# TFG: Privacy in dynamic graphs
# Informe de progrés (II)

Guillem Garcia [NIU: 1636279]

Data d'entrega: 25/05/2025

## 1 Recapitulació

Aquest informe és una continuació de *l'Informe de progrés (I)*, en el qual es van repassar els fonaments teòrics i pràctics del projecte, així com el disseny inicial i la implementació dels mètodes de privacitat. En aquesta segona fase, es detallen els avenços realitzats a partir del punt en què es va concloure l'informe anterior, tot centrant-se en el desenvolupament i avaluació dels mètodes proposats sobre els conjunts de dades seleccionats.

## 2 Desenvolupament (continuació)

S'han establert les mètriques per observar com canvien a nivell d'utilitat, a nivell estructural entre grafs, i quina és la pèrdua d'informació. Les mètriques que s'han escollit són les següents:

1. **Índex de Jaccard:** Per una banda ens serveix per observar la similaritat entre connexions dels grafs protegits i originals. Per l'altra, s'ha utilitzat com a mesura de similaritat entre els nodes més centrals dels algorismes de *Betweenness*, *Closeness* i *Degree Centrality*.

2. **DeltaCon** [10]**:** Mesura de similaritat estructural entre dos grafs, que es basa en l'afinitat entre nodes. A diferència del índex de *Jaccard*, aquest no només considera els enllaços directes, sinó també els camins indirectes. És a dir, té en consideració la influència dels nodes amb la resta de la xarxa.

3. **Densitats dels grafs i graus dels nodes**: Informació d'utilitat per comparar si els grafs que es generen comparteixen el nombre de connexions respecte els grafs originals.

   Tenint les mètriques, s'ha adaptat el diagrama de classes que correspon a la *Figura 1.* S'ha afegit un mòdul anomenat *Metrics*, que implementa aquestes, guarda els resultats en format *.json*, i també permet visualitzar-les.

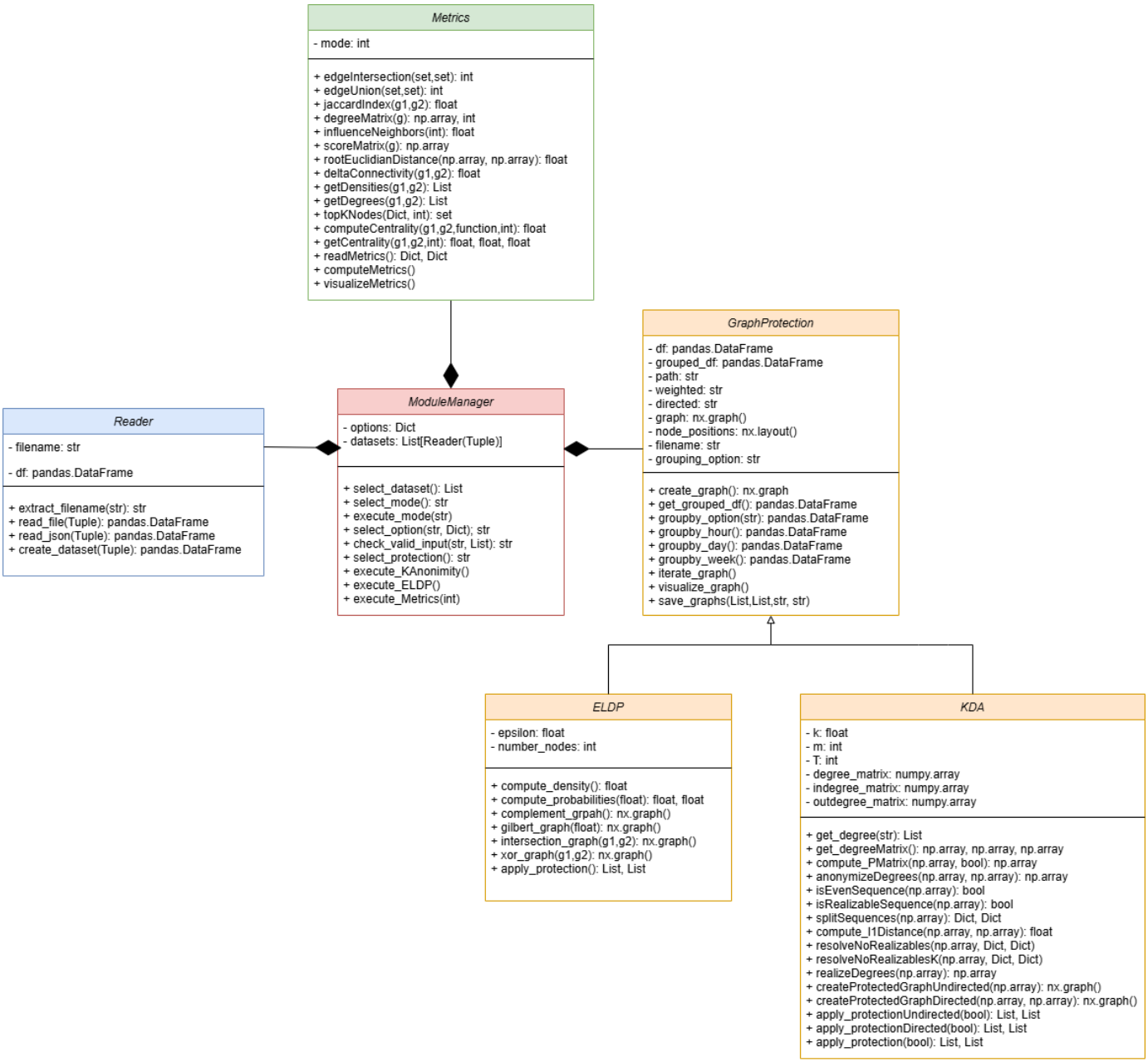


Figura 1: Diagrama de classes amb la incorporació del mòdul *Metrics*, que permet calcular i visualitzar les mètriques corresponents.

Un cop completada la implementació, es va decidir prioritzar l'anàlisi de la generació de comunitats i com comparar-los de forma dinàmica. Per tal de dur a terme aquesta tasca, s'utilitza [11], que implementa diversos algorismes basats en el mètode *TSCAN*, els quals tenen com a objectiu identificar nodes que actuïn com a *StableCores* dins les xarxes temporals. Per formar *StableCores*, els nodes han de mantenir una similaritat estructural ($\epsilon$) amb un cert nombre de veïns ($\mu$) en múltiples *snapshots* temporals ($\tau$) consecutius. Es tenen els algorismes:

- **TSCAN-B:** Aquesta és la versió bàsica del algorisme, on no s'utilitza cap eina de *pruning* per fer *clustering* de *StableCores*.
- **TSCAN-A:** A diferència de *TSCAN-B*, s'utilitzen tècniques de *pruning* per descartar en primer lloc els nodes que no siguin candidats a *StableCores*.
- **TSCAN-S:** És una variant que utilitza directament *StrongCores*, una relaxació dels *StableCores*, com a nucli per a formar les comunitats, obtenint una major eficiència a canvi d'una lleugera pèrdua de precisió.

També es tenen mètriques per mesurar la qualitat de les comunitats generades, que són les següents:

- **Separabilitat (AS):** Mesura fins a quin punt una comunitat està ben separada de la resta de la xarxa. Es calcula com la proporció entre el nombre d'arestes temporals internes (entre nodes de la comunitat) i el nombre d'arestes temporals externes (entre nodes de dins i fora de la comunitat). Un valor alt indica una comunitat ben delimitada.
- **Densitat (AD):** Indica la connectivitat interna de les comunitats. Es defineix com el nombre mitjà d'arestes temporals per node dins de cada comunitat. Com més alt sigui aquest valor, més interaccions hi ha entre els membres de la comunitat.
- **Cohesió (AC):** Reflecteix la dificultat de dividir una comunitat en subcomunitats. Quan més alt és el valor indica que les comunitats estan més cohesionades (més díficil de separar).

# 3 Resultats

Després d'aplicar els mètodes de privacitat als datasets, s'han calculat i visualitzat les corresponents mètriques. Atès que ambdós algorismes incorporen processos aleatoris, s'ha decidit executar-los cinc vegades per analitzar el seu comportament de manera més robusta.

Llavors, s'ha fet aquest procediment per tots els *datasets*, però principalment les diferències són notòries segons com de grans i densos són els grafs. Per això, es mostraràn els resultats més destacables dels *datasets*: *mammalia-voles*, *insecta-ant-colony* i *enron-employees*.

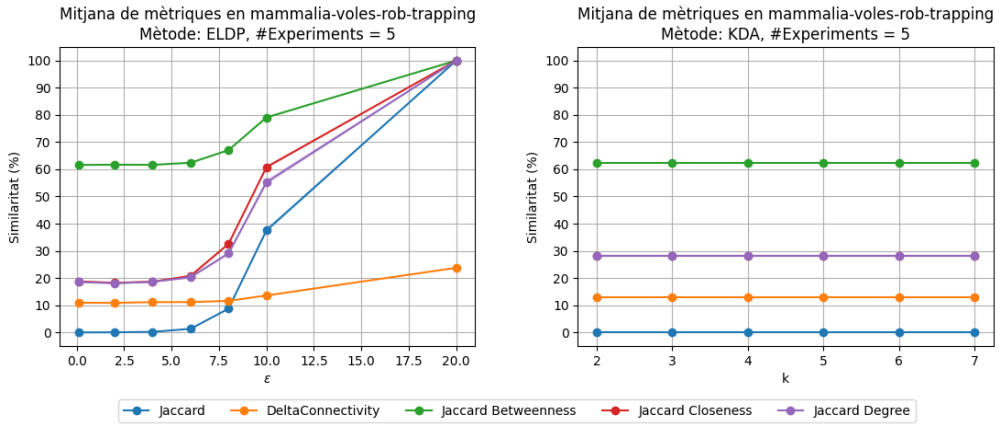


Figura 2: Mitjana de mètriques de similaritat en *mammalia-voles*. Els gràfics representen el valor de les mètriques per cada paràmetre dels algorismes de privacitat utilitzats.

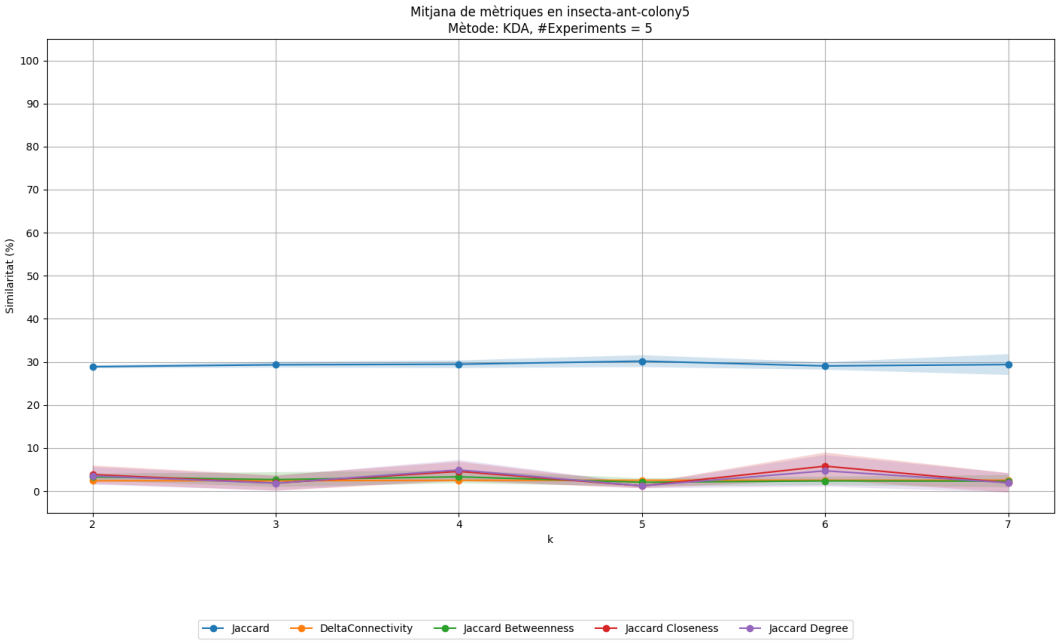


Figura 3: Mitjana de mètriques de similaritat en *insecta-ant*. En aquest cas només s'ha fet *K-Degree Anonimity*, perquè les densitats dels grafs són majors a 0.5, el que vol dir que no es pot realitzar *ELDP* per definició.

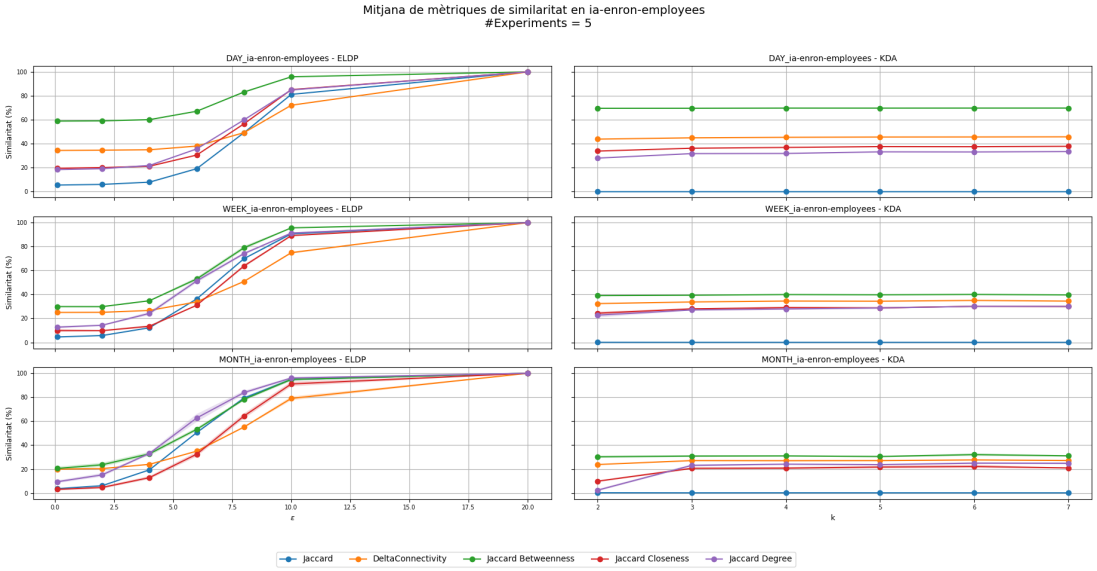


Figura 4: Mitjana de mètriques de similaritat en *enron-employees*. Els gràfics representen el valor de les mètriques per cada paràmetre dels algorismes de privacitat utilitzats per cada agrupament temporal.

Les *Figures 2,3 i 4* representen la mitjana de les mètriques de *similaritats* pels dos algorismes en cada *dataset*. Cal recalcar que pel càlcul de les mètriques de centralitat, s'ha escollit fer *l'índex de Jaccard* pel 5% de nodes més centrals. Es poden fer vàries observacions en aquests gràfics:

1. En l'algorisme *ELDP* es pot controlar la pèrdua d'informació i d'utilitat segons el paràmetre $\epsilon$. Quan es tria una major $\epsilon$, s'està afegint menys soroll, el que implica que siguin més similars els grafs protegits en comparació als originals.

2. L'algorisme *KDA* no implica el que passa en *ELDP*, i es veu que els resultats són similars per totes les $k$ provades. Sobretot, són sorprenents els valors obtinguts. El motiu de ser baixos per tots els conjunts de dades, es deu a la reconstrucció dels grafs amb *Havel-Hakimi*. Utilitzant *Havel-Hakimi* no t'assegura que els nodes dels grafs tinguin els veïns que es tenien en l'original, el que afecta directament a aquestes mesures.

També s'ha notat diferències entre els algorismes en les gràfiques de densitats i de graus, com es poden veure en les *Figures 5, 6 i 7*. En cas de *ELDP*, la densitat es preserva quan s'aplica la protecció als grafs en tots els casos. En *KDA*, es preserva la densitat segons la $k$, i segons quina densitat tenen els grafs originals. Per exemple, si la densitat i els graus són molt baixos (per defecte) com en *mammalia-voles*, els grafs que generen són buits, pel simple fet que les medianes que es calculen en l'algorisme i s'assignen és igual a 0.

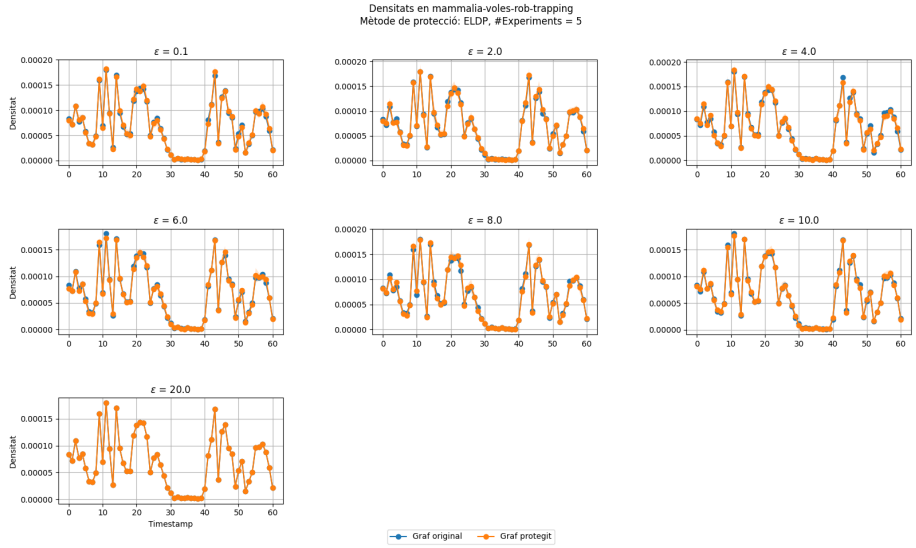


Figura 5: Densitats pel mètode *ELDP* del *dataset mammalia-voles*. Es pot comprovar en aquesta imatge com l'algorisme preserva la densitat en els grafs protegits.

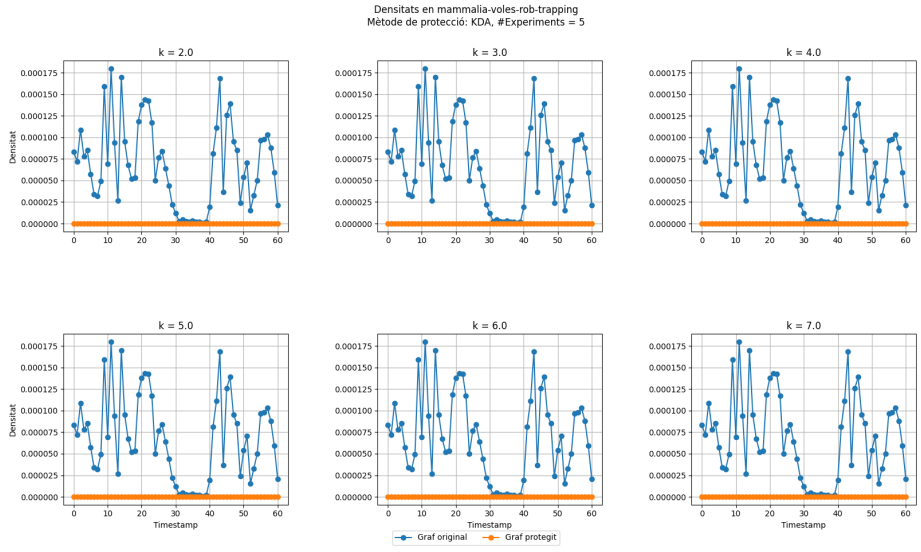


Figura 6: Densitats pel mètode *KDA* de *mammalia-voles*. Aquí les densitats dels grafs protegits és 0, el que vol dir que generen grafs buits.

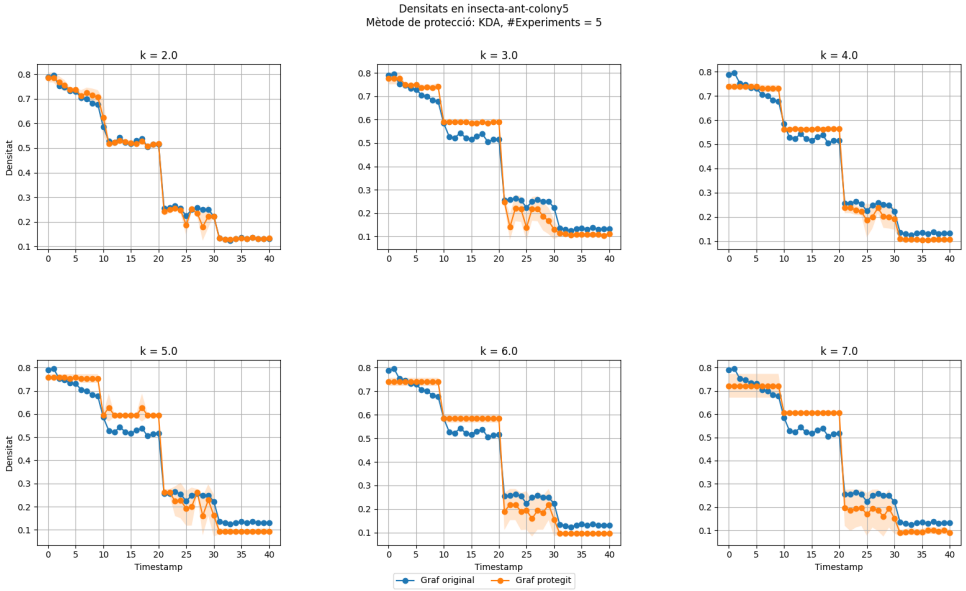


Figura 7: Densitats pel mètode *KDA* del *dataset insecta-ant-colony*. Es pot veure que més o menys en aquest cas es preserva la densitat. Quan menor és el paràmetre $k$, les densitats s'assemblen més als grafs originals.

| | $\epsilon$ | $\mu$ | $\tau$ |
|---|---|---|---|
| Valor per defecte | 0.2 | 3.0 | 3.0 |
| Valors utilitzats | [0.2, 0.5, 0.8] | [3.0, 5.0, 10.0] | [3.0, 5.0, 10.0] |

Taula 1: Paràmetres utilitzats per a la detecció de comunitats

Seguidament, s'han calculat les mètriques de detecció de comunitats per *TS-CAN*. Com a començament, s'ha establert un valor ($\epsilon$-$\mu$-$\tau$) per defecte, i després s'han realitzat experiments variant els paràmetres. Els paràmetres utilitzats són els de la *Taula 1*. Un exemple dels resultats que obtenim són la *Figura 8 i 9*, que es visualitzen els resultats de les mètriques per cada possible mètode. Com es poden veure en les figures, és possible que en alguns casos amb certs paràmetres no es detecten comunitats, i per tant no apareixen en les gràfiques. Això vol dir que no s'ha format cap *StableCore*, que és a causa d'agafar paràmetres ($\epsilon$-$\mu$-$\tau$) que no compleixen els requisits. Quan més grans són aquests paràmetres, més restrictiu és la forma de trobar comunitats.

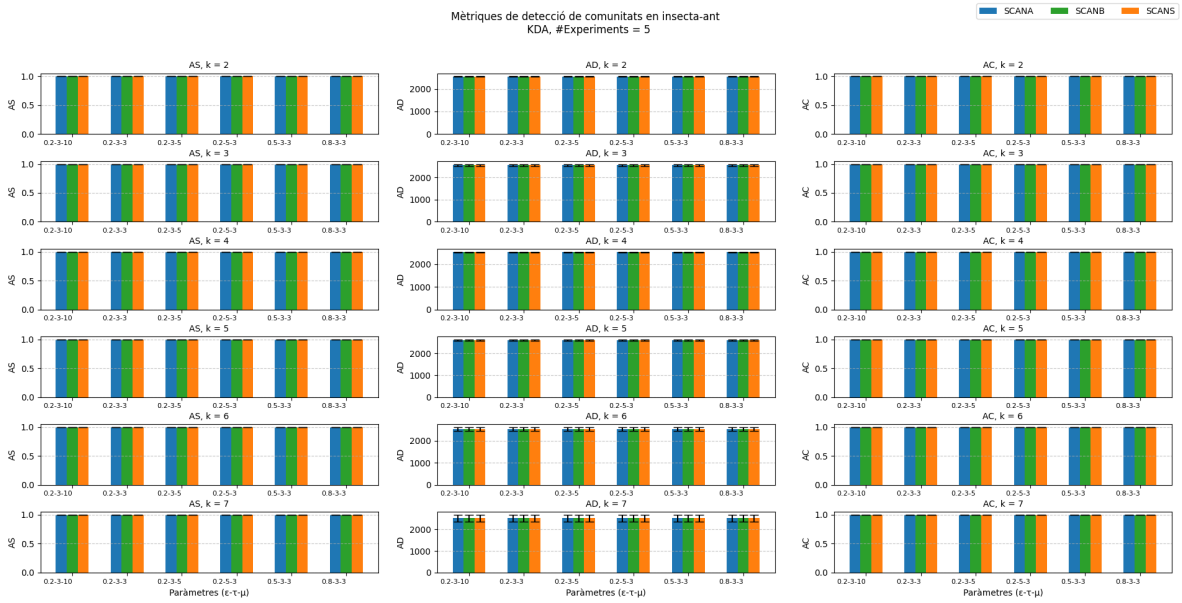


Figura 8: Mètriques de detecció de comunitats en el *dataset insecta-ant* utilitzant l'algorisme *KDA*. S'observen per cada paràmetre del algorisme *KDA*, els paràmetres ($\epsilon$-$\mu$-$\tau$) provats, i els resultats amb cada mètode de detecció.

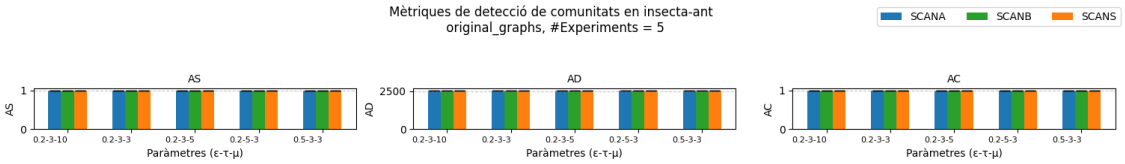


Figura 9: Mètriques de detecció de comunitats en el *dataset insecta-ant* en els seus grafs originals. Es pot observar que els valors no canvien gaire respecte a aplicar les mètriques en les dades protegides pel mètode *KDA*.

# 4 Conclusions provisionals

En aquest projecte s'ha investigat, dissenyat, implementat i analitzat dues tècniques de privacitat per a grafs: *Edge-Local Differential Privacy* i *K-Degree Anonymity*. Les metodologies proposades s'han aplicat amb èxit sobre diversos conjunts de dades, assolint els objectius principals i obtenint els resultats esperats.

Tanmateix, un dels objectius inicials (la integració dels grafs anonimitzats en una *Graph Neural Network*) es va haver de descartar per limitacions de temps. Aquest aspecte representa una línia clara de continuació del treball, amb l'objectiu de validar l'impacte de les tècniques de privacitat en tasques

d'aprenentatge automàtic.

A més, el projecte es podria ampliar explorant nous enfocaments de protecció de privacitat no tractats en aquest treball, com ara la incorporació de pesos a les arestes dels grafs, una característica especialment rellevant en escenaris com les xarxes de transaccions.

# Referències


[1] J. Leskovec, Stanford Network Analysis Project (SNAP). Disponible en: https://snap.stanford.edu/index.html [Darrer accés: 26-feb-2025].

[2] Ryan A. Rossi i Nesreen K. Ahmed, The Network Data Repository with Interactive Graph Analytics and Visualization, 2015. Disponible en: https://networkrepository.com/dynamic.php [Darrer accés: 26-feb-2025].

[3] L. Rossi, M. Musolesi i A. Torsello, "On the k-Anonymization of Time-Varying and Multi-Layer Social Graphs", Proceedings of the International AAAI Conference on Web and Social Media, 9(1), 377-386, 2021. Disponible en: https://ojs.aaai.org/index.php/ICWSM/article/view/14605 [Darrer accés: 26-feb-2025].

[4] S. Paul, J. Salas i V. Torra, "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, (2023, Agost).

[5] B. Ruan, J. Gan, H. Wu, i A. Wirth, "Dynamic Structural Clustering on Graphs", arXiv preprint arXiv:2108.11549, 2021. Disponible en: https://arxiv.org/pdf/2108.11549 [Darrer accés: 1-mar-2025].

[6] E. Castrillo, E. León, i J. Gómez, "Dynamic Structural Similarity on Graphs", arXiv preprint arXiv:1805.01419, 2018. Disponible en: https://arxiv.org/pdf/1805.01419 [Darrer accés: 1-mar-2025].

[7] B. Rozemberczki, Awesome Community Detection - Temporal Networks. GitHub. Disponible en: https://github.com/benedekrozemberczki/awesome-community-detection [Darrer accés: 26-feb-2025].

[8] "Havel–Hakimi algorithm", Wikipedia, l'enciclopèdia lliure. Disponible en: https://en.wikipedia.org/wiki/Havel–Hakimi_algorithm [Darrer accés: 13-abr-2025].

[9] "Erdős–Gallai theorem", Wikipedia, l'enciclopèdia lliure. Disponible en: https://en.wikipedia.org/wiki/Erdos–Gallai_theorem [Darrer accés: 14-abr-2025].

[10] D. Koutra, J. T. Vogelstein i C. Faloutsos, "DeltaCon: A Principled Massive-Graph Similarity Function with Attribution", SIAM International Conference on Data Mining (SDM), 2013. Disponible en: https://web.eecs.umich.edu/ dkoutra/papers/DeltaCon_KoutraVF_withAppendix.pdf. [Darrer accés: 19-abril-2025].

[11] H. Qin, R.-H. Li, G. Wang, X. Huang, Y. Yuan i J. X. Yu, "Mining Stable Communities in Temporal Networks by Density-Based Clustering", IEEE Transactions on Big Data, vol. 8, núm. 3, pp. 671–684, 1 juny 2022. Disponible en: https://doi.org/10.1109/TBDATA.2020.2974849. [Darrer accés: 4-maig-2025].