Detecció de Comunitats amb Privacitat Diferencial

Martí Llinés Viñals[1] , Julián Salas[2]

Abstract—Per tal d'afavorir la recerca, les organitzacions publiquen les seves dades. Aquestes dades es protegeixen per no revelar cap mena d'informació personal de les persones implicades. Si parlem de grafs, una propietat única d'aquesta estructura de dades és la manera que tenen els nodes d'agrupar-se entre ells, conegut com a detecció de comunitats. Aquesta informació té diversitat d'aplicacions, i per tant seria interessant que fos una propietat que canviés el mínim possible. En aquest TFG observarem com afecta la protecció, també coneguda com anonimització, dels grafs a la detecció de comunitats.

Paraules clau—Grafs, Detecció de Comunitats, Privacitat Diferencial

1 Context

El graf com a estructura de dades té dos components principals: els nodes, que acostumen a representar entitats; i les arestes, que connecten els nodes. Es poden classificar principalment segons si les arestes tenen sentit d'un node cap a l'altre (aleshores es parla d'un graf dirigit o no dirigit) i segons si les arestes tenen un valor numèric associat (i per tant es denominaria ponderat o no ponderat). Les arestes solen indicar certa proximitat o similaritat entre els nodes, coneguts també com a vèrtexs. Això dona pas a una gran quantitat d'estructures de diferents propietats geomètriques cadascuna, però en aquest TFG ens centrarem en les connexions (arestes) entre nodes, que aporten un nou nivell d'informació més abstracte: les comunitats.

Una comunitat, també anomenada mòdul o *clustering*, està formada per nodes, els quals estan relacionats entre ells mitjançant les arestes [1]. Aquesta definició és poc rígida, però denota que els nodes d'una mateixa comunitat són semblants entre ells, ja sigui per característiques, maneres de comportar-se o ambdues, depenent del context del graf [2]. Cal remarcar que la informació que aporten els *clusterings* és abstracta: la similaritat mencionada anteriorment ve donada per les característiques del graf, no dels possibles atributs que puguin tenir els nodes. També és abstracta la pròpia comunitat, atès que hi ha diferents algorismes per detectar-les i a vegades donen resultats diferents com es mostra a Fig. 1.

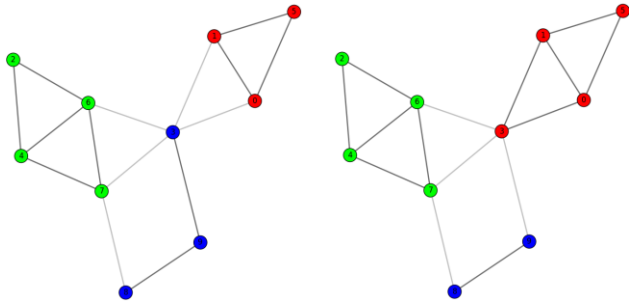

Fig. 1. Detecció de comunitats d'un mateix graf realitzada amb els algorismes *Walktrap* a l'esquerra i *Multilevel* a la dreta. Els nodes estan colorits segons el *clustering* el qual pertanyen.

2 Objectius

Els objectius d'aquest Treball de Final de Grau són els següents:

1. Analitzar la informació que aporta un graf, sobretot la detecció de comunitats.
2. Justificar la importància de la privacitat en un graf.
3. Explicar els diversos mètodes de privatització d'un graf.
4. Garantir que la privacitat diferencial es compleixi amb els diferents grafs.
5. Emprar diversos algorismes de detecció de comunitats per observar les diferències entre el graf original i el graf protegit.

3 Estat de l'art

3.1 Grafs. Detecció de comunitats

Si bé a la introducció es parla sobre què és una comunitat, en aquest apartat ampliarem el concepte i els seus usos.

La detecció de comunitats té diverses aplicacions, com la recomanació d'usuaris o contingut a una xarxa social [3], detecció de patrons en medicina [4] o ciberseguretat [5], entre altres.

Com s'ha mencionat abans, la definició de comunitat és poc rígida. Una definició informal però més específica seria que un *cluster* és un grup de nodes densament interconnectats (mitjançant les arestes) en comparació amb la resta de

1 Correu de l'alumne: Marti.Llines@uab.cat
2 Departament d'Enginyeria de la Informació i de les Comunicacions, Universitat Autònoma de Barcelona. Correu del tutor: julian.salas@uab.cat

nodes [2], [6]. No obstant, aquesta noció segueix essent susceptible a diverses interpretacions respecte com arribar a definir a una comunitat, i dona lloc a gran varietat d'algorismes segons la seva aproximació [7]. A continuació es mostren algunes interpretacions.

1. Aproximacions basades per modularitat: consisteix a definir dues mesures pels conceptes de "cohesió" i "separació" per després computar la seva diferència o proporció. La variant més coneguda és la modularitat definida per [8].
2. Aproximacions basades en similaritat de nodes: es té en compte com de semblants són els nodes comparats amb els de la resta del mapa. Si dos nodes comparteixen la majoria de veïns[1], probablement pertanyin a la mateixa comunitat [9].
3. Aproximacions basades en eliminació de nodes: es basa en eliminar els nodes que estiguin "enmig" de les comunitats per així formar comunitats aïllades [8].
4. Aproximacions basades en difusió: estableix el paradigma que els nodes poden enviar un missatge als seus veïns. Al final els nodes d'una mateixa comunitat comparteixen el mateix missatge [10].

Tornant a la modularitat mencionada a 1), aquest valor es fa servir per indicar la qualitat de les comunitats detectades, independentment de quina aproximació faci servir l'algorisme de detecció de comunitats. Segons [11], un *cluster* que tingui una modularitat d'entre 0,3 i 0,7 normalment té una estructura de comunitat forta.

3.2 Protecció de dades

Abans de res, és important saber el motiu el qual es fan servir els mètodes de privatització en primer lloc. En altres paraules, per què una organització no pot publicar les dades tal i com són? A la Unió Europea, publicar dades d'un individu no protegides consta com a violació de la *GDPR*. Segons la definició proporcionada a l'article 4 de la *General Data Protection Regulation* [12], "'Dades personals'" significa "tota informació sobre una persona física identificada o identificable". Amb això, les dades no protegides i publicades poden ser penalitzades, en la majoria dels casos, per la *GDPR* si la informació fa referència a persones. No seria il·legal publicar dades que no facin referència a humans, com per exemple l'estructura d'una molècula, rutes d'aus migratòries, o informació veterinària (sempre i quan no es pugui identificar al propietari de la mascota). Tornant a l'activitat punible, una organització pot evitar els riscos de multa si protegeix les dades de manera que semblin anònimes. Segons el recital número 26 de la *GDPR* [12], els principis de protecció de dades no s'haurien d'aplicar a informació anònima. Així doncs, es pot concloure que les dades han de passar per un procés d'anonimització abans de ser publicades.

Existeixen diversos mètodes de protecció de dades. En aquest apartat parlarem principalment de dos mètodes i discutirem quin és més viable per a protegir un graf com a estructura de dades. El primer mètode és la k-anonimitat, la qual protegeix les dades de manera que cada registre té la mateixa informació que k-1 altres registres. D'aquesta manera, un atacant té una probabilitat de 1/k d'identificar correctament la seva víctima. La k-anonimitat es va definir per a dades tabulars, no per a grafs o altres estructures. Igualment, hi ha treballs com el de [13] que tracta de redefinir el concepte per a que sigui apte per a grafs, però també es menciona que s'hauria de complementar amb el que anomenen (k, l)-anonimitat. El graf protegit, doncs, consistiria de nodes on cadascun té el mateix nombre d'arestes que uns altres k-1 nodes. Així doncs, el principal motiu el qual es descarta la k-anonimitat en aquest TFG és perquè la protecció no necessàriament manté la densitat[2] del graf original. Això és rellevant perquè implica que l'addició o eliminació de tantes arestes afecta fortament a les comunitats que acaben formant els nodes.

El segon mètode, la privacitat diferencial, es basa en què el resultat d'una consulta a una base de dades no hauria de resultar afectada per la presència o absència d'un element al conjunt [14].

En el context de grafs, la privacitat diferencial es pot aplicar de diverses maneres:

1. *Edge differential privacy*: l'element que es considera absent o present és una sola aresta del graf.
2. *Node differential privacy*: l'element que es considera absent o present és un node del graf i totes les arestes relacionades amb aquest.
3. *Local differential privacy*: en aquest cas, la informació sobre totes les arestes és pertorbada, de manera que el graf emmagatzemat conté arestes que a la realitat són veritables i d'altres que no ho són.

Hi ha treballs que aborden les diverses definicions. Respecte la llista anterior, [15] aplica la el concepte de 1), [16] fa servir la noció de 2) i [17] proposa la manera de calcular l'existència de les arestes del graf protegit, seguint la definició de 3).

A diferència de la k-anonimitat, la privacitat diferencial és capaç de mantenir la densitat del graf. Tant en 1) com en 3) s'eliminen arestes (a 3) també s'afegeixen) i aleshores la densitat es pot corregir amb facilitat per a que sigui l'original. En el cas de 2) es podria estimar el nombre esperat d'arestes que s'eliminarien per node, cosa que en alguns grafs no alteraria massa la densitat resultant.

És important destacar que tot mètode d'anonimització té un *tradeoff* entre la privacitat proporcionada i la precisió de les dades resultants. Dels mètodes mencionats els paràmetres que ofereixen aquest pressupost de privacitat per la k-anonimitat i la privacitat diferencial són els valors k i ε respectivament. Del primer valor ja n'hem parlat i del segon l'explicarem més detalladament a l'apartat de metodologia. Els dos valors es comporten de manera contrària. Un valor de k alt implicarà que la protecció de la k-anonimitat sigui molt bona, però les dades serien inservibles. Passaria al revés amb un valor de k baix. En el cas d'ε per la privacitat

[1] Per a un node, un veí és aquell node el qual comparteix una aresta

[2] La densitat d'un graf relaciona el nombre d'arestes |E| i de nodes |V| que té. Per a grafs no dirigits, $Densitat = \frac{|E|}{|V| \cdot (|V|-1)}$

diferencial, si s'aproxima a 0 oferirà una alta privacitat però diferirà més de la informació original. A mesura que ε incrementa, la protecció serà menys efectiva però les dades s'aproximaran a la realitat.

Arrel de *tradeoff* mencionat, sorgeix la pèrdua d'informació en la protecció de dades. Aquesta consisteix a mostrar l'impacte que té anonimitzar les dades, comparant la informació original amb la protegida mitjançant valors numèrics. Si parlem de grafs, existeix gran varietat de mètriques per comparar-los. A l'apartat 4.5 s'explicaran les mètriques escollides considerades importants per a respondre l'objectiu 5.

4 METODOLOGIA

Aquest apartat està dedicat als últims dos objectius proposats. Els experiment consistirà a protegir un graf mitjançant la privacitat diferencial i avaluar la pèrdua d'informació a través d'unes mètriques seleccionades. En aquesta secció es plantejaran els experiments i es respondrà l'objectiu 4 a l'apartat 4.3.

4.1 Entorn d'execució

Els experiments es realitzaran amb *Python*. A més de l'ús de llibreries pròpies com per exemple per gestionar arxius i emmagatzemar objectes, es farà servir la llibreria *igraph* [18] per a la creació de grafs i detecció de comunitats.

4.2 Graf

El graf escollit pertany a la *Lightning Network* [19]. S'ha decidit simplificar el contingut del graf de manera que el graf resultant sigui no dirigit i no ponderat. Considerem que és un graf suficientment gran per al nostre experiment.

A la taula 1 es mostren algunes característiques sobre el graf. A la figura Fig. 2 s'observa un histograma dels graus (explicació al peu de la imatge) del graf.

TAULA 1
CARACTERÍSTIQUES GENERALS DEL GRAF

Característica	Valor
Nodes	10066
Arestes	18826
Densitat	0.00037

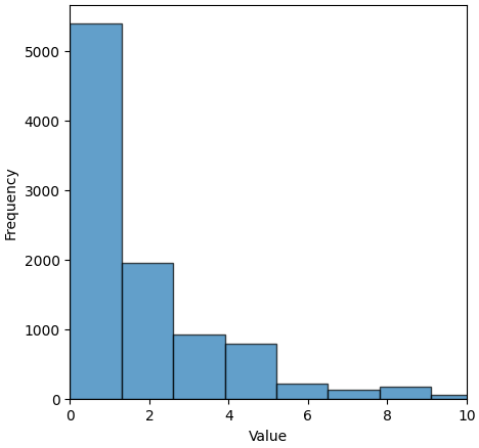

Fig. 2. Histograma de graus del graf. El grau fa referència al nombre de veïns que té un node. En aquesta representació es seleccionen els nodes amb menys grau (fins a 10), però formen part de més del 85% dels nodes al graf.

Amb la taula 1 i Fig. 2 s'extreuen dues conclusions. La primera és que, com que el graf és poc dens i un 50% de nodes tenen una sola connexió, és possible que les comunitats detectades presentin una baixa modularitat, atès que és probable que la majoria de comunitats estiguin formades per pocs nodes. La segona ve relacionada amb la primera, i és que l'anonimització del graf pot empitjorar la qualitat dels clusters, donant lloc a una baixa modularitat.

Amb això, s'ha decidit crear una variant del graf on no existeixin nodes aparellats, és a dir, que no hi hagi nodes on el seu únic veí tampoc tingui més veïns. Aquest graf té les següents propietats:

TAULA 2
CARACTERÍSTIQUES GENERALS DEL GRAF

Característica	Valor
Nodes	9272
Arestes	18429
Densitat	0.00043

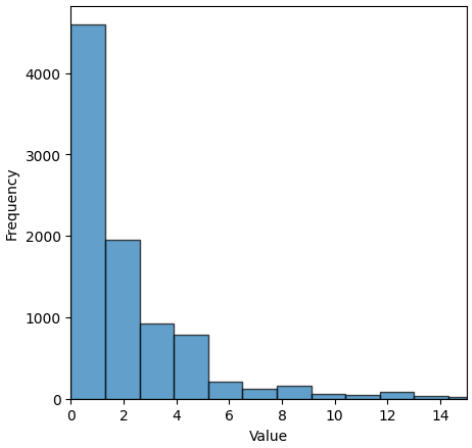

Fig. 3. Histograma de graus de la segona versió del graf.

És important destacar que s'han eliminat el 7,89% dels nodes respecte el graf original, però això només ha afectat al 2,11% de les arestes i un 1,15% a la densitat. Amb el segon

experiment hi ha l'objectiu addicional de comprovar com són les comunitats en el graf sense nodes que aportin més aviat poc a la xarxa (s'aporta poc perquè només s'interactua amb un altre node), i contrastar-ho amb el graf original.

4.3 Grafs protegits

Tal i com hem explicat a l'apartat 3.2, les dades seran més o menys anònimes en funció del valor de ε. Hem seleccionat un total de 13 valors per veure els canvis que ofereix tenir molta o poca privacitat. En resum,
$\varepsilon \in \{0.01,0.1,0.5,1,2,3,4,5,6,7,8,9,10\}$.

A l'apartat 4.4 es mencionarà que hi ha una selecció aleatòria en el procés d'anonimització. Per tal d'evitar irregularitats en cas que un únic graf doni resultats imprevistos, es faran servir 5 llavors diferents en aquell procés. Atès que les 5 llavors es faran servir per cada valor de ε, hi haurà un total de 65 grafs protegits.

4.4 Detecció de comunitats

Els algorismes de detecció de comunitats seleccionats per a les proves són *Label Propagation*, *Multilevel*, *Walktrap* i *Edge Betweenness*. A part de ser exemples de les aproximacions 4), 1), 2) i 3), respectivament, mencionades a l'apartat 3.1, els resultats de [20] han servit per a la decisió. Els temps d'execució són acceptables per a l'experiment, tret de l'últim que és més costós (vegeu Taula 3).

TAULA 3
COMPLEXITAT DELS ALGORISMES

Algorisme	Complexitat
Label Propagation	O(m)
Walktrap	$O(n^2 \cdot \log(n))$
Multilevel	$O(n \cdot \log(n))$
Edge Betweenness	$O(n^3)$

n representa nombre de nodes i m el nombre d'arestes

4.5 Privacitat diferencial

S'aplicarà la *Local differential privacy* definida anteriorment a l'apartat 3.2. El graf es protegirà amb la proposta adaptada de [17]. Per tal d'assegurar que el mètode sigui ε-diferencialment privat, la probabilitat p_o que una aresta segueixi sense existir després de protegir el graf es determinarà per ε i la densitat del graf original d_G que en grafs no dirigits es calcula de la següent manera amb el nombre de nodes |V| i el nombre d'arestes |E| del graf.

$$d_G = \frac{2|E|}{|V|\cdot(|V|-1)}.$$
$$p_0 = 1 - \frac{1}{e^{\varepsilon}-1+\frac{1}{d_G}}.$$

Similarment, la probabilitat p_1 que una aresta es mantingui després de la protecció serà

$$p_1 = \frac{e^{\varepsilon}}{e^{\varepsilon}-1+\frac{1}{d_G}}.$$

Aquestes probabilitats serviran per crear els grafs aleatoris, que en el nostre experiment farem servir el model d'Erdős-Rényi [21] El conjunt de grafs generats segons el nombre de nodes n i probabilitat p es denota $\mathcal{G}$(n, p). Cal esmentar que hi haurà dos conjunts $\mathcal{G}$(n, 1-p) i $\mathcal{G}$(n, 1-p) els quals de cadascun es seleccionaran 5 grafs per evitar irregularitats en cas que un únic graf doni resultats imprevistos. Al codi, això es tradueix a fer servir determinades llavors per generar els mateixos 5 grafs per cada conjunt.

El mecanisme $\mathcal{A}$ s'encarrega d'atorgar soroll a la matriu d'adjacència[3] del graf original G de manera que el graf resultant sigui ε-diferencialment privat és
$\mathcal{A}_{p0,p1}(G) = G \oplus \quad G_0 \oplus \quad G_1$, on

$G_0 = G' \setminus G \text{ per } G' \in \mathcal{G}(n, 1-p_0)$ i

$G_1 = G'' \cap G \text{ per } G'' \in \mathcal{G}(n, 1-p_1)$.

En resposta a l'objectiu 4, la privacitat diferencial es compleix, és a dir, que el mecanisme és ε-diferencialment privat si es compleix la següent inequació. Donats els valors $p_{00} = p_0;\ p_{01} = 1-p_0;\ p_{10} = 1-p_1;\ p_{11} = p_1$,
la inequació $e^{\varepsilon} \geq \max\left\{\frac{p_{10}}{p_{00}}, \frac{p_{11}}{p_{01}}, \frac{p_{00}}{p_{10}}, \frac{p_{01}}{p_{11}}\right\}$
ha de ser certa.

Les validacions corresponents venen proporcionades per [16]. Una observació d'aquest requisit és que el mecanisme serà sempre ε-diferencialment privat quan la densitat sigui inferior o igual a 0,5. Aquest requisit el compleix el graf original, cosa que implica que els 65 grafs protegits són ε-diferencialment privat pels respectius valors de ε.

4.6 Mètriques

Per determinar la pèrdua d'informació d'haver protegit les dades, mostrarem els resultats de tres paràmetres.

4.6.1 Coeficient de Jaccard

Donat un conjunt d'arestes E(G) d'un graf G, el coeficient de Jaccard entre dos grafs G i G' es calcula de la manera següent:
$Jaccard(G, G') = \frac{|E(G) \cap E(G')|}{|E(G) \cup E(G')|}$.

La mètrica serveix com a mesura de similaritat entre dos conjunts, i en aquest cas s'avaluarà la similaritat dels conjunts d'arestes.

4.6.2 Modularitat

Si bé no es fa servir directament en cap dels algorismes per detectar comunitats, aquest paràmetre serveix per demostrar la "facilitat" o "dificultat" que ha tingut un algorisme a detectar les comunitats. La "facilitat" o "dificultat" esmentada significa com de probable és que un node pertanyent al *clustering* assignat pertanyi realment a aquell mòdul i no a cap altre. La modularitat ja està implementada a la llibreria *igraph*.

4.6.3 Coeficient de Jaccard mitjà

Fent servir la primera mètrica mencionada, però amb cada comunitat detectada dels grafs a comparar. Cada mòdul d'un graf és un subgraf. Amb això, per cada *clustering* del

[3] Una matriu d'adjacència Adj representa de manera matricial les arestes que hi ha al graf. Donat un node i i un altre node j, $Adj_{(i,j)} = 1$ si existeix una aresta entre els dos nodes. En cas contrari, $Adj_{(i,j)} = 0$.

graf G, es busca en l'altre graf G' un candidat que serà aquell mòdul que més s'assembli (la cerca es fa amb el coeficient de Jaccard), s'emparellen i es suma la semblança. Després es repeteix el procés per un altre comunitat del primer, però no es tenen en compte els candidats ja emparellats del segon. Aquest bucle no tracta les comunitats formades per un sol node, però es tenen en compte per al càlcul final. Donat *emps*, un conjunt de tuples dels clusterings emparellats i *s(G)*, la funció que retorna la quantitat de mòduls formats per un únic node d'un graf G,

$$Jaccard\ mitjà(G, G') = \\ = \frac{\left(\sum_{i \in emps} \quad Jaccard(emps_i[1],\ emps_i[2])\right)}{|emps| + \min(s(G), s(G'))} + \\ + \frac{\min(s(G), s(G'))}{|emps| + \min(s(G), s(G'))}$$

No obstant, cal remarcar uns punts febles de la implementació. El primer punt és que el nombre de *clusters* per a un graf i per a un altre no tenen per què coincidir, donant lloc a mòduls desaparellats. Sabent això, la funció mira quin dels dos grafs té més comunitats detectades per decidir sobre quin graf iterar. D'aquesta manera, el codi programat produeix el màxim d'emparellaments. El segon punt va relacionat en part amb el primer, i és que la variació de comunitats detectades és degut a que les arestes afegides i eliminades durant el mecanisme per protegir les dades ajuntin o separin comunitats, Fig. 4 representa gràficament els casos plantejats. Respecte aquest punt, el codi no el resol i per tant no té en compte els mòduls desaparellats, però considerem que la mètrica segueix essent una aproximació decent per demostrar els objectius proposats.

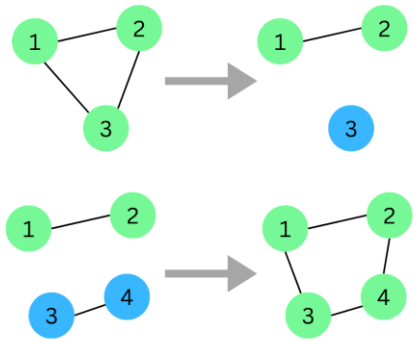

Fig. 4. A dalt, el procés d'anonimització elimina arestes en una comunitat formada per tres nodes, donant pas a dues comunitats detectades al graf protegit. A baix es representa el procés contrari: el graf protegit ha creat una comunitat a detectar de dues del graf original.

5 Procés de desenvolupament

El TFG ha progressat de la manera prevista pels informes de progrés (aproximadament). Hi ha hagut canvis a mesura que es definia més i més la metodologia. L'ús de llavors per homogeneïtzar els resultats obtinguts o el fet de descartar la possibilitat de mostrar algunes característiques generals de tant el graf original com els grafs protegits són alguns dels canvis.

L'experiment amb el segon graf proposat no era una idea inicial, només es va plantejar un cop visualitzat el graf. Amb el segon experiment es vol observar si afecta en gran quantitat l'eliminació de les comunitats més petites.

A part d'això, també hi ha hagut entrebancs. El més rellevant ha sigut el temps d'execució de l'algorisme *Edge Betweenness*, el qual justificava l'ús d'un node d'execució. De manera empírica es van calcular els temps d'execució de cada algorisme donat un graf protegit. Els resultats són els de la taula 4.

Taula 4
Temps d'execució dels algorismes

Algorisme	Temps en segons
Label Propagation	0.08231
Walktrap	1.257
Multilevel	0.27033
Edge Betweenness	79297.64574

Amb aquesta informació, el temps d'execució per un graf protegit concret es tradueix a 22 hores aproximadament. Assumint que es tractava d'un cas on l'algorisme va trigar un temps raonablement esperable donades les característiques del graf, es va sol·licitar l'accés a un dels nodes de la UAB per tal de, com a mínim, detectar les comunitats dels grafs protegits amb els diversos valors de ε per una sola llavor, a més de les comunitats detectades del graf original amb el mateix algorisme. Així doncs, abans de mostrar els resultats, volíem aclarir que els resultats relacionats amb *Edge Betweenness* s'han efectuat amb una sola llavor, en contrast amb les 5 que es fan servir amb els altres algorismes. Tenint en compte la poca variabilitat que presentaven els resultats de les 5 llavors en l'apèndix 1, considerem que hi ha una baixa probabilitat que els resultats on s'hagi fet servir l'algorisme *Edge Betweenness* ofereixin resultats poc precisos en comparació amb els altres. De totes formes, creiem que és important mantenir-lo per comparar el seu rendiment amb els altres escollits.

6 Resultats

A continuació es mostraran els resultats de les mètriques proposades a la metodologia, tant pel primer experiment com amb el segon.

6.1 Experiment 1

Aquest experiment s'ha realitzat amb el graf enunciat a la taula 1.

6.1.1 Coeficient de Jaccard

A la figura Fig. 5 s'observa un clar increment de la similaritat que presenten els grafs anonimitzats a mesura que el valor de ε incrementa. Això corrobora el *tradeoff* mencionat a la secció 3.2, on un valor de ε que s'aproximi a 0 garanteix més privacitat, però perquè les dades protegides

s'assemblen poc a les dades originals.

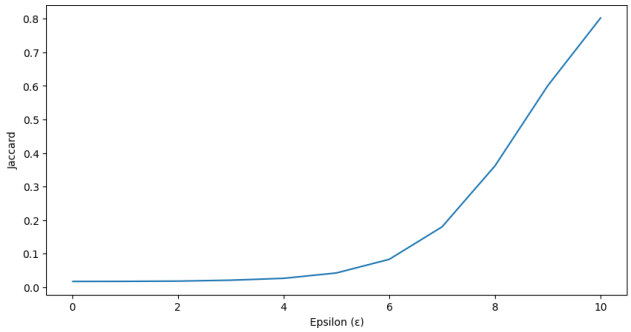

Fig. 5. Similaritat. Coeficient de Jaccard per a diversos valors de ε, primer experiment.

6.1.2 Modularitat

A la figura Fig. 6 es contempla una millora de la modularitat a mesura que creix ε de tots els algorismes exceptuant l'algorisme *Edge Betweenness* el qual millora de manera molt subtil. Amb els resultats anteriors, aquesta és la segona mètrica que segueix el *tradeoff* explicat. No obstant, cal recordar que la modularitat indica una certesa sobre si un node pertany a la comunitat que se li ha assignat. Per complementar aquesta informació es té la tercera mètrica

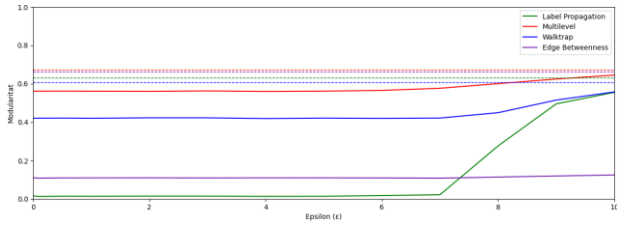

Fig. 6. Variació de la modularitat per a diversos valors de ε, primer experiment. Les línies horitzontals discontínues són les modularitats del graf original. Atès que potser la imatge és més aviat petita, s'enumeraran els valors de les modularitats del graf original en ordre descendent: *Multilevel*, *Edge Betweenness*, *Label Propagation*, *Walktrap*.

6.1.3 Coeficient de Jaccard mitjà

A la figura Fig. 7 es visualitza una irregularitat en la tendència degut als punts febles de la mètrica programada. En primer lloc, la tendència de ser més similar a mesura que el valor de augmenta la segueix l'algorisme *Multilevel* de manera més visible, seguit de *Walktrap*. En segon lloc, les comunitats detectades per *Edge Betweenness* són irreconeixibles. Aquest pobre resultat s'atribueix al funcionament de l'algorisme: si després de la protecció del graf resulta que els nodes que estaven "enmig" de les comunitats passen a estar aïllats o a estar més "dintre" d'una comunitat, és comprensible que les comunitats detectades siguin tan diferents a les originals. En tercer lloc, sembla que l'algorisme *Label Propagation* manté una similaritat relativament constant si es compara amb els altres. Si es considera tolerable una similaritat de Jaccard mitjana de 0,625 aproximadament, es podrien realitzar experiments amb altres grafs per determinar si *Label Propagation* és un algorisme apte per a grafs protegits.

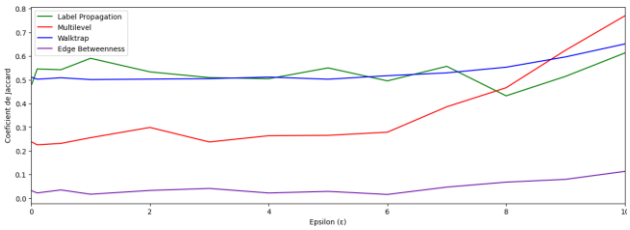

Fig. 7. Similaritat mitjana de Jaccard per a diversos valors de ε, primer experiment.

6.2 Experiment 2

Aquest experiment s'ha realitzat amb el graf enunciat a la taula 1. Veient el baix rendiment de l'algorisme *Edge Betweenness*, es descartarà per aquest experiment. A continuació s'observaran els resultats del segon experiment, dedicats a respondre l'objectiu addicional proposat de comprovar si la baixa modularitat és deguda al volum de comunitats formades per pocs nodes.

6.2.1 Coeficient de Jaccard

A la figura Fig. 8 s'observa una variació de la similaritat de Jaccard quasi bé idèntica a la del primer experiment. Això es deu a que el mecanisme d'anonimització de les dades altera les arestes que hi ha al graf amb més o menys probabilitat. Com que aquesta mètrica només contempla les arestes dels grafs, és comprensible arribar a un resultat semblant.

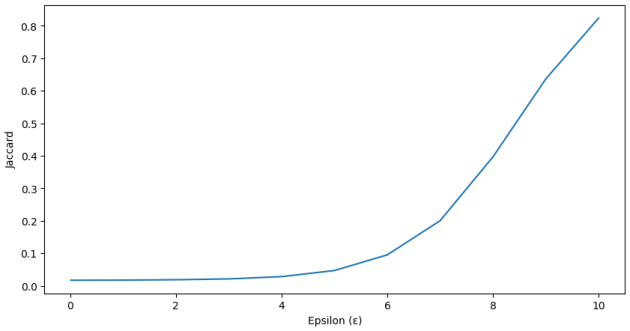

Fig. 8. Similaritat. Coeficient de Jaccard per a diversos valors de ε, segon experiment. La distinció més visible entre Fig. 5 i Fig. 8 és l'increment entre l'interval de valors de ε [7,9].

6.2.2 Modularitat

A la figura Fig. 9 es contempla un decrement insignificant de la modularitat. Aquesta gràfica nega el fet que el valor de modularitat en aquest graf es veu disminuïda pel nombre de *clusters* compostos de dos elements. Com amb el primer experiment, els tres algorismes de detecció de comunitats es comporten de la mateixa manera.

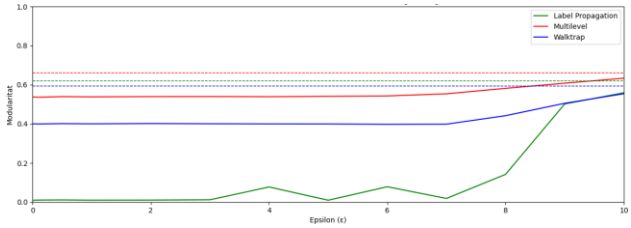

Fig. 9. Variació de la modularitat per a diversos valors de ε, segon experiment.

6.2.3 Coeficient de Jaccard mitjà

A la figura Fig. 10 es produeixen resultats semblants als del primer experiment, tot i que amb unes similaritats més baixes. Atès que es demostra el mateix patró, es confirmen completament les interpretacions dels resultats del primer experiment.

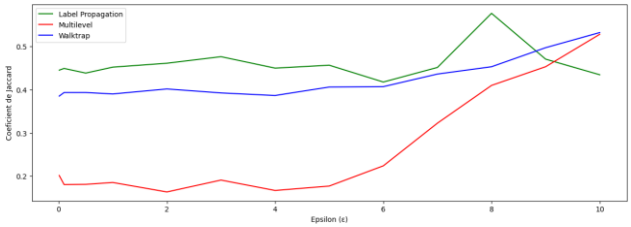

Fig. 10. Similaritat mitjana de Jaccard per a diversos valors de ε, segon experiment.

7 Conclusions

En aquest TFG s'han assolit els següents objectius:

1. S'ha descrit què és un graf i algunes les diverses interpretacions de com detectar comunitats en aquest.
2. S'ha explicat per què és obligatori protegir les dades relacionades amb les persones
3. S'ha justificat per què es privatitza un graf mitjançant la privacitat diferencial abans que amb k-anonimitat i s'han descrit mètodes més concrets del primer.
4. S'ha garantit que la privacitat diferencial es complirà durant el procés d'anonimització
5. S'ha observat com el *tradeoff* de privacitat contra utilitat afecta als grafs protegits i als diferents algorismes de detecció de comunitats.
6. Si bé el segon experiment resulta redundant, la interpretació d'aquest és que es pot eliminar una part d'un graf de baixa densitat per obtenir resultats semblants. Recordant el que es parla a [11], les modularitats obtingudes indiquen una estructura de comunitat forta.

Tot i així, el treball es podria ampliar de les següents maneres:

1. Realitzar l'experiment sobre més grafs, ja siguin similars o que formin altres estructures
2. Per a que la situació sigui la més real possible, habilitar tots els processos de l'experiment per a que es puguin tractar grafs dirigits ponderats.
3. Aplicar més mètriques de similaritat, no només observar la informació de les arestes
4. Simular atacs per identificar un node al graf protegit i avaluar la probabilitat de desanonimitzar una persona.
5. En relació amb 6), eliminar nodes de manera més o menys aleatòria per veure si els nous *clusters* identificats són igual de bons que els originals.

Agraïments

A Julián Salas, Guillermo Navarro-Arribas i Guillem García Dausà per acompanyar-me durant el transcurs del TFG responent qualsevol dubte plantejat.

Bibliografia

[1] Newman, M. E. (2003). The structure and function of complex networks. SIAM review, 45(2), 167-256.

[2] Fortunato, S. (2010). Community detection in graphs. Physics reports, 486(3-5), 75-174.

[3] Bedi, P., & Sharma, C. (2016). Community detection in social networks. *Wiley interdisciplinary reviews: Data mining and knowledge discovery*, *6*(3), 115-135.

[4] Rostami, M., Oussalah, M., Berahmand, K., & Farrahi, V. (2023). Community detection algorithms in healthcare applications: A systematic review. *IEEE Access*, *11*, 30247-30272.

[5] Park, J. H., & Kwon, H. Y. (2022). Cyberattack detection model using community detection and text analysis on social media. ICT Express, 8(4), 499-506.

[6] Danon, L., Duch, J., Arenas, A., & Díaz-Guilera, A. (2007). Community structure identification. In Large scale structure and dynamics of complex networks: from information technology to finance and natural science (pp. 93-114).

[7] Orman, G. K., Labatut, V., & Cherifi, H. (2012). Comparative evaluation of community detection algorithms: a topological approach. *Journal of Statistical Mechanics: Theory and Experiment*, *2012*(08), P08001.

[8] Newman, M. E., & Girvan, M. (2004). Finding and evaluating community structure in networks. Physical review E, 69(2), 026113.

[9] Pons, P., & Latapy, M. (2005). Computing communities in large networks using random walks. In *Computer and Information Sciences-ISCIS 2005: 20th International Symposium, Istanbul, Turkey, October 26-28, 2005. Proceedings 20* (pp. 284-293). Springer Berlin Heidelberg.

[10] Raghavan, U. N., Albert, R., & Kumara, S. (2007). Near linear time algorithm to detect community structures in large-scale networks. Physical Review E—Statistical, Nonlinear, and Soft Matter Physics, 76(3), 036106.

[11] Xie, J., & Szymanski, B. K. (2011, June). Community detection using a neighborhood strength driven label propagation algorithm. In 2011 IEEE Network Science Workshop (pp. 188-195). IEEE.

[12] European Union. (2016). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parlia-

ment and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[13] Stokes, K., & Torra, V. (2012). Reidentification and k-anonymity: a model for disclosure risk in graphs. Soft Computing, 16, 1657-1670.

[14] Dwork, C. (2006, July). Differential privacy. In International colloquium on automata, languages, and programming (pp. 1-12). Berlin, Heidelberg: Springer Berlin Heidelberg.

[15] Nguyen, H. H., Imine, A., & Rusinowitch, M. (2016, October). Detecting communities under differential privacy. In Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society (pp. 83-93).

[16] Zhang, S., Ni, W. W., & Fu, N. (2023). Community-Preserving Social Graph Release with Node Differential Privacy. Journal of Computer Science and Technology, 38(6), 1369-1386.

[17] Paul, S., Salas, J., & Torra, V. (2023, August). Edge local differential privacy for dynamic graphs. In International Symposium on Security and Privacy in Social Networks and Big Data (pp. 224-238). Singapore: Springer Nature Singapore.

[18] Csardi, G., & Nepusz, T. (2006). The igraph software package for complex network research. InterJournal, Complex Systems, 1695.

[19] Poon, J., & Dryja, T. (2015). The bitcoin lightning network. Scalable o-chain instant payments, 20-46.

[20] Yang, Z., Algesheimer, R., & Tessone, C. J. (2016). A comparative analysis of community detection algorithms on artificial networks. Scientific reports, 6(1), 30750.

[21] ERDDS, P.; R&WI, A. On random graphs I. Publ. math. debrecen, 1959, vol. 6, no 290-297, p. 18.

APÈNDIX

Apèndix 1. desviació estàndard de coeficient de Jaccard i modularitats per ε

Les mostres són de 5 elements, que equival a les llavors fetes servir.

ε	Coefficient de Jaccard	Modularitat de *Label Propagation*	Modularitat de *Multilevel*	Modularitat de *Walktrap*
0.01	0.000076	0.004207	0.001291	0.002658
0.1	0.000091	0.002186	0.000943	0.002081
0.5	0.000097	0.003459	0.002744	0.002592
1	0.000027	0.003471	0.002503	0.001859
2	0.000142	0.002525	0.002483	0.002011
3	0.000329	0.001823	0.001602	0.00237
4	0.000343	0.002148	0.004013	0.004948
5	0.000698	0.001359	0.002791	0.002646
6	0.001638	0.001325	0.000752	0.001873
7	0.002718	0.001062	0.003493	0.008597
8	0.002486	0.185984	0.004035	0.00771
9	0.002544	0.060601	0.001705	0.004636
10	0.00217	0.046857	0.000959	0.003401