usuaris basant-se en la seva ubicació actual
- Usuari: Persona que busca un servei que es basa en la seva localització.
- Anonimitzador: Aplica alguna de les tècniques explicades a continuació per a ocultar dades de l'usuari al servidor LBS

Les tècniques d'anonimització que s'han estudiat són proposades per tal de minimitzar l'impacte o reduir en cert nombre els atacs que es poden donar que posin en risc la privacitat en relació a la localització d'un usuari. Es diferencien dos grans principis dins l'estudi:

- Indistinguibilitat
- Desinformació

A més d'aquests dos principis es troben diferents treballs que adopten nocions menys rigoroses de la privacitat, els quals fan una menció més general d'aquest terme i que s'agrupen en un tercer:

- Mitigació

Cal destacar que els principis de privacitat per a ser aplicats a casos reals han d'estar especialitzats en criteris de privacitat. Aquests són els que defineixen els requeriments que la base de dades necessita per a poder complir amb el principi pertinent. En les següents seccions es fa una descripció dels principis i es destaquen les tècniques emprades més important per a complir amb aquests principis.

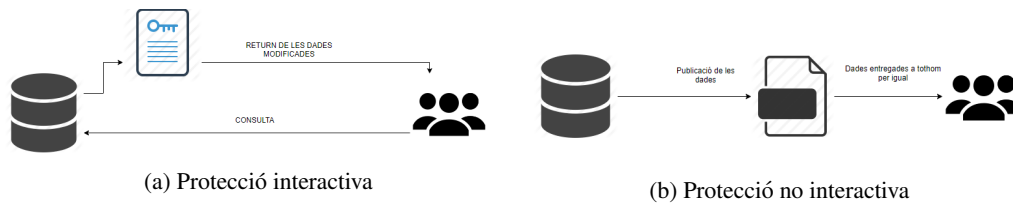


Fig. 3: Protecció interactiva vs protecció no interactiva

7.1 INDISTINGUIBILITAT

Recomana que cada registre d'una base de dades sigui indistingible de la resta de registres existents a la mateixa base de dades, eliminant així la unicitat¹. Aquest objectiu s'aconsegueix implementant k -anonimitat o alguns dels seus mètodes derivats com ℓ -diversity o t -closeness. La idea és que un grup de punts espai-temporals de cada usuari en les microdades de trajectòria de una base de dades no sigui distingible per almenys $k-1$ altres usuaris en la mateixa base de dades.

Les solucions proposades es basen en les diferents variacions del model de k -anonimitat i per tant s'ha de tindre en compte que encara no s'ha determinat quin és el millor valor de k per a reduir la usabilitat de les microdades de trajectòria. En segon lloc, s'ha de tindre en compte que aquest model ofereix solucions únicament pels atacs del tipus enllaç de registres.

7.1.1 K -ANONIMITAT VIA GENERALITZACIONS ESPAI-TEMPORALS

És la tècnica base usada per aconseguir la k -anonimitat en les microdades de trajectòria. Tracta de reduir l'exactitud espacial així com la granularitat temporal dels punts de les trajectòries que es troben a la base de dades, ocultant els punts d'una trajectòria determinada amb altres punts d'altres trajectòries. Seguint aquesta filosofia, com s'ha explicat anteriorment, es pot arribar al punt de perdre suficient exactitud en els registres de les dades que aquestes quedin inservibles. Podem veure un exemple d'actuació a la **Figura 4**.

Els investigadors Zang i Bolot proposen una primera opció en decrementar la unicitat mentre que la granularitat espacial de la trajectòria també ho fa, però apel·la a la dificultat de fer-ho donat que si un atacant sapigués les 3 localitzacions més visitades per part d'un usuari seria inútil intentar trobar la 2-anonimitat ja que s'hauria de publicat una quantitat de dades realment petita. En un posterior estudi [11], s'investiga el per què de la dificultat tant elevada d'aplicar la k -anonimitat, explicant que en una base de dades prou gran es té moltes localitzacions comunes entre tots els usuaris però que sempre hi haurà localitzacions úniques que serà molt difícil d'ocultar. A més, demostra en el mateix estudi com introduint una $k > 2$ es perdria utilitat de les dades. A partir d'aquestes observacions, els autors proposen una tècnica anomenada GLOVE un algoritme que aconsegueix finalment la k -anonimitat de les microdades de les trajectòries via generalitzacions d'espai-temporals. Explica com en el seu mètode s'aplica la reducció de la granularitat a cada

punt de forma individual, a diferència de com s'havia estat fent fins el moment, on s'aplicava al conjunt de punts de la trajectòria. Basant-se en aquests fets, els mateixos autors defineixen una mètrica creada per ells mateixos, "fingerprint stretch effort" que quantifica la pèrdua necessària de granularitat per tal d'ocultar cada mostra d'una trajectòria amb la mostra més propera d'una altra trajectòria. La millora d'aquesta tècnica GLOVE, permet anonimitzar una base de dades de desenes de milers de registres conservant registres fins a 1 kilòmetre de la trajectòria inicial en la dimensió espacial i 1 hora en la temporal, demostrant que es perden menys dades a mesura que s'incrementa la mida de la base de dades.

7.1.2 K -ANONIMITAT VIA SUPRESSIÓ

Aquesta altre tècnica, tracta d'esborrar els punts espai-temporals de la trajectòria original. Diferents tècniques han estat presentades, les més destacables com la proposta un algoritme que elimina iterativament alguns punts de les trajectòries fins a satisfer la k -anonimitat. El funcionament és el següent: per cada iteració, els punts que trenquen la k -anonimitat són detectats, i el que comporta una distorsió Euclidian mínima és seleccionat per a ser esborrat. Aquest fet comporta diverses hipòtesis sobre atacs i format de dades:

- Les trajectòries són purament espacials, no tenen la dimensió del temps.
- La dimensió de l'espai es dividirà en un número definit de localitzacions.
- Els possibles atacants seran menys, i tota la possible informació que poden tindre és anonimitzable.

7.1.3 K -ANONIMITAT VIA GENERALITZACIÓ I SUPRESSIÓ

Els investigadors Gramaglia i Fiore [9] destaquen que la supressió serà beneficiosa per a la k -anonimització donat que descartant alguna petita fracció de punts únics determinats, s'eliminarà un conjunt de trajectòries que el nivell de precisió de les quals era prou alt. Posteriorment, es realitzen diferents estudis que continuen en la mateixa línia en el que fa referència a la impossibilitat de generalitzar punts de trajectòries que tenen un nombre diferent de punts. És a dir, no es pot realitzar aquest mètode ja que comportaria generalitzar dos o més punts d'una trajectòria amb tant sols un punt d'una altra. Per altre banda es basen en una mètrica de similitud de parelles de trajectòries diferent², aquesta

¹ Mesura que caracteritza la diversitat de moviments de un mateix individu. A major unicitat de les micro-dades de trajectòria major probabilitat que un atacant pugui relacionar informació de una víctima

² Fingerprint Stretch Efoort



Fig. 4: k -anonimitat via generalització espaietemporal. Imatge extreta de [1]

es diu mètrica de cost de registre i mostra com pot aconseguir 2-anonimització eliminant tant sols el 2 o 3% de les dades, mentre que anteriorment hauria comportat una eliminació d'un 25% com a mínim. No ofereixen resultats exactes, però mostren com els resultats en clustering conserven una precisió del 50-90%. Dues tècniques són proposades a posteriori, conegudes com *kam_cut* i *kam_rec*. La primera és usada per a grans conjunts de dades i explica bàsicament com crea una estructura d'arbres de trajectòries on els nodes pare representen les més comunes i els fill les menys comunes però més completes dels mateixos usuaris. A partir d'aquest arbre, i triant una determinada k , s'eliminen les branques amb menys de k trajectòries compartides. *Kam_rec* és una extensió de la primera per a conjunts de dades més petits, i intenta reinserir punts de les subtrajectòries que s'han eliminat buscant la seva subseqüència de punts més llarga amb la condició que apunti a alguna trajectòria que es trobi encara en l'arbre, o que sigui compartida per almenys una altra subtrajectòria que ha estat eliminada.

7.1.4 K-ANONIMITAT VIA AGREGACIÓ I SUPRESSIÓ

Per explicar la microagregació cal mencionar que consta de dos passos principals:

- **Partició:** En aquest primer pas s'agrupen les trajectòries inicials que són més semblants, de forma que els clusters que es generen al final tindran una cardinalitat igual a K .
- **Aggregació:** Les trajectòries d'un cluster seran substituïdes per un prototip de cluster, obtingut a través de computar els mateixos punts del cluster. Fent això s'aconsegueix k -anonimitzar el conjunt de dades fent que les trajectòries en el cluster siguin en conclusió igual al del prototip.

La introducció de noves mètriques de similitud entre parelles com per exemple la mètrica de distància sincronitzada[7] entre trajectòries són introduïdes com a millores de l'anterior. El procés per trobar aquesta distància segueix les següents passes:

- En primer lloc sincronitzant totes les trajectòries segons un mateix criteri.

- Es computa la distància Euclidian entre els diferents punts contemporanis, si es dona el cas que existeixen dues trajectòries en un rang de temps diferent, es suprimeixen tots els punts no coincidents i la mètrica que era usada per a calcular la distància es divideix pel percentatge total de punts que s'han suprimit. D'aquesta manera el càlcul entre parells serà més ràpid

“SwapLocation” és una tècnica coneguda per l'ús d'aquesta similitud entre parelles. Per a cada trajectòria en un clúster canvia tots els punts espaietemporals per punts de altres trajectòries en el mateix clúster. Aquest canvi ha de respectar els l·lindars de temps i espai definits en un principi. A més, si un punt no té possibilitat de realitzar cap canvi amb un altre degut als l·lindars es suprimeix. En els resultats que mostren els autors, es fan servir dades reals i sintètiques i aquests obtenen que a les dades sintètiques per una $k=10$ hi ha una important supressió: amb un l·lindar espacial de 1 km s'obté una eliminació = 50% de les trajectòries i el 80% dels punts. Si s'augmenta el l·lindar a 3km es redueix la supressió a un 5% i els punts es mantenen. En el cas de dades reals i una $K=2$. El 29% dels punts són eliminats i la distorsió espacial se situa en 2.4 km.

7.2 DESINFORMACIÓ

Menciona que el guany en termes de quantitat que un atacant obtindrà després de realitzar un atac ha de ser molt petit. Aquest principi té com a objectiu la protecció contra atacs probabilístics, i usa la privacitat diferencial com a criteri estàndard per tal de poder complir-lo. El primer cas proposat fa referència a l'ús d'un model Laplacà per a afegir soroll a una sortida en forma de vector escalar. Aquest model és modificat més endavant on es proposa una sortida en forma de distribució de probabilitats a través d'un conjunt de resultats, aconseguint privacitat diferencial a través de randomitzar les probabilitats fent ús d'un mecanisme exponencial. En les dues situacions exposades s'obindrà com a resultat un vector amb soroll, el qual vindrà donat per un element ϵ així com la diferència màxima entre totes les sortides possibles quan es suprimeix un registre únic.

7.2.1 PRIVACITAT DIFERENCIAL SINTÈTICA

A partir d'aquesta tècnica es pot aconseguir l'objectiu principal fent ús de diferents:

- Complint els principis de privacitat diferencial, és a dir, que alguna representació de les microdades de trajectòria original sigui randomitzada.
- Com les trajectòries randomitzades són derivades de les originals, es pot dir que aquestes compleixen amb el principi de privacitat diferencial.

El primer treball que representa aquesta idea, és presentat per l'investigador Chen [6], explicant que el seu treball es basa en la construcció d'un arbre jeràrquic en el que les trajectòries s'agruparan en base a subseqüències d'localitzacions coincidents. En primer lloc, es creen els nodes fills de la iteració base (root) i es fa el mateix per totes les iteracions. En segon lloc, un cop es té un primer arbre, s'afegeix soroll a cada node generalitzat fent ús del model Laplaciana. A continuació, els nodes que tinguin un soroll per sota d'un llindar establert en un principi no s'expandiran més, i només ho faran els que superin el llindar i fins a un nivell d'expansió establert per l'usuari en un principi. Per acabar, es conclou l'arbre amb els sorolls de Laplace dividits de forma que la suma dels valors dels nodes fills no puguin tindre un valor més alt que els nodes pares. Realitzant una taula final de trajectòries sintètiques seguint aquest arbre sintètic.

7.2.2 MITIGACIÓ

L'objectiu principal és reduir el risc de privacitat associat a les dades sense definir un principi clar de privacitat. Per tal de mitigar els riscos existents de la privacitat de les microdades de trajectòria, es proposa un model que afegeix soroll de forma aleatòria als punts espai-temporals reduint així la resolució espacial o temporal de les dades, o com a mínim retallar les trajectòries. Aquesta estratègia, però, no assegura que es preservi la privacitat de les dades. És aleshores quan es proposa un nou model presentat per a preservar la privacitat en els recorreguts que fan servir GPS basat en la mitigació de les zones mixtes. Una zona mixta és una regió espacial en la que els punts espai-temporals dels usuaris no són enregistrats i, a més, els pseudoidentificadors dels usuaris seran modificats cada cop que entrin a una nova zona mixta. Si s'aconsegueix afegir quantitats suficients de trajectòries en una zona mixta serà molt difícil per a un atacant reconèixer un usuari en el moment que deixi aquesta zona. Com es pot apreciar l'efectivitat de l'heurística dependrà completament de la quantitat de trajectòries espai-temporals que atrevessen la zona mixta durant un interval particular de temps.

Les tècniques proposades, es basen principalment en la transformació que pateixen les dades:

7.2.3 OFUSCACIÓ

Aquesta tècnica consisteix en afegir soroll per tal de distorsionar les dades de les localitzacions. És introduïda per primer vegada per evitar possibles atacs a través de la mineria de dades de localització per Agrawl i Srikant [5] i formalitzada més tard amb el nom d'ofuscació per Duckham i Kulik [8]. Cal destacar que uns anys més tard s'afegeixen diferents models a aquesta tècnica basats en l'addició d'una quantitat elevada de soroll aleatori a representacions de grafs socials amb els que demostren la capacitat per a reduir considerablement l'èxit en atacs d'enllaç de registre.

Els atacs d'enllaç de registre pertanyen a la categoria més investigada d'atacs, i defineixen el seu objectiu com la relació dels registres de les microdades de la trajectòria d'un usuari amb informació privada de la víctima. Aquesta informació inclou identificadors personals i dades privades sobre la seva mobilitat de la base de dades que es vol atacar. Per tant, un atacant podria aconseguir la relació d'aquests registres si la base de dades objectiu conté atributs sensibles.

7.2.4 ENCOBRIMENT

Es recolza en reduir la granularitat³ en les dades de trajectòria en dimensions d'espai o temps. Considerant la dimensió temporal, Hoh [10] es defineix una tècnica que demostra la capacitat de reduir de la reidentificació de un 85% a un 40% incrementant d'un a quatre minuts l'interval de mostreig de les microdades. En quant a la dimensió espacial, Murakami defensa a [16] la idea de suprimir uns punts determinats de cada trajectòria per tal de reduir les oportunitats per un atac d'enllaç de registre. El mateix autor afirma que amb la eliminació de 5 punts de cada trajectòria a cada base de dades es pot arribar a suprimir l'èxit d'atacs d'enllaç de registres fins a la meitat, tot i que continuaria sent un número molt alt. Posteriorment es presenten diferents treballs que continuen treballant amb la dimensió espacial, aquests afirmen que han treballat sobre una base de dades pròpia i que reduir la precisió geogràfica no té un clar efecte positiu sobre la unicitat. Posen en evidència aquestes aclaracions amb un experiment fet sobre aquesta base de dades, en el que si un atacant sap com a mínim 8 punts de la ruta de l'usuari objectiu la probabilitat d'èxit s'eleva fins el 50%.

7.2.5 SEGMENTACIÓ

Tècnica proposada per Song a [15] on proposa la segmentació de cada trajectòria i l'ús de diferents pseudo identificadors per a cada segment resultant. Aquesta segmentació és proposada donat que la unicitat augmenta paral·lament amb la longitud de cada trajectòria, de forma que pretén reduir-la al màxim per tal d'afavorir el resultat de l'anonimització, i que aquesta sigui en conclusió, menys única. Aquesta és una proposta teòrica, ja que com demostra el mateix autor en un experiment realitzat a una base de dades pròpia el 80% de les particions que es realitzaran seguiran sent úniques, fet que a part reduiria l'utilitat de les mateixes donat que evitarien molts anàlisis que requereixen de la informació completa sobre els moviments dels usuaris.

7.2.6 INTERCANVI

L'autor Salas a [14] Com bé indica el seu nom, basa el seu funcionament en l'intercanvi de porcions de trajectòries de forma iterativa entre els diferents usuaris, fent així de les trajectòries resultants segments composts de trajectòries de múltiples usuaris. Aquesta tècnica és coneguda com a SwapMob. Resultats de tests demostren la reducció real en l'efectivitat d'atacs d'enllaç de registre, tot i que afirmen que si un atacant sapigués 10 punts podria arribar a relacionar fins el 42% dels usuaris i aprendre el 50% de les trajectòries originals en el 5% dels casos.

³Representa el nivell de detall amb el que desitja emmagatzemar les dades tractades

7.2.7 ZONES MIXTES

Considerat el model més popular adoptat per les tècniques de mitigació de risc de privacitat, és considerat també molt important per a preservar la privacitat en models que es basen en la ubicació. Assumeix que un atacant podria rastrejar el seu objectiu en el pas del temps, fet que faria que s'hagi de protegir la seqüència completa dels punts espai-temporals i no pas punts individuals tal i com farien els models de serveis basats en localització. El primer model proposat per Beresford [2] garanteix que dins la zona mixta els atacs per enllaç de registre no es podran realitzar sempre i quan el nombre de trajectòries que surten de una zona mixta durant un mateix interval de temps sigui suficientment gran i si la seva entropia de mobilitat⁴ és suficientment gran per a que l'atacant no sigui capaç de saber cap a on anirà una trajectòria. Posterior a aquesta primera proposta, surgen de noves que miren de millorar l'estat actual. Es destaca la tècnica introduïda per Hoh i Gruteser [4] anomenada confusió de ruta, la qual intenta protegir els usuaris d'un possible enllaç de punts de la trajectòria al llarg d'un període de temps de forma que un atacant podria reconstruir la trajectòria inicial. Funciona de la següent manera: en lloc de basar-se en una zona en la que es barregen les trajectòries, es produeix una confusió de ruta, és a dir, sempre que dos o més rutes d'usuaris qualsevols siguin prou semblants entre elles la informació sobre la ruta d'un usuari es pertorbarà de forma que l'atacant confongui les seves rutes. A la **Figura 5** s'aprecia el seu funcionament. Una següent proposta feta per Hoh i altres investigadors a l'article [3], es basa en l'introducció d'un model que a més d'operar en la dimensió de l'espai opera també en la del temps. Demostra com amb aquesta tècnica més recent s'aconsegueix que un atacant tant sols pugui fer un seguiment continuat per ordre dels segons mentre que possibiliten l'ús d'aplicacions de control de trafic. De nou es continua refinant aquesta tècnica, i surgeix la necessitat de crear zones mixtes al voltant del conjunt de localitzacions sensibles que els usuaris visiten. Com a conclusió d'aquesta tècnica, s'extreu que el problema roman en trobar el nombre de zones mixtes òptim a desplegar. Aquest, és tractat per Liu en el seu article [12] on es proposen heurístiques que tindran en compte la influència de la densitat de la trajectòria. També es pot afegir, que en comparació amb les tècniques de segmentació o basades en intercanvi, aquesta limita la utilitat de les microdades de trajectòria per anàlisis que precisen d'un seguiment exhaustiu dels usuaris al llarg del temps.

8 MARC PRÀCTIC

Després de realitzar l'estudi de les diferents tècniques usades per tal de mitigar els riscos existents en la re-identificació d'usuaris, s'ha procedit amb un aprofundiment major en un dels mètodes portant aquest a la pràctica per tal de poder estudiar els resultats que s'obtinguerien en l'anonimització d'un conjunt determinat de dades i complir així amb els objectius marcats. Donada la complexitat d'alguns, l'estat de l'art realitzat, i les fonts d'informació de les que s'ha disposat el mètode escollit ha estat "Swap mobility location". L'experiment consta d'una part dedicada a la construcció del codi i la búsqueda de les dades, s'ha de tindre

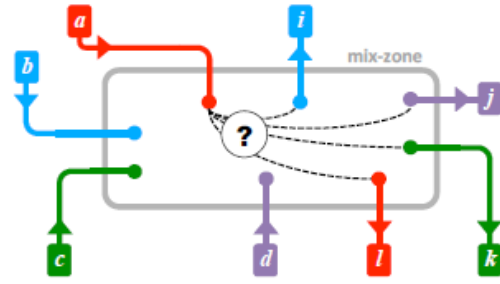


Fig. 5: Canvi de pseudonim al entrar a una zona mixta. Imatge extreta de [1]

en compte que aquest no s'ha trobat de forma oberta ("open source"), sinó que s'han trobat petites explicacions en forma de pseudocodi que s'han usat per a extreure una lleugera idea per a la posterior programació del codi. Les dades s'han extret de la base de dades de [13]. En primer lloc, es va realitzar aquest experiment a petita escala i un cop testejat i funcional s'exporta a un volum de dades molt major. Això ha estat possible gràcies a que s'ha facilitat l'accés a un servidor per a la seva execució donat que l'ordinador personal no suportava tal quantitat de càlculs. Finalment, una segona part dedicada a l'estudi dels resultats obtinguts i realització d'unes conclusions a partir de l'experiència empírica.

8.1 SWAP MOBILITY LOCATION

En aquest apartat es fa referència a l'algorisme implementat **Algorithm 1** així com els inconvenients trobats en el seu desenvolupament. A la **Figura 6**, es pot apreciar un resum del funcionament del mètode, en el que dos usuaris tenen a les seves rutes algun punt coincident i pels que s'aplica el l'algorisme. Aquest, el que fa és intercanviar les rutes dels usuaris amb punts coincidents a partir d'aques mateix punt. Cal aclarar que un cop un usuari ha patit un canvi, i en cas de tindre més punts coincidents, si aquests degut al canvi formen part d'un altre usuari aquesta modificació s'obviarà. Això es fa per a conservar en la mesura del possible la integritat de les dades per a que posteriorment no quedin inservibles.

8.1.1 INCONVENIENTS DEL MÈTODE

Com es pot veure a la **Figura 6**, aquest mètode no aplicarà per a usuaris que no tinguin cap punt en comú amb altres, és a dir, si un usuari està registrat a la base de dades amb una ruta única, i no coincident l'algorisme anterior no aplicarà en el seu cas. Aquest podria ser un problema en el cas que en la base de dades objectiu tots els usuaris tinguessin una ruta única, de forma que un atacant podria realitzar una re-identificació del conjunt d'usuaris. Tenint però, determinats usuaris amb ruta única i la resta amb punts coincidents, l'algorisme s'aplicarà a la resta i per tant un atacant no podria seguir per complet de que la seva re-identificació fos d'aquells als que no aplica el mètode i tindria altes probabilitats d'escollir un dels usuaris amb ruta modificada.

Intercanvi entre les localitzacions següents al punt en comú dels usuaris que el contenen, d'aquesta forma es canviaria l'identificador per tots els punts posteriors.

⁴la diversitat de direccions que prenen un cop deixen la zona mixta



(a) Conjunt de localitzacions posteriors a l'aplicació de l'algoritme (b) Conjunt de localitzacions previs a l'aplicació de l'algoritme

Fig. 6: Comparació aplicació del mètode

8.1.2 DADES

El conjunt de dades és extret d'una base de dades que conté les diferents trajectòries a partir del GPS d'usuaris que han fet servir taxis desde el 2 de Febrer del 2008 fins el dia 8 de Febrer del mateix any, a Pequín. L'experiment es realitza amb un conjunt de 100 usuaris on el nombre de localitzacions trobades per és variant per cada un. Les dades s'emmagatzemen en fitxers diferenciats per cada usuari, en cada fitxer el format apareix com un cúmul de línees, on cada línea representa una localització en un moment determinat per l'usuari tractat. Dins la línea trobem les següents dades separades per comes:

- ID de l'usuari.
- L'any, el mes i el dia en format YYYY-MM-DD.
- L'hora en que es recull la localització en format HH:MM:SS
- Longitud.
- Latitud.

En la realització d'algun dels experiments les dades es retallen fins un total de dos decimals, el que suposa un desviació d'uns 20 metres aproximadament de la posició inicial. S'ha decidit retallar les dades per a aconseguir un major nombre de localitzacions coincidents entre usuaris, donat que és complicat trobar usuaris que hagin coincidit en una posició exacta, i poder així mostrar en major mesura el resultat d'aplicar aquest mètode.

8.2 RESULTATS

Amb l'objectiu de poder evaluar el mètode implementat, i comprovar si el seu ús en un cas real tindria més beneficis que pèrdua en el valor de les dades es realitzen diferents experiments amb les mateixes dades però condicions canviants. En el primer, l'execució es du a terme amb les dades extretes directament de la base de dades, en el segon es retalla un decimal per tal de poder agrupar un major nombre d'usuaris, i per acabar es retallen fins dos decimals tant de la latitud com de la longitud. S'adjuntarà una taula per cada una de les execucions, la qual es podrà comparar amb la **Taula 1** que contindrà els punts inicials i finals dels usuaris sense modificar.

Els individus agafats en cada una de les execucions són els mateixos, s'han agafat els 5 primers del llistat d'usuaris.

8.2.1 EXECUCIÓ ÍNTEGRA

En aquesta primera execució, s'aprecia un nombre molt petit de canvis efectuats, concretament 8, entre usuaris tenint en compte la quantitat de usuaris de la que es disposava. Com es veu a la **Taula 2** els usuaris escollits tindran la mateixa latitud i longitud que haurien tingut en el cas de no haver aplicat cap mètode de protecció de micro dades de trajectòria. Això és així donat que les coordenades consten de fins a 5 decimals, fet que augmenta molt el nivell de precisió de les localitzacions i que dificulta que cap altre usuari tingui la mateixa.

8.2.2 EXECUCIÓ AMB UN DECIMAL RETALLAT

Obviant un decimal, tot i que el nombre de canvis efectuats al conjunt d'usuaris de la base de dades és major, exactament de 24 canvis de 100 usuaris, no s'aconsegueix reflectir cap canvi en els usuaris escollits. Com es pot apreciar a la **Taula 3** les coordenades finals seran exactament les mateixes que en els dos casos anteriors, i per tant, no hauran petit cap canvi en les respectives trajectòries.

8.2.3 EXECUCIÓ AMB DOS DECIMALS RETALLATS

Retallant fins a 2 decimals de cada coordenada s'aconsegueix reflectir els canvis en els usuaris escollits en un principi. Tal i com es veu a la **Taula 4**, i agafant d'exemple l'usuari 1, les coordenades inicials són les mateixes però s'arriba a un punt final diferent, producte de l'aplicació del mètode.

8.2.4 UTILITAT DE LES DADES

Retallar decimals fa que es perdi exactitud en quant a les trajectòries dels usuaris, però com s'ha comprovat, dins un escenari on l'exactitud de les localitzacions és tan definida, es converteix en un recurs necessari per tal d'aconseguir un nombre més alt de coincidències i poder protegir la intimitat de més persones. Un major nombre de canvis implica també una major pèrdua d'integritat de les trajectòries reals dels usuaris, les quals han de quedar el més semblant possibles per tal de poder ser aprofitades en posteriors estudis. En aquests experiments s'ha pogut comprovar com el mètode canvia els punts finals als que arribaran els usuaris; prenent de nou la Figura 4, s'ha fet una búsqueda exacta a referència a google maps, per tal de visualitzar amb total exactitud la diferència que hi ha en la ruta final d'un usuari

amb ruta modificada i sense modificar. Representada aquesta desviació gràficament a la Figura X, es veu que la posició final del usuari 1 real en comparació amb la modificada dista exactament de X metres, distància força gran de cara a la integritat de les dades.

REFERÈNCIES

- [1] Ulrich Aïvodji. Privacy of trajectory micro-data: a survey, 2019.
- [2] Alastair Beresford and Frank Stajano. Location privacy in pervasive computing, 2003.
- [3] B.Hoh, M.Gruteser, H.Xiong, and A.Alrabady. Preserving privacy in gps traces via uncertainty-aware path cloakin, 2007.
- [4] B.Hoh, M.Gruteser, H.Xiong, and A.Alrabady. Achieving guaranteed anonymity in gps traces via uncertainty-aware path cloaking, 2010.
- [5] Jordi Casas Roma and Cristina Romero Tris. *Privacidad y anonimización de datos*. Editorial UOC, 2017.
- [6] Rui Chen, Benjamin Fung, Marco Sossou, N’eriah, and Marco Fiore. Differentially private transit data publication: A case study on the montreal transportation system, 2012.
- [7] Josep Domingo-Ferrer and Trujillo-Rasua Rolando. Microaggregation-and permutation-based anonymization of movement data. information sciences, 2012.
- [8] Matt Duckham and Lars Kulik. A formal model of obfuscation and negotiation for location privacy, Berlin 2005.
- [9] Marco Gramaglia and Marco Fiore. Hiding mobile traffic fingerprints with glove. in proceedings of the 11th acm conference on emerging networking experiments and technologies, page 26, 2015.
- [10] Baik hoh, Marco Gruteser, Hui Xiong, and Ansaf Alrabady. Enhancing security and privacy in traffic-monitoring systems, 2006.
- [11] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. Privacy beyond kanonymity and l-diversity. in data engineering, 2007.
- [12] Xinxin Liu, Han Zhao, Miao Pan, Hao Yue, Xiaolin Li, and Yuguang Fang. Traffic-aware multiple mix zone placement for protecting location privacy, 2012.
- [13] Klara Nahrstedt and Long Vu. Crawdad, 2012.
- [14] Julián Salas, David Megías, and Vicenç Torra. Swapping trajectories for mobility anonymization, 2018.
- [15] Y. Song, D Dahlmeier, and Bressan S. A simple and effective algorithm for anonymizing location data. in international workshop on privacy preserving ir, 2014.
- [16] T.Murakami, A.Kanemura, and H.Hino. Group sparsity tensor factorization for reidentification of open mobility traces, 2017.

Appendices

A TAULES DE RESULTATS

A.1 TRAJECTÒRIES INICIALS

TAULA 1: Trajectòries inicials

ID	Longitud inicial	Latitud inicial	Longitud final	Latitud final
1	116.51172	39.92123	116.54723	39.90841
2	116.36422	39.88781	116.26975	39.92127
3	116.35743	39.88957	116.43003	39.93209
4	116.47002	39.90660	116.52252	39.92111
5	116.62934	39.82726	116.59029	39.83682

A.2 EXECUCIÓ SENSE RETALLS

TAULA 2: Execució sense retalls

ID	Longitud inicial	Latitud inicial	Longitud final	Latitud final
1	116.51172	39.92123	116.54723	39.90841
2	116.36422	39.88781	116.26975	39.92127
3	116.35743	39.88957	116.43003	39.93209
4	116.47002	39.90666	116.52252	39.921111
5	116.62934	39.82726	116.59029	39.83682

A.3 EXECUCIÓ RETALLANT UN DECIMAL

TAULA 3: Execució amb retall d'un decimal

ID	Longitud inicial	Latitud inicial	Longitud final	Latitud final
1	116.5117	39.9212	116.5472	39.9084
2	116.3642	39.8878	116.2697	39.9212
3	116.3574	39.8895	116.4300	39.9320
4	116.4700	39.9066	116.5225	39.9211
5	116.6293	39.8272	116.5902	39.8368

A.4 EXECUCIÓ RETALLANT DOS DECIMALS

TAULA 4: Execució amb retall de dos decimals

ID	Longitud inicial	Latitud inicial	Longitud final	Latitud final
1	116.511	39.921	116.590	39.836
2	116.364	39.887	116.465	39.92
3	116.357	39.889	116.318	39.951
4	116.470	39.906	117.107	40.114
5	116.629	39.827	116.289	39.957

Algorithm 1: Swap Mobility Location

```

1 for element in coordenades do
2   | Creem un diccionari que guardi les coordenades per cada usuari
3 end
4 for element in len(diccionari.items()) do
5   for actual in diccionari.values()[element] do
6     | for seguent in diccionari.values()[element+1] do
7       | if actual==seguent then
8         |   afegir a un array que omplirem amb el valor de les interseccions
9       | else
10        |   No fer res
11       | end
12     | end
13   end
14 end
15 if nombre de vegades que es repeteix una localització més gran que lambda then
16   | Afegir la localització al array
17 else
18   | No afegir la localització
19 end
20 for element in interseccions do
21   for elementValorsInicials in coordenades do
22     | while contador j valors que hi hagi a l'element do
23       | if valor d'aquesta intersecció == element then
24         |   guardem el identificador de l'usuari d'aquesta posició
25       | else
26         |   Següent element
27       | end
28     | end
29   end
30 end
31 while recorrem tots els ids repetits do
32   | trobem aquest identificador a les coordenades inicials for x in identificador.Values() do
33     | busquem el valor que tenim emmagatzemat d'aquest identificador que és repetit. Afegim les localitzacions
34     | següents a un array
35   end
36 for x in la resta de identificadors repetits do
37   | for y in les posicions d'aques id en les coordenades inicials do
38     | if si trobem la coordenada que busquem then
39       |   Afegim les localitzacions següents a un array
40     | else
41       | end
42   | end
43   | fem el swap dels dos arrays
44 end

```
