Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi
Afyon Kocatepe University Journal of Science and Engineering

AKÜ FEMÜBİD **23** (2023) 035102 (661-670) AKU J. Sci. Eng. **23** (2023) 035102 (661-670)
DOI: 10.35414/akufemubid.1149701

Araştırma Makalesi / Research Article

Performance Analysis of *K*-Degree Anonymization on Barabási-Albert Graph

Fatih SOYGAZİ[1], Damla OĞUZ[2*]

[1] *Aydın Adnan Menderes University, Faculty of Engineering, Department of Computer Engineering, Aydın.*
[2] *İzmir Institute of Technology, Faculty of Engineering, Department of Computer Engineering, İzmir.*

e-mail[1]: fatih.soygazi@adu.edu.tr *ORCID ID: http://orcid.org/0000-0001-8426-2283*
Corresponding author e-mail[2]: damlaoguz@iyte.edu.tr* *ORCID ID: http://orcid.org/0000-0001-6556-7444*

Geliş Tarihi: 27.07. 2022 Kabul Tarihi: 02.05.2023

Abstract

Anonymity is one the most important problems that emerged with the increasing number of graph-based social networks. It is not straightforward to ensure anonymity by adding or removing some nodes from the graph. Therefore, a more sophisticated approach is required. The consideration of the degree of the nodes in a graph may facilitate having knowledge about specific nodes. To handle this problem, one of the prominent solutions is *k*-degree anonymization where some nodes involving particular degree values are anonymized by masking its information from the attackers. Our objective is to evaluate the achievement of *k*-degree anonymization with a well-known graph structure, namely, Barabási-Albert graph, which is similar to the graphs on social networks. Hence, we generate multiple synthetic Barabási-Albert graphs and evaluate the *k*-degree anonymization performance on these graphs. According to experimental results, the success of *k*-degree anonymity approximately proportional to the number of edges or nodes.

***K*eywords**
Anonymization; *K*-Degree Anonymity; Barabási -Albert Graph; Social Networks; Knowledge Bases

Barabási-Albert Çizgesinde *K*-Derece Anonimleştirmenin Performans Analizi

Öz

Anonimlik, çizge tabanlı sosyal ağların sayısının artmasıyla ortaya çıkan en önemli sorunlardan biridir. Çizgeye bazı düğümler ekleyerek veya çıkararak anonimliği sağlamak kolay değildir. Bu nedenle, daha komplike bir yaklaşım gereklidir. Çizgenin yapısı veya çizgedeki düğümlerin derecesi, belirli düğümler hakkında bilgi sahibi olmayı kolaylaştırabilir. Bu sorun için öne çıkan çözümlerden biri olan *k*-derece anonimleştirme, belirli dereceleri içeren bazı düğümlerin bilgilerinin saldırganlardan gizlenerek anonimleştirilmesidir. Amacımız, sosyal ağlardaki çizgelere benzeyen Barabási-Albert çizgesi gibi iyi bilinen bir çizge yapısı ile *k*-derece anonimleştirmenin başarısını değerlendirmektir. Bu nedenle, birden çok sentetik Barabási-Albert çizgesi değerlendiriyoruz. Deneysel sonuçlara göre, *k*-derece anonimliğin başarısı, yaklaşık olarak kenar veya düğüm sayısı ile orantılıdır.

Anahtar kelimeler
Anonimleştirme; *K*-Derece Anonimlik, Barabási-Albert Çizgesi; Sosyal Ağlar; Bilgi Tabanları

1. Introduction

The immense data on social networks that has sharply increased in the last decade leads to anonymity problems and analyzing them helps attackers to infer knowledge about the identities of the users. The solution for the anonymity on social networks might be provided by graph-based anonymization approaches. In a social network, nodes are the individual identities that may describe some social entities, and the edges indicate the relationships between these nodes. The main question at this point is about the graph modification by applying a minimum number of operations when the identity of each graph element is kept anonymous.

There are three critical anonymity problems that need to be considered such as identity, link, and content disclosures in a social network. Identity disclosure is related to the identity of an individual

node. Link disclosure deals with the privacy of the relationships among the nodes. Content disclosure considers the data of the nodes that are transmitted between each node: like social media messaging between two individuals frequently. While different techniques propose solutions for each disclosure, our aim is to work on identity disclosure in this paper, namely *k*-degree anonymization (Liu and Terzi 2008).

The definition for *k*-degree anonymization is: "Given a graph *G* and an integer *k*, modify *G* via a set of edge-addition (or deletion) operations in order to construct a new *k*-degree anonymous graph *G*', in which every node v has the same degree with at least $k - 1$ other nodes." (Liu and Terzi 2008). *k*-degree anonymity aims to apply a minimum number of modifications to the graph. Hence, the general structure of the graph is preserved mostly, and the degree of anonymity is ensured at the same time.

The aim of this paper is to analyze the achievement of *k*-degree anonymity on social networks. Network topologies provide a way of structural understanding of a graph in a social network. Therefore, this structure may facilitate generating a simulated social network recognizing the real one. Network topologies can be classified into three categories: random graphs, scale-free and small-world networks (Albert and Barabási 2002). Social networks have similar properties with scale-free networks which follow the power law distribution. This distribution pertains to the network degree of the nodes with their relationships in social networks (Barabási 2016). In simple terms, the probability of making a connection with another node of a specific node increases proportionally with the degree of that node. There is an 80-20 rule between these nodes that denote that 80% of the nodes have a probability of 20% linking with the other nodes in the network (Barabási 2016). Hence, a new relationship between a new node and the existing nodes has higher linking probability for nodes who already have a high node degree compared to the nodes with low degree theoretically. Barabási and Albert (Barabási and Albert 1999), (Barabási et al. 1999) propose a well-known scale-free network, Barabási-Albert model and the generated graph from this model called Barábasi-Albert graph, that is appropriate for generation of a social network.

In this paper, we generate various numbers of Barabási-Albert graphs and apply *k*-degree anonymization on these graphs to assess identity disclosure performance by changing the number of nodes, edges, and *k* value as a parameter in *k*-degree anonymization. Hence, we discuss the success of *k*-degree anonymization for different configurations in social networks.

The rest of this paper is organized as follows: Section 2 explores the related work. Section 3 introduces the methodology used in this study. Section 4 presents the results and discussions on performance evaluation. Lastly, Section 5 concludes the paper.

2. Related Work

The increase of data especially on the Web has brought about a requirement to handle the identifiability of that data by attackers. Therefore, data anonymization has started to be worked especially on databases and the well-known anonymity technique named as *k*-anonymity is introduced when disclosing information (Samarati and Sweeney 1998b). Until the emergence of social networks, the studies about anonymization on tabular data have been popular (Samarati and Sweeney 1998a, Aggarwal *et al.* 2005, Bayardo and Agrawal 2005, Zhong *et al.* 2005, Ciriani *et al.* 2007). The common use of social networks has changed the focus from tabular data to graphs with respect to anonymization. Liu and Terzi (2008) propose *k*-degree anonymity to avoid disclosure of individual's identities in a graph by attackers. Their objective is to keep the identity of each individual anonymously by a graph-based approach. Hay *et al*. (2008) focus on the structural knowledge in the network and propose a model named *k*-candidate anonymity

with at least *k* candidate vertices. Their work aggregates the various network structures and generates a sampling model from these structures that facilitate graph anonymization. Narayanan and Shmatikov (2009) present a framework to obtain an anonymized social network graph. Their work on real time data in Twitter and this data can be re-identified with 12% error rate on Twitter graph with 224K nodes. Zou *et al*. (2009) focuses on the problem that the adversary can retain the information about the subgraphs linked to the target node. If a subgraph around a certain node in an anonymized graph is identified with high probability, the chance of identification for the target node also increases. Therefore, the authors have an objective to "construct a graph *G'* from the original graph *G* so that for any subgraph $X \subset G$, *G* contains at least *k* subgraphs isomorphic to *X"* (Zou *et al.* 2009). They also work on the information loss by modifying the original graph from *G* to *G'*. Accordingly, lower anonymization cost to measure the information loss indicates the number of fewer changes in the constructed graph or vice versa (Wu et al. 2010). Ying *et al.* (2009) compare the edge-based approach with *k*-degree anonymization schemes regarding utility and privacy risks. Casas-Roma *et al*. (2013, 2017) present a new algorithm for achieving *k*-degree anonymity on large networks with minimal edge modifications by utilizing univariate micro-aggregation. Lin and Liao (2015) propose a method for anonymizing social network data by modeling it as directed graphs with signed edge weights and developing a graph anonymization approach based on privacy and attack models. Additionally, a clustering algorithm for graphs is introduced, which groups similar nodes in the graph into clusters while ensuring a minimum cluster size constraints. Their proposed approach employs a relaxed-balance step to lower computational cost and space requirements for large and realistic datasets.

The Barabási-Albert model is a mathematical model that is widely used to study real-world networks. This model has been used in a wide range of fields to understand the behavior of real-world networks and has been shown to be a useful tool for predicting the behavior of these networks under different conditions. Türker and Sulak (2018) propose that the Twitter hashtag network and typical real networks exhibit power-law degree distributions, indicating that nodes tend to self-organize with preferential attachment mechanisms. They conduct a two-layer analysis of tag networks using Twitter entries data. They examine the intersection layer, consisting of edges present in both layers, and find that it more closely resembles the pure Barabási-Albert model. This similarity can be largely attributed to the semantically validated co-occurrence edges. Türker and Albayrak (2018) find that the most efficient data transfer rates are found in pure Barabási-Albert topology, where the time and number of nodes required for data transfer are minimized.

There are some recent studies (Rossi *et al.* 2015, Qian et al. 2016, Ma *et al.* 2017, Mohapatra and Patra 2017, Minello *et al.* 2020, Kiabod *et al.* 2019; 2021, Li *et al.* 2022) which focus on identity disclosure following *k*-degree anonymity to reduce the total running time or information loss.

To the best of our knowledge, there is not a comprehensive study which analyzes the impact of *k*-value, number of nodes and edges of *k*-degree anonymity separately in Barabási-Albert model graphs. In our paper, we analyze the *k*-degree anonymity (Liu and Terzi 2008) on simulated Barabási-Albert model graphs (Albert and Barabási 2002) by assessing with different parameters to comprehend the graph anonymity in various cases. These cases actually mimic the real social networks following scale-free property (Barabási 2016). Our research aims to provide an understanding of graph anonymization when facing different social networks with different node/edge combinations.

3. Methodology

In this section, first we provide the essential principles of *k*-degree anonymity (Liu and Terzi 2008) and Barabási-Albert graph (Barabási and Albert 1999), (Barabási et al. 1999) which are the constitutive elements of our proposal. Then, we present the application of *k*-degree anonymity in a widely used model that is appropriate for social networks, Barabási-Albert graph.

3.1 K-Degree Anonymity

As social media emerges and the private information of the people are easily accessible on the Web, the interlinked data facilitates accessing the information of the people. A fingerprint about a person caught in a social network even without the name or the surname might help traversing different data sources and obtaining a great amount of information. Although the explicit identifiers like name or mobile phone number can be encrypted to minimize the accessibility of those individuals, other jointly used properties (like birthdate, gender, and the city of birth), called quasi-identifiers, can cause the identification of them. Samarati and Sweeney (1998) propose that the generalization or suppression of each property is the way of anonymization to make it difficult for identification. For example, a postcode as 09100 that resembles the city and also the town information is hidden by defining as 09000. Hence the town information is kept secret (generalization). In another case, the date of birth for a person is changed from "1982" to "between 1980 and 1985" (suppression). Hence, a way of generalization or suppression for the common data obfuscates the information retrieval in the social network. The commonly used technique, namely *k*-anonymity (Ciriani *et al.* 2007, Samarati 2001, Samarati and Sweeney 1998a, Sweeney 2002), anonymizes the dataset where an individiual's information cannot be distinguished from at least *k*-1 individuals. While *k*-anonymity is mostly focused on tabular data, the social networks are an application area of graph data structure. Hence, a graph-based anonymization technique similar to *k*-anonymity is needed. Graph anonymization mainly focuses on masking the information of a node from the attackers. An attacker having some knowledge about a specific user in a social network facilitates revealing the information of that user. For example, if the number of connections of a user is unique in a social network, he/she might be easily identified. *k*-degree anonymity (Liu and Terzi 2008, Lu *et al.* 2012, Minello *et al.* 2020, Ren *et al.* 2014) is another technique to make this user (or the node) to anonymize the network in which at least *k*-1 nodes have the same properties. Hence, the number of edges of each node will be the same with at least *k*-1 nodes.

Liu and Terzi (2008) define the concept of the graph-anonymization problem. The problem involves operating a graph construction process on graph *G* to create a *k*-degree anonymous graph with the least possible modifications to the original graph. As an example, if there is just one person in the social network involving a unique number of friends such as 178, the identity disclosure of that person is obvious. Hence, the minimum number of graph-based modifications would resolve this situation.

Formally, let $G(V, E)$ be a simple graph; V is a set of nodes and E the set of edges in G. Given a graph $G(V, E)$ and an integer k (degree anonymity value), Liu and Terzi (2008) propose the modification of G via the minimum number of edge addition or deletion operations to construct a new graph $G'(V', E')$.

Definition 1. If every distinct value in a vector v appears at least k-times, v is called k-anonymous. For example, v = [7,7,7,4,4,4,4,3,3,3,3,2,2,2] is 3-anonymous.

Definition 2. For every node $v \in V$ there is at least k-1 other nodes that have the same degree. In that case graph G which involves the nodes V with k-anonymity property is a k-degree anonymous graph. Figure 1 represents sample *k*-degree anonymous graphs. Figure 1(a) is a 2-degree anonymous graph since there are two nodes with degree 1 and the

degree sequence of *G* is d_G = [1,1] accordingly. Figure 1(b) is a 4-degree anonymous graph since there are four nodes with degree 1 and the degree sequence of *G* is d_G = [1,1,1,1]. Similarly Figure 1(c) is also a 4-degree anonymous graph since there are four nodes with degree 2 and the degree sequence of *G* is d_G = [2,2,2,2].

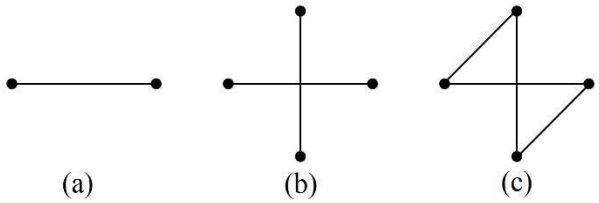

Figure 1. *K*-degree anonymous graph examples

Definition 3. The symmetric difference between two graphs *G*(*V*, *E*) and *G*′(*V*′, *E*′) is given in Equation (1). The symmetric difference between *G* and *G*′ must be minimal for *k*-degree anonymization. In simple terms, the minimum number of update operations must be applied on *G* to acquire *G*′.

$$SymmDiff(G, G') = (E' \setminus E) \cup (E \setminus E') \qquad (1)$$

Figure 2 shows a sample situation for symmetric difference between graphs. The blue lines in Figure 2(c) define the difference from the graph in Figure 2(a) to the graph in Figure 2(b). The pink lines represent the difference from the graph in Figure 2(b) to the graph in Figure 2(a). Then, the symmetric difference between the graphs is 7.

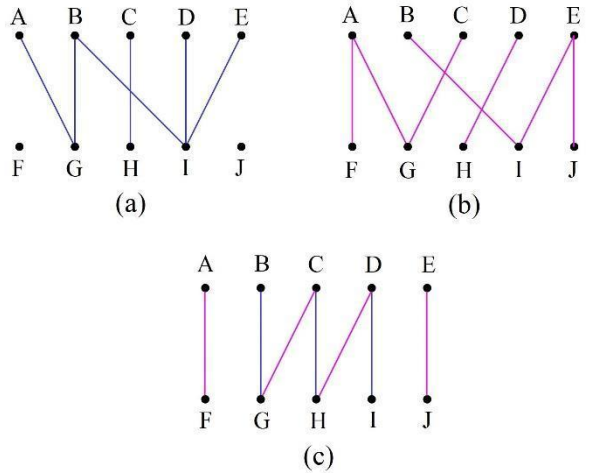

Figure 2. Symmetric difference between two graphs

From the perspective of *k*-degree anonymity, the modification of the original graph should bring about an anonymous graph with minimum number of operations. Figure 3 shows the *k*-degree anonymization process by checking symmetric difference. Adding one edge from *B* to *E* in Figure 3 anonymizes the initial graph. While the degree sequence of initial graph *G* is [2,1,1,1,1,1] and *A* node is susceptible for attacking, the anonymized graph *G*′ has the degree sequence [2,2,2,1,1] and it is a 2-degree anonymous graph after edge addition.

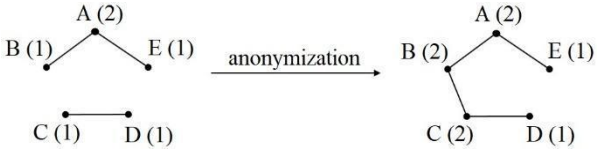

Figure 3. The 2-degree anonymization of a graph

3.2 Barabási-Albert Model

Barabási and Albert (1999) propose a prominent research generating the model to describe the scale free networks. A scale-free network is a network whose degree distribution follows a power law. The degree distribution of the number of edges per node is given in Equation (2) (Cohen *et al.* 2003) where λ is the exponent, it is frequently in the range 2 < λ < 3 and *c* is a proportionally constant normalization factor. Barabási-Albert model is an algorithm for generating scale-free networks like Figure 4(a) with the degree distribution shown in Figure 4(b).

$$P(k) = ck^{-\lambda} \qquad (2)$$

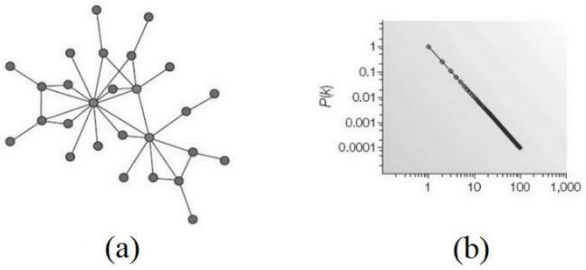

Figure 4. Scale-free network and its degree distribution (Rosato et al. 2008)

Barabási-Albert model has growth and preferential attachment which are the two important general concepts of this model. Both of these attachments are the terms widely appearing in real networks. Growth denotes the addition of new node(s) to the network at each time interval and consequently, defines the number of nodes. Preferential attachment refers to the tendency of a new node in a network to connect to a node that already has a large number of links, and the probability of a node receiving a new link is proportional to its degree. This is also known as the "rich get richer" phenomenon. For example, a newcomer in a social network mostly would like to become acquainted with a well-known person (node).

Barabási-Albert model has two parameters: *n*, which refers to the number of nodes in the graph, and *m*, which represents the number of edges in the graph that connect each new node to the existing nodes. Hence, when the total number of nodes in the network is *n*, the total number of links in the network can be calculates as $n\ x\ m$ [3]. Figure 5(a), (b) and (c) represent the Barabási-Albert model graph with 10 nodes with number of edges 1, 2 and 3 respectively.

The network is generated gradually by the addition of new nodes. Each node is inserted to the network one by one. The new node tends to connect with an existing node having more links. The probability p_i that the new node connected to the node *i* is given in Equation (3) (Albert and Barabási 2002) where k_i denotes the number of degree of node *i* and the sum describes the sum of all previously existing nodes *j* in the graph. According to Equation (3), the nodes around the center of the graph have more degree than the newly added nodes as shown in Figure 5(a), (b) and (c).

$$p_i = \frac{k_i}{\sum_j k_j} \tag{3}$$

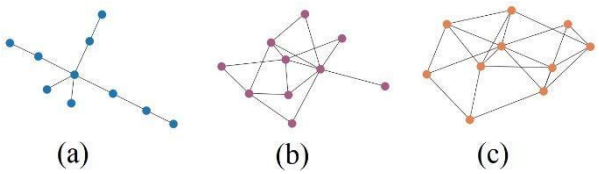

Figure 5. Barabási Albert Model Graph with various degrees

4. Evaluation

This section presents the evaluation results of *k*-degree anonymization on social networks. We generate synthetic social networks based on the Barabási-Albert model to evaluate anonymization performance with respect to various anonymization-based parameters. We use the *NetworkX* library in Python to create synthetic social networks using the Barabási-Albert model. We generate different graphs by changing the number of nodes and edges in a graph.[1] First, we aim to analyze the effect of the number of edges and nodes on the *k*-degree anonymity. Second, we aim to understand how the *k* value affects the success of *k*-degree anonymity on social networks. We use the percentage of edges overlap as the evaluation metric.

4.1 Impact of Number of Nodes and Edges

In this case we calculate the percentage of edges overlap for different edge numbers when the *k* value and the number of nodes are fixed. We conduct the experiments for two different numbers of nodes, and we compute 50 anonymized graphs for each experiment. Figure 6 shows the percentage of edges overlap when the *k* value is assigned to 5 and the number of nodes is assigned to 500 and 5000, respectively. Regardless of the number of nodes, the percentage of edges overlap increases as the number of edges increases. However, the percentage of edges overlap is ≈ 95% in the worst

[1]https://networkx.org/

case. That is, *k*-degree anonymity provides graph anonymization with high similarity to the original graph even when the number of edges is small. Furthermore, the success of *k*-degree anonymity increases as the number of nodes increases.

Figure 7 shows the percentage of edges overlap when the *k* value is set to 10 and the number of nodes is set to 500 and 5000, respectively. The success of *k*-degree anonymity increases as the number of edges increases for the both number of nodes. Although the behaviors of results of Figure 6 and Figure 7 are similar, the percentages of edges overlaps are slightly higher in Figure 6. In the generated social networks in Figure 6 and Figure 7, the number of edges is set to 5, 10, 25, 50 and 100 while the *k* value is fixed to 5 and 10, respectively. When the *k* value is 10, the anonymization work is a bit more complicated, and it slightly affects the success of edges overlap. However, even the lowest percentage of edges overlap is ≈ 91%.

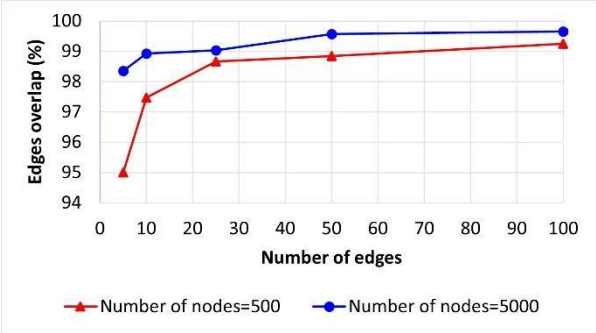

Figure 6. Impact of number of nodes and edges when *k* = 5

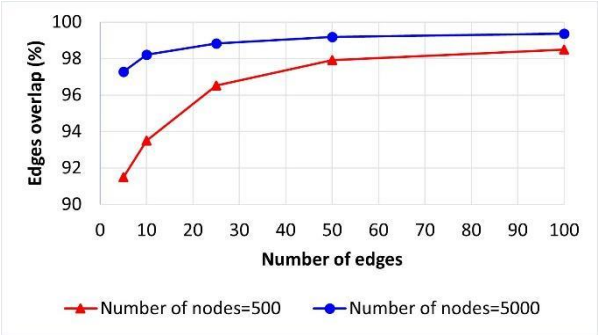

Figure 7. Impact of number of nodes and edges when *k* = 10

Based on the experiments presented in this section, we can conclude that the success of *k*-degree anonymity is slightly influenced by the number of nodes. As the number of nodes increases, the edges overlap increases on a small scale. For the same number of nodes, the success of *k*-degree anonymity increases as the increase in the number of edges.

4.2 Impact of the k Value

In Section 4.1, we have shown that the number of nodes slightly affects the success of *k*-degree anonymity, and we have noticed that the *k* value has an effect on the percentage of edges overlap. For this reason, in this case we fix the number of nodes and edges when the *k* value is changed to show the impact of the *k* value on the success of *k*-degree anonymity. In order to analyze different conditions we evaluate the percentage of edges overlap when the number of nodes and edges respectively i) 500 and 5, ii) 500 and 10, iii) 500 and 50, iv) 5000 and 5, v) 5000 and 10, and vi) 5000 and 50.

Figure 8 shows the percentage of edges overlap for the first three conditions. The increase in the *k* value decreases the success of *k*-degree anonymity since the approach should need to make more changes to provide the anonymization. On the other hand, the increase in the number of edges in the social network affects the success of *k*-degree anonymity positively. In other words, the flexibility of *k*-degree anonymity increases as the number of edges in the original network increases. Figure 9 shows the percentage of edges overlap for the remaining conditions - when there are exactly 5000 nodes.

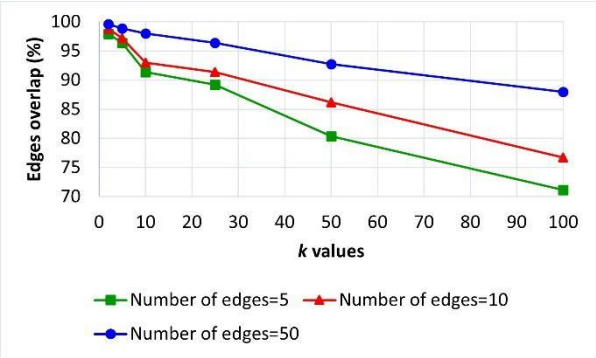

Figure 8. Impact of *k* value when number of nodes = 500

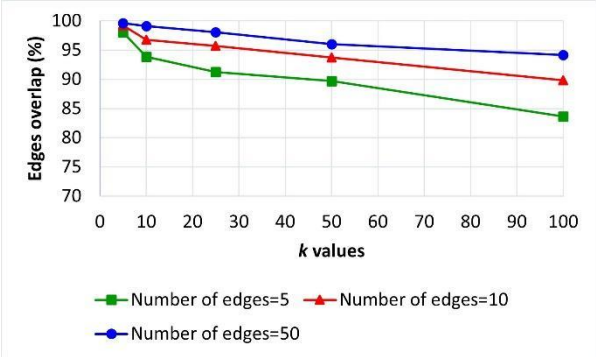

Figure 9. Impact of *k* value when number of nodes = 5000

According to the comparison of results in Figure 8 and Figure 9, the *k*-degree anonymity is more successful when the number of nodes is higher in the original social network because the approach is more flexible in a higher number of nodes for the same *k*-values.

5. Conclusion

In this paper, we focus on the anonymization of social networks and the efficiency of *k*-degree anonymization on various social networks based on the Barabási-Albert model. We evaluate the success of *k*-degree anonymity according to the percentage of edges overlap because it shows the percentage of preserved edges from the original graph. The results of the performance evaluation show the efficiency of *k*-degree anonymity for the Barabási-Albert graph, which is similar to the graphs on social networks. In conclusion, the success of *k*-degree anonymity increases proportionally with the number of nodes and edges independently. The success of *k*-degree anonymity decreases as the *k* value increases since more changes are needed to anonymize the original graph. However, *k*-degree anonymity is substantially successful at social network anonymization in high *k* values.

We are motivated to evaluate the achievement of *k*-degree anonymization with other graphs such as Erdős-Rényi graph and Watts-Strogatz graph, as they can provide insights into the effectiveness of this technique in various types of networks, including social networks.

6. References

Aggarwal, G., Feder, T., Kenthapadi, K., Motwani, R., Panigrahy, R., Thomas, D., and Zhu, A., 2005. Approximation algorithms for *k*-anonymity. *Journal of Privacy Technology (JOPT)*.

Albert, R. and Barabási, A. L., 2002. Statistical mechanics of complex networks. *Reviews of modern physics*, **74(1)**, 47.

Barabási, A. L. 2002. Linked: The New Science of Networks. Perseus Books Group.

Barabási, A. L. 2016. Network Science. Cambridge University Press, Cambridge.

Barabási, A. L. and Albert, R., 1999. Emergence of scaling in random networks. *Science,* **286(5439)**, 509-512.

Barabási, A. L., Albert, R., and Jeong, H. 1999. Mean-field theory for scale-free random networks. *Physica A: Statistical Mechanics and its Applications,* **272(1-2)**, 173-187.

Bayardo, R. J., and Agrawal, R. 2005. Data privacy through optimal *k*-anonymization. *In 21st International Conference on Data Engineering (ICDE'05)*, 217-228.

Casas-Roma, J., Herrera-Joancomartí, J., and Torra, V. 2013. An algorithm for *k*-degree anonymity on large networks. *In Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining,* 671-675.

Casas-Roma, J., Herrera-Joancomartí, J., and Torra, V. 2017. *k*-Degree anonymity and edge selection: ımproving data utility in large networks. *Knowledge and Information Systems*, **50**, 447-474.

Ciriani, V., Capitani di Vimercati, S. D., Foresti, S., and Samarati, P. 2007. "κ-anonymity", Secure Data Management in Decentralized Systems, 323-353.

Cohen, R., Rozenfeld, A. F., Schwartz, N., Ben-Avraham, D., and Havlin, S. 2003. Directed and non-directed scale-free networks. *Statistical Mechanics of Complex Networks,* 23-45.

Hay, M., Miklau, G., Jensen, D., Towsley, D., and Weis, P., 2008. Resisting structural re-identification in anonymized social networks. *Proceedings of the VLDB Endowment,* **1(1)**, 102-114.

Kiabod, M., Dehkordi, M. N., and Barekatain, B. 2019. TSRAM: A time-saving *k*-degree anonymization method in social network. *Expert Systems with Applications*, **125**, 378-396.

Kiabod, M., Dehkordi, M. N., and Barekatain, B., 2021. A fast graph modification method for social network anonymization. *Expert Systems with Applications*, **180**, 115-148.

Li, K., Tian, L., Zheng, X., and Hui, B., 2022. Plausible Heterogeneous Graph *k*-Anonymization for Social Networks. *Tsinghua Science and Technology*, **27(6)**, 912-924.

Lin, S. H., and Liao, M. H. 2016. Towards publishing social network data with graph anonymization. *Journal of Intelligent & Fuzzy Systems*, **30(1)**, 333-345.

Liu, K. and Terzi, E., 2008. Towards identity anonymization on graphs. *In Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data*, 93-106.

Lu, X., Song, Y., and Bressan, S. 2012. Fast identity anonymization on graphs. *In International Conference on Database and Expert Systems Applications*, 281-295.

Ma, J., Qiao, Y., Hu, G., Huang, Y., Sangaiah, A. K., Zhang, C., ... and Zhang, R., 2017. De-anonymizing social networks with random forest classifier. *IEEE Access*, **6**, 10139-10150.

Minello, G., Rossi, L., and Torsello, A. 2020. *k*-Anonymity on Graphs Using the Szemerédi Regularity Lemma. *IEEE Transactions on Network Science and Engineering*, **8(2)**, 1283-1292.

Mohapatra, D., and Patra, M. R. 2017. A level-cut heuristic-based clustering approach for social graph anonymization. *Social Network Analysis and Mining,* **7(1)**, 1-13.

Narayanan, A., and Shmatikov, V., 2009. De-anonymizing social networks. *In 2009 30th IEEE Symposium on Security and Privacy*, 173-187.

Qian, J., Li, X. Y., Zhang, C., and Chen, L., 2016. De-anonymizing social networks and inferring private attributes using knowledge graphs. *In IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications,* 1-9.

Ren, X. M., Jia, B. X., Wang, K. C., and Cheng, J. 2014. Research on *k*-anonymity privacy protection of social network. *Applied Mechanics and Materials*, **530**, 701-704.

Rosato, V., Meloni, S., Simonsen, I., Issacharoff, L., Peters, K., Festenberg, N. V., & Helbing, D. 2008. A complex system's view of critical infrastructures. Managing Complexity: Insights, Concepts, Applications, Springer, 241-260.

Rossi, L., Musolesi, M., and Torsello, A., 2015. On the *k*-anonymization of time-varying and multi-layer social graphs. *In Ninth International AAAI Conference on Web and Social Media (ICWSM 2015).*

Samarati, P., 2001. Protecting respondents identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering*, **13(6)**, 1010-1027.

Samarati, P., and Sweeney, L. 1998a. Protecting privacy when disclosing information: *k*-anonymity and its enforcement through generalization and suppression.

Samarati, P., and Sweeney, L. 1998b. Generalizing data to provide anonymity when disclosing information. *PODS*, **98(188)**.

Sweeney, L. 2002. *k*-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems,* **10(05)**, 557-570.

Türker, İ., and Sulak, E. E. 2018. A multilayer network analysis of hashtags in twitter via co-occurrence and semantic links. *International Journal of Modern Physics B*, **32(04)**, 1850029.

Wu, X., Ying, X., Liu, K., and Chen, L., 2010. A survey of privacy-preservation of graphs and social networks. *In Managing and Mining Graph Data,* Springer, 421-453.

Ying, X., Pan, K., Wu, X., & Guo, L. 2009. Comparisons of randomization and k-degree anonymization schemes for privacy preserving social network publishing. *In Proceedings of the 3rd workshop on social network mining and analysis* (pp. 1-10).

Zhong, S., Yang, Z., and Wright, R. N. 2005. Privacy-enhancing *k*-anonymization of customer data. *In Proceedings of the Twenty-Fourth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems,* 139-147.

Zou, L., Chen, L., & Özsu, M. T., 2009. K-automorphism: A general framework for privacy preserving network publication. *Proceedings of the VLDB Endowment*, **2(1)**, 946-957.