On analyzing and evaluating privacy measures for social networks under active attack

Bhaskar DasGupta[a,1,*], Nasim Mobasheri[a,1], Ismael G. Yero[b,2]

[a] *Department of Computer Science, University of Illinois at Chicago, Chicago, IL 60607, USA*

[b] *Departamento de Matemáticas, Escuela Politécnica Superior, Universidad de Cádiz, 11202 Algeciras, Spain*

Abstract

Widespread usage of complex interconnected social networks such as *Facebook*, *Twitter* and *LinkedIn* in modern internet era has also unfortunately opened the door for privacy violation of users of such networks by malicious entities. In this article we investigate, both theoretically and empirically, privacy violation measures of large networks under active attacks that was recently introduced in (*Information Sciences*, 328, 403–417, 2016). Our theoretical result indicates that the network manager responsible for prevention of privacy violation must be very careful in designing the network *if its topology does not contain a cycle*. Our empirical results shed light on privacy violation properties of eight real social networks as well as a large number of synthetic networks generated by both the classical Erdös-Rényi model and the scale-free random networks generated by the Barábasi-Albert preferential-attachment model.

Keywords: Privacy measure, social networks, active attack, empirical evaluation

2010 MSC: 68Q25, 68W25, 05C85

[*] Corresponding author

Email addresses: bdasgup@uic.edu (Bhaskar DasGupta), nmobas2@uic.edu (Nasim Mobasheri), ismael.gonzalez@uca.es (Ismael G. Yero)

[1] Research partially supported by NSF grant IIS-1160995.

[2] This research was done while the author was visiting the University of Illinois at Chicago, USA, supported by "Ministerio de Educación, Cultura y Deporte", Spain, under the "José Castillejo" program for young researchers (reference number: CAS15/00007)

1. Introduction

Due to a significant growth of applications of graph-theoretic methods to the field of social sciences in recent days, it is by now a standard practice to use the concepts and terminologies of network science to those social networks that focus on interconnections between people. However, social networks in general may represent much more than just networks of interconnections between people. Rapid evolution of popular social networks such as *Facebook*, *Twitter* and *LinkedIn* have rendered modern society heavily dependent on such virtual platforms for their day-to-day operation. The powers and implications of social network analysis are indeed *indisputable*; for example, such analysis may uncover previously unknown knowledge on community-based involvements, media usages and individual engagements. However, all these benefits are *not* necessarily cost-free since a malicious individual could compromise privacy of users of these social networks for harmful purposes that may result in the disclosure of sensitive data (attributes) that may be linked to its users, such as node degrees, inter-node distances or network connectivity. A natural way to avoid this consists of an "anonymization process" of the relevant social network in question. However, since such anonymization processes may *not* always succeed, an important research goal is to be able to quantify and measure how much privacy a given social network can achieve. Towards this goal, the recent work in [43] aimed at evaluating the *resistance* of a social network against active privacy-violating attacks by introducing and studying theoretically a new and meaningful privacy measure for social networks. This privacy measure arises from the concept of the so-called k-metric antidimension of graphs that we explain next.

Given a connected simple graph $G = (V, E)$, and an ordered sequence of nodes $S = (v_1, \dots, v_t)$, the *metric representation* of a node u that is *not* in S with respect to S is the vector (of t components) $\mathbf{d}_{u,-S} = (\text{dist}_{u,v_1}, \dots, \text{dist}_{u,v_t})$, where $\text{dist}_{u,v}$ represents the length of a shortest path between nodes u and v. The set S is then a k-*antiresolving set* if k is the largest positive integer such that for every node v not in S there also exist *at least* other $k-1$ different nodes $v_{j_1}, \ldots, v_{j_{k-1}}$ not in S such that $v, v_{j_1}, \ldots, v_{j_{k-1}}$ have the *same* metric representation with respect to S (*i.e.*, $\mathbf{d}_{v,-S} = \mathbf{d}_{v_{j_1},-S} = \cdots = \mathbf{d}_{v_{j_{k-1}},-S}$). The *$k$-metric antidimension* of G is defined to be value of the minimum cardinality among all the k-antiresolving sets of G [43]. If a set of attacker nodes S represents a k-antiresolving set in a graph G, then an adversary controlling the nodes in S cannot *uniquely* re-identify other nodes in the network (*based on the metric representation*) with probability higher than $^1/_k$. However, given that S is unknown, any privacy measure for a social network should quantify over *all* possible subsets S of nodes. *In this sense, a social network G meets (k,ℓ)-anonymity with respect to active attacks to its privacy if k is the smallest positive integer such that the k-metric antidimension of G is no more than ℓ. In this definition of (k,ℓ)-anonymity the parameter k is used for a privacy threshold, while the parameter ℓ represents an upper bound on the expected number of attacker nodes in the network.* Since attacker nodes are in general difficult to inject without being detected, the value ℓ could be estimated based on some statistical analysis of other known networks. A simple example that explains the role of k and ℓ to readers is as follows. Consider a complete network K_n on n nodes in which every node is connected with every other node. It is readily seen that for any $0 < \ell < n$, this network meets $(n-\ell,\ell)$-anonymity. In other words, this means that a social network K_n guarantees that a user cannot be re-identified (based on the metric representation) with a probability higher than $1/(n-\ell)$ by an adversary controlling at most ℓ attacker nodes. For other related concepts for metric dimension of graphs, the reader may consult references such as [14, 25, 30].

Chatterjee *et al.* in [9] (see also [49]) formalized and analyzed the computational complexities of several optimization problems motivated by the (k,ℓ)-anonymity of a network as described in [43]. In this article, we consider three of these optimization problems from [9], namely Problems 1–3 as defined in Section 2. A high-level itemized overview of the contribution of this article is as follows (see Section 3 for precise technical statements and details of all contributions):

- Our theoretical result concerning the anonymity issues for networks without cycles is provided in Theorem 1 in Section 3.1. Some consequences of this theorem are also discussed *immediately following a statement of the theorem.*

- In Section 3.2, we first describe briefly efficient implementations of the high-level algorithms of Chatterjee *et al.* [9] for Problems 1–3 (namely Algorithms I and II in Section 3.2.1). We then tabulate and discuss the results of applying these implemented algorithms for the following type of network data:

  - eight real social networks listed in Table 3 in Section 3.4.2,
  - the classical undirected Erdös-Rényi random networks $G(n, p)$ for four suitable combinations of n and p, and
  - the *scale-free random networks* $G(n, q)$ generated by the Barábasi-Albert *preferential-attachment* model for four suitable combinations of n and q.

  The 6 tables that provide tabulations of the empirical results are Tables 4–9 in Section 3.2 and the type of conclusions that one can draw from these tables are stated in the 11 conclusions numbered ①–⑪ in the same section. Despite our best efforts, we do not know of any other alternate approaches (*e.g.*, sybil attack framework) that will provide a significantly simpler theoretical framework to reach all the 11 conclusions as mentioned above.

As an illustration of a potential application, consider the *hub fingerprint query* model of Hey *et al.* [26]. Noting that the largest hub fingerprint for a target node u is the metric representation of u with respect to the hub nodes, results on (k, ℓ)-anonymity are directly applicable to this setting of Hey *et al.* [26] that models an adversary trying to identify the hub nodes in a network. For example, assuming that the quantity k_{opt} in Problem 1 (see Section 2 for a definition) is 10, the network is vulnerable with respect to hub identification in the model of Hey *et al.* in the sense that it is *not* possible to guarantee that an adversary will not be able to uniquely re-identify any node in the network with probability at most 0.1.

1.1. Some remarks regarding the model and our contribution (to avoid possible confusion)

To avoid any possible misgivings or confusions regarding the technical content of the paper as well as to help the reader towards understanding the remaining content of this article, we believe the following comments and explanations may be relevant.

- ▶ The computational complexity investigations in this paper has nothing to do with the model in the paper by Backstrom *et al.* [5]. We *whole-heartedly* and *without any reservations* agree that the paper by Backstrom *et al.* [5] is seminal, but the research investigations in this paper has nothing to do with the model or any measure introduced in the paper by Backstrom *et al.* [5]. The notion of active attack is very different in that paper, and therefore the computational problems that arise in that paper are very different from those in the current paper and in fact incomparable. Finally, the goal of this paper is not to compare various network privacy models but to investigate, theoretically and empirically, the model in [43].

- ▶ This paper does *not* introduce any new privacy model or measure, but simply investigates, both theoretically and empirically, computational problems for a model that is published in "*Information Sciences*, 328, 403–417, 2016" (reference [43]). There have been several other subsequent papers investigating this privacy measure, *e.g.*, see [9, 44, 49, 34]. Thus, researchers in network privacy are certainly interested in this model or related computational complexity questions. Of course, this does not contradict the fact that the paper by Backstrom *et al.* [5] is seminal.

► Even though the network privacy model was introduced in [43] and therefore the best option for clarification of any confusion regarding the model would be to look at that paper, we provide the following clarification just in case. In this model, nobody is trying to prevent adversaries. Informally, the privacy measure only gives a "measure" on how much secure a graph is against active attacks, *i.e.*, a probability with which we can assert that, if there are controlled nodes in a graph, then we can in some sense know which is the probability to be reidentified in such graph (for details please see the texts preceding and following the statements of Problems 1–3 in Section 2). No new nodes are added at all. This is not a problem that involves dynamic graphs. The model in [43] is not the same as the one by Backstrom *et al.* [5].

1.2. Comparison with other existing works

Model comparison Unfortunately, different models of network privacy have quite different objectives and consequently quite different measures that cannot in general be compared to one another. In particular, we know of no other different but comparable model or measure of network privacy that can be compared to those in our paper. For example, the network privacy model introduced by Backstrom *et al.* [5] is interesting, but the notion of active attack is very different in that paper, and therefore the computational problems that arise in that paper are very different from those in the current paper and in fact *incomparable.*

Algorithmic comparison Note that algorithms for different models *cannot* be compared in terms of their worst-case (or average-case) computational complexities. For example, consider the *scale-free network model* and the computational complexity paper for this model in [21]. Now, consider the *Erdös-Rényi random regular network* model, and consider the paper in [51]. Even though [51] provides better algorithmic results in terms of time-complexity and approximability, that does not nullify the research results in [21].

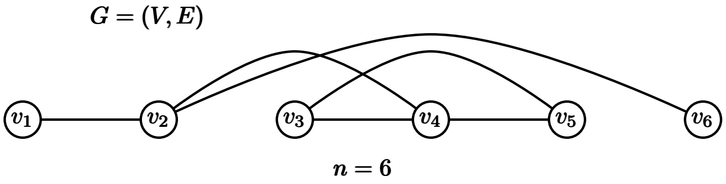
Privacy preservation in learning theoretic framework The recent surge in popularity of machine learning applications to different domains, specifically in the context of *deep learning* methods, has motivated many Internet companies to provide numerous online cloud-based services and frameworks for developing and deploying machine learning applications (Machine Learning as a Service or MLaaS) such as the Google Cloud ML Engine. Typically, an user (customer) of such a system first estimates the parameters of a suitable model by training the model with data and afterwards, once the correct model is determined, uploads the model to the cloud provider such that remote users can use the model. This type of service frameworks lead to two possible privacy concerns, the first concerning privacy violations of the training data, and the second concerning privacy violations of data uploaded by remote users. For some recent papers dealing with possible remedies of these privacy violations, such as introducing suitable random noises to perturb the data, see papers such as [40, 50]. However, these privacy concerns are quite different from the current topic of our paper, such as they are not specific to networks and they involve learning paradigms which are not of interest to this paper. Whether privacy questions in the MLaaS framework can be combined with those in this paper is an interesting research question but unfortunately beyond the scope of this paper.

2. Basic notations, relevant background and problem formulations

Let $G = (V, E)$ be the undirected input network over n nodes $v_1, \dots, v_n$. The authors in [9] formalized and analyzed the computational complexities of several optimization problems motivated by the (k, ℓ)-anonymity of a network as described in [43]. The notations and terminologies from [9] relevant for this paper are as follows (*see Fig 1 for an illustration*)[3]:

- ▶ $\mathbf{d}_{v_i} = (\text{dist}_{v_i,v_1}, \text{dist}_{v_i,v_2}, \dots, \text{dist}_{v_i,v_n})$ denotes the metric representation of a node v_i. For example, in Fig 1, $\mathbf{d}_{v_1} = (0, 1, 3, 2, 3, 2)$.

[3] The notations and the theoretical frameworks are actually *not* that complicated once one goes over them carefully. Although one may wonder if significantly simpler notations could have been adopted without neglecting the complexities of the frameworks, it does not seem to be possible in spite of our best efforts for over an year.



$\mathbf{dist}_{v_i,v_j}$ **values**

	v_1	v_2	v_3	v_4	v_5	v_6
v_1	0	1	3	2	3	2
v_2	1	0	2	1	2	1
v_3	3	2	0	1	1	3
v_4	2	1	1	0	1	2
v_5	3	2	1	1	0	3
v_6	2	1	3	2	3	0

Figure 1: An example for illustration of some basic definitions and notations in Section 2.

- ► $\mathsf{Nbr}\,(v_\ell) = \{\, v_j \mid \{v_\ell, v_j\} \in E \,\}$ is the (open) *neighborhood* of node v_ℓ in $G = (V, E)$. For example, in Fig 1, $\mathsf{Nbr}\,(v_2) = \{\, v_1, v_4, v_6 \,\}$.

- ► For a subset of nodes $V' = \{v_{j_1}, v_{j_2}, \ldots, v_{j_t}\} \subset V$ with $j_1 < j_2 < \cdots < j_t$ and any other node $v_i \in V \setminus V'$, $\mathbf{d}_{v_i,-V'} = \big(\mathrm{dist}_{v_i,v_{j_1}}, \mathrm{dist}_{v_i,v_{j_2}}, \ldots, \mathrm{dist}_{v_i,v_{j_t}}\big)$ denotes the metric representation of v_i with respect to V'. The notation is further generalized by defining $\mathcal{D}_{V'',-V'} = \{\, \mathbf{d}_{v_i,-V'} \,|\, v_i \in V'' \,\}$ for any $V'' \subseteq V \setminus V'$. For example, in Fig 1, $\mathbf{d}_{v_3,-\{v_1,v_5,v_6\}} = \big(\underset{v_1}{3}, \underset{v_5}{1}, \underset{v_6}{3}\big)$ and $\mathcal{D}_{\{v_2,v_3\},-\{v_1,v_5,v_6\}} = \big\{(\overbrace{\underset{v_1}{1}, \underset{v_5}{2}, \underset{v_6}{1}}^{\text{from } v_2}), (\overbrace{\underset{v_1}{3}, \underset{v_5}{1}, \underset{v_6}{3}}^{\text{from } v_3})\big\}$.

- ► A partition $\Pi' = \{V_1', V_2', \ldots, V_\ell'\}$ of $S' \subseteq V$ is called a *refinement* of a partition $\Pi = \{V_1, V_2, \ldots, V_k\}$ of $S \supseteq S'$, denoted by $\Pi' \prec_r \Pi$, provided Π' can be obtained from Π in the following manner:

  - ▷ For every node $v_i \in \big(\cup_{t=1}^{k} V_t\big) \setminus \big(\cup_{t=1}^{\ell} V_t'\big)$, remove v_i from the set in Π that contains it.
  - ▷ *Optionally*, for every set V_ℓ in Π, replace V_ℓ by a partition of V_ℓ.
  - ▷ Remove empty sets, if any.

  For example, for Fig 1, $\{\{v_2\}, \{v_3\}, \{v_4, v_5\}\} \prec_r \{\{v_1, v_2, v_3\}, \{v_4, v_5\}\}$.

► The following notations pertain to the equality relation (an equivalence relation) over the set of (same length) vectors $\mathcal{D}_{V\setminus V',-V'}$ for some $\emptyset \subset V' \subset V$:

- ▷ The set of equivalence classes, which forms a partition of $\mathcal{D}_{V\setminus V',-V'}$, is denoted by $\Pi^{=}_{V\setminus V',-V'}$. For example, in Fig 1, $\mathcal{D}_{\{v_2,v_3,v_4,v_5\},-\{v_1,v_6\}} = \big\{ (\overbrace{\underset{v_1}{1}, \underset{v_6}{1}}^{\text{from } v_2}), (\overbrace{\underset{v_1}{3}, \underset{v_6}{3}}^{\text{from } v_3}), (\overbrace{\underset{v_1}{2}, \underset{v_6}{2}}^{\text{from } v_4}), (\overbrace{\underset{v_1}{3}, \underset{v_6}{3}}^{\text{from } v_5}) \big\}$ and $\Pi^{=}_{\{v_2,v_3,v_4,v_5\},-\{v_1,v_6\}} = \Big\{ \big\{ (\overbrace{\underset{v_1}{1}, \underset{v_6}{1}}^{\text{from } v_2}) \big\}, \big\{ (\overbrace{\underset{v_1}{2}, \underset{v_6}{2}}^{\text{from } v_4}) \big\}, \big\{ (\overbrace{\underset{v_1}{3}, \underset{v_6}{3}}^{\text{from } v_3}), (\overbrace{\underset{v_1}{3}, \underset{v_6}{3}}^{\text{from } v_5}) \big\} \Big\}$.
- ▷ Abusing terminologies slightly, two nodes $v_i, v_j \in V \setminus V'$ will be said to belong to the *same* equivalence class if $\mathbf{d}_{v_i,-V'}$ and $\mathbf{d}_{v_j,-V'}$ belong to the same equivalence class in $\Pi^{=}_{V\setminus V',-V'}$, and thus $\Pi^{=}_{V\setminus V',-V'}$ also defines a partition into equivalence classes of $V \setminus V'$. For example, in Fig 1, v_3 and v_5 belong to the same equivalence class in $\Pi^{=}_{\{v_2,v_3,v_4,v_5\},-\{v_1,v_6\}}$ and $\Pi^{=}_{\{v_2,v_3,v_4,v_5\},-\{v_1,v_6\}}$ also defines the partition $\big\{\{v_2\},\{v_4\},\{v_3,v_5\}\big\}$.
- ▷ The *measure* of the equivalence relation is defined as $\mu\left(\mathcal{D}_{V\setminus V',-V'}\right) \overset{\text{def}}{=} \min_{\mathcal{Y}\in\Pi^{=}_{V\setminus V',-V'}} \big\{ \, |\mathcal{Y}| \, \big\}$. Thus, if a set S is a k-antiresolving set, then $\mathcal{D}_{V\setminus S,-S}$ defines a partition into equivalence classes whose measure is k. For example, in Fig 1, $\mu\left(\Pi^{=}_{\{v_2,v_3,v_4,v_5\},-\{v_1,v_6\}}\right) = 1$.

By using the terminologies mentioned above, the following three optimization problems were formalized and studied in [9]. *We need to stress that one really needs to study the three different problems and consequently the three objectives (namely, k_{opt}, $\mathcal{L}^{\geq k}_{\text{opt}}$ and $\mathcal{L}^{=k}_{\text{opt}}$) separately because they are motivated by different considerations as explained before and after the problem definitions and as stated in ($\star$), ($\bowtie$) and (♠). Informally and briefly, Problem 1 and k_{opt} are used to provide an absolute privacy violation bound assuming the attacker can control as many nodes as it needs, restricting the number of attacker nodes employed by the adversary leads to Problem 2, and Problem 3 is motivated by a type of trade-off question between (k,ℓ)-anonymity vs. (k',ℓ')-anonymity. Thus, it is simply not possible to combine them into fewer than three problems.*

Problem 1 (metric anti-dimension or ADIM**).** *Find a subset of nodes V' such that* $k_{\text{opt}} = \mu\left(\mathcal{D}_{V\setminus V',-V'}\right) = \max\limits_{\emptyset\subset S\subset V}\left\{\, \mu\left(\mathcal{D}_{V\setminus S,-S}\right)\,\right\}$.

A solution of Problem 1 asserts the following:

($\star$) Assuming that there is *no* restriction on the number of nodes that can be controlled by an adversary, the following statements hold:

- ***(a)*** The network administrator *cannot* guarantee that an adversary will not be able to uniquely re-identify any node in the network (based on the metric representation) with probability $1/k_{\text{opt}}$ or less.
- ***(b)*** It *is* possible for an adversary to uniquely re-identify k_{opt} nodes in the network (based on the metric representation) with probability $1/k_{\text{opt}}$.

Thus, informally, Problem 1 and k_{opt} give an absolute privacy violation bound assuming the attacker can control as many nodes as it needs. In practice, however, the number of attacker nodes employed by the adversary *may* be restricted. This leads us to Problem 2.

Problem 2 ($k_{\geq}$-metric anti-dimension or ADIM$_{\geq k}$**).** *Given a positive integer k, find a subset $V_{\text{opt}}^{\geq k}$ of nodes of* minimum *cardinality* $\mathcal{L}_{\text{opt}}^{\geq k} = \left|V_{\text{opt}}^{\geq k}\right|$, *if one such subset at all exists, such that* $\mu\big(\mathcal{D}_{V\setminus V_{\text{opt}}^{\geq k},-V_{\text{opt}}^{\geq k}}\big) \geq k$.

Similar to ($\star$), a solution of Problem 2 (if it exists) asserts the following:

($\bowtie$) Assuming that an adversary may control up to α nodes, the following statements hold:

- ***(a)*** If $\alpha < \mathcal{L}_{\text{opt}}^{\geq k}$ then the network administrator *can* guarantee that an adversary will not be able to uniquely re-identify any node in the network (based on the metric representation) with probability $1/k$ or less.

- ***(b)*** If $\alpha \geq \mathcal{L}_{\rm opt}^{\geq k}$ then the network administrator *cannot* guarantee that an adversary will not be able to uniquely re-identify any node in the network (based on the metric representation) with probability $1/k$ or less.
- ***(c)*** If $\alpha \geq \mathcal{L}_{\rm opt}^{\geq k}$ then it *is* possible for an adversary to uniquely re-identify a subset of β nodes in the network (based on the metric representation) with probability $1/\beta$ for some $\beta \geq k$ (note that β may be much larger compared to k).

The remaining third problem is motivated by the following trade-off question between (k,ℓ)-anonymity vs. (k',ℓ')-anonymity: if $k' > k$ but $\ell' < \ell$ then (k',ℓ')-anonymity has *smaller* privacy violation probability $1/k' < 1/k$ compared to (k,ℓ)-anonymity but can only tolerate attack on *fewer* $\ell' < \ell$ number of nodes.

Problem 3 ($k_=$-metric antidimension or ADIM$_{=k}$**).** *Given a positive integer k, find a subset $V_{\rm opt}^{=k}$ of nodes of* minimum *cardinality $\mathcal{L}_{\rm opt}^{=k} = \left|V_{\rm opt}^{=k}\right|$, if one such subset at all exists, such that $\mu\big(\mathcal{D}_{V\setminus V_{\rm opt}^{=k},-V_{\rm opt}^{=k}}\big) = k$.*

One can describe assertions to a solution of Problem 2 (if it exists) in a manner similar to that in ($\star$) and ($\bowtie$). Chatterjee *et al.* in [9] studied the computational complexity aspects of Problems 1–3. They provided efficient (polynomial-time) algorithms to solve Problems 1 and 2 and showed that Problem 3 is *provably* computationally hard for exact solution but admits an efficient approximation for the particular case of $k = 1$ (see Algorithm II). Since we use this approximation algorithm for $k = 1$, we explicitly state below the implication of a solution of ADIM$_{=1}$ (note that a solution of ADIM$_{=1}$ always exists and $\mathcal{L}_{\rm opt}^{=1}$ is trivially at most $n-1$):

- **(♠)** It suffices for an adversary to control a *suitable* subset of $\mathcal{L}_{\rm opt}^{=1}$ nodes in the network to *uniquely* re-identify at least one node in the network (based on the metric representation) with *absolute certainty* (*i.e.*, with a probability of one).

3. Our theoretical and empirical results

3.1. Theoretical result

Suppose that a given graph G is a "k'-metric antidimensional" graph, *i.e.*, k' is the largest positive integer such that G has *at least* one k'-antiresolving set. Then obviously G does *not* contain any k''-antiresolving set for every $k'' > k'$. In contrast, it is not *a priori* clear if G contains k-metric antiresolving sets for any $k < k'$. For instance, a complete graph K_n on n nodes is $(n-1)$-metric antidimensional and moreover, for every $1 \leq k \leq n-1$, there exists a set of nodes in K_n which is a k-antiresolving set. *Au contraire*, if we consider the wheel graph $W_{1,n}$ (see Fig 2 for an illustration for $n = 16$), it is easy to see that the central node v_n is the *unique* n-antiresolving set, 1-antiresolving and 2-antiresolving sets exist, 3-antiresolving sets also exist (if n is larger than 5), but *no* k-antiresolving set exists for $4 \leq k \leq n-1$. This motivates the following research question:

> *For a given class of k'-metric antidimensional networks, can we decide if they also have k-antiresolving sets for all $1 \leq k \leq k'-1$?*

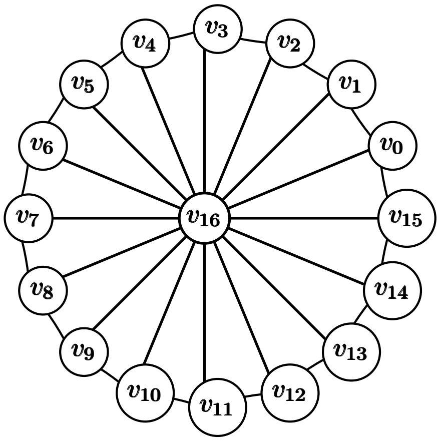


Figure 2: The wheel graph $W_{1,n}$ for $n = 16$.

The following theorem answers the question affirmatively for all networks without a cycle.

Theorem 1. *If T is a k'-metric antidimensional tree, then for every $1 \leq k \leq k'$ there exists a k-antiresolving set for T.*

Some consequences of Theorem 1

Some consequences of the above result in relation to the (k, ℓ)-anonymity measure are as follows. Note that what is stated below is *not* the same as the observations in [34].

Clearly, since trees have nodes of degree one (called leaves), it is always possible to identify at least one node of the tree [34]. However, if the network manager introduces some "fake" nodes as leaves, then this advantage for the adversary is avoided. In this sense, the result above asserts that an adversary will never be sure that the set of nodes which it could control will always identify at least one node of the given tree. Another related interesting observation is that for this to happen, the tree must be k-metric antidimensional for some $k \geq 2$, otherwise the tree is *completely insecure*. A characterization of that trees which are 1-metric antidimensional (graphs that contain only 1-antiresolving sets) was given in [44].

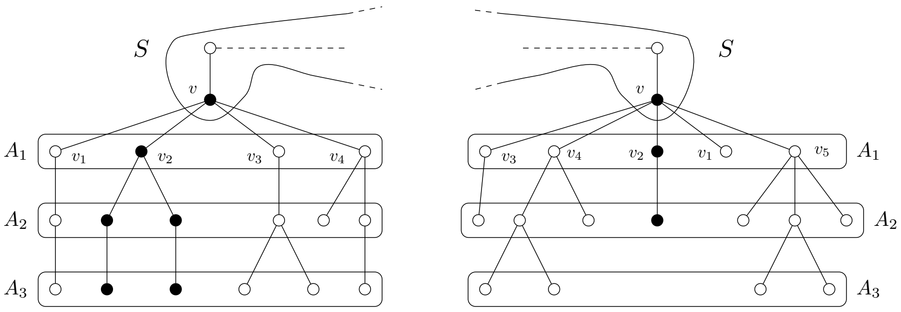
Note that in the above we claim nothing about what happens if the network does contain a cycle, or how a network manager can break cycles in a network. Note that the topology need not be "fully" controlled by a network manager, but can be influenced by adding extra nodes.

Proof of Theorem 1

We will use the following result from [44] in our proof.

Lemma 2.[44] *Any k-antiresolving set S in a tree T with $k \geq 2$ induces a connected subgraph of T.*

Since Problem 1 was shown to be solvable in polynomial time in [9], we may assume that we know the value k' for which the tree T is k'-metric antidimensional. If $k = 1$ or $k = k'$ then a k-antiresolving set for T clearly exists. We may also assume $k > 1$, since otherwise our result follows trivially. Suppose that $k = k' - 1$ and let S be a k'-antiresolving set of minimum cardinality for T. By Lemma 2, S induces a connected subgraph of T. Moreover, according to the definition of a k-antiresolving set, there exists an equivalence class $Q \in \Pi^{=}_{V \setminus S, -S}$ such that $|Q| = k'$. Select $v \in S$ such that $\mathsf{Nbr}(v) \setminus S \neq \emptyset$ and let $v_1, v_2, \ldots, v_r \in \mathsf{Nbr}(v) \setminus S$ for some $r \geq 1$. Clearly, the set $A_1 = \{v_1, v_2, \ldots, v_r\}$ forms an equivalence class of $\Pi^{=}_{V \setminus S, -S}$. Moreover, the set $A_2 = \bigcup_{i=1}^{r} \mathsf{Nbr}(v_i) \setminus \{v\}$, if not empty, also forms an equivalence class of $\Pi^{=}_{V \setminus S, -S}$. Fig 3 shows two examples which are useful to clarify all the notations of this proof (recall that the *eccentricity* of a node v is the maximum over the set of distances between v to all other nodes in the graph).



(I)

(II)

Figure 3: Two auxiliary trees. Notice that eccentricity of v in the subtrees is three in both cases. The set S is a 4-antiresolving set. The nodes of the subtree T_2 are shown in bold in both trees.

Assume that T is rooted at node v and, for every $v_i \in A_1$, let T_i be the subtree of T with node set $V(T_i)$ formed by v, v_i, and the set of descendants of v_i. Let e_i be the eccentricity of v in T_i for $1 \leq i \leq r$. Moreover, let A_j be the subset of nodes x in $\bigcup_{i=1}^{r} V(T_i)$ such that $\text{dist}_{v,x} = j$ for every $1 \leq j \leq \max\{e_i : 1 \leq i \leq r\}$. Observe that each A_j, with $1 \leq j \leq \max\{e_i : 1 \leq i \leq r\}$, is an equivalence class of $\Pi^{=}_{V \setminus S, -S}$ and thus, $|A_j| \geq k'$ since otherwise S is *not* a k'-antiresolving set. Moreover, without loss of generality, we can assume there exists a set A_q such that $|A_q| = k'$ (*e.g.*, in Fig 3 the sets A_1 and A_4). If there is no such set, then we choose another node v' of T for which this situation happen. If there is no such node v' at all, then the cardinality of every equivalence class of $\Pi^{=}_{V\setminus S,-S}$ is *strictly* larger than k', which contradicts the definition of a k'-antiresolving set. We now consider the following situations.

Case 1: $e_1 = e_2 = \cdots = e_r$ (*e.g.*, in Fig 3 (I) all the eccentricities are equal to 3). Notice that in this case $A_j \cap V(T_i) \neq \emptyset$ for every $1 \leq j \leq \max\{e_i : 1 \leq i \leq r\}$ and every $1 \leq i \leq r$. Moreover, there exist α, β such that $|A_\alpha \cap V(T_\beta)| = 1$ (*e.g.*, in Fig 3 (I) $\alpha = 1$ and β can take any value between 1 and 4). Thus, for the set $S' = S \cup V(T_\beta)$ it follows that $A_\alpha \setminus V(T_\beta)$ is an equivalence class of the equivalence relation $\Pi^{=}_{V\setminus S',-S'}$ and $|A_\alpha - V(T_\beta)| = k' - 1$. Moreover, for every other equivalence class X of $\Pi^{=}_{V\setminus S',-S'}$ it follows $|X| \geq k' - 1 = k$. Thus, X is a $(k'-1)$-antiresolving set. Clearly, X could not be of minimum cardinality.

Case 2: There are at least two subtrees T_i and T_j such that $e_i \neq e_j$. Without loss of generality, assume that $e_1 \leq e_2 \leq \cdots \leq e_r$. As in Case 1, there exist γ such that $|A_\gamma| = k'$ (*e.g.*, in Fig 3 (II) $\alpha = 3$). Let $S_1 = S \cup V(T_1)$ (note that T_1 is the subtree in which v has the minimum eccentricity). If $|A^{(1)}_j| \geq k'$ for every $A^{(1)}_j = A_j \setminus V(T_1)$ with $1 \leq j \leq e_1$, then $\gamma > e_1$ and thus S_1 is *also* a k'-antiresolving set. Hence, we consider $S_2 = S_1 \cup V(T_2)$ (note that T_2 is the subtree in which v has the second minimum eccentricity). If $|A^{(2)}_j| \geq k'$ for every $A^{(2)}_j = A^{(1)}_j \setminus V(T_2)$ with $1 \leq j \leq e_2$, then $\gamma > e_2$. Repeating this procedure, we shall find a set $S_q = S_{q-1} \cup V(T_q)$ such that $\gamma \leq e_q$ and moreover, $|A_{\alpha'} \cap V(T_{\beta'})| = 1$ for some $1 \leq \alpha' \leq e_r$ and $q \leq \beta' \leq r$. Thus, the set $A^{(q+1)}_j = A^{(q)}_j \setminus V(T_{q+1})$ satisfies $|A^{(q)}_j| = k' - 1$ and consequently $S_{q+1} = S_q \cup V(T_{q+1})$ is a $(k'-1)$-antiresolving set (*e.g.*, in Fig 3 (II) the process must be done two times, first we remove the nodes in the set $V(T_1) \setminus \{v\}$ and next we remove the nodes in the set $V(T_2) \setminus \{v\}$, thereby getting the required $(k'-1)$-antiresolving set).

Thus, in both cases we obtain a $(k'-1)$-antiresolving set. By using the same procedure and a $(k'-1)$-antiresolving set of minimum cardinality, we can find a $(k'-2)$-antiresolving set and in general a k-antiresolving set for every

$2 \leq k \leq k' - 1$, which completes the proof.

3.2. Empirical results

We remind the readers about the assertions in ($\star$), ($\bowtie$) and ($\spadesuit$) while we report our empirical results and related conclusions.

3.2.1. Algorithms for Problems 1–3 (Algorithms I and II)

We obtain an exact solution for Problem 2 by implementing the following algorithm (Algorithm I) devised in [9] by Chatterjee *et al.*. In this algorithm, an absence of a valid solution is indicated by $\mathcal{L}_{\text{opt}}^{\geq k} \leftarrow \infty$ and $V_{\text{opt}}^{\geq k} \leftarrow \emptyset$.

```
(* Algorithm I *)
1.      Compute $\mathbf{d}_{v_i}$ for all $i = 1, \ldots, n$ using any algorithm that solves
            all-pairs-shortest-path problem [12].
2.      $\widehat{\mathcal{L}_{\text{opt}}^{\geq k}} \leftarrow \infty$ ; $\widehat{V_{\text{opt}}^{\geq k}} \leftarrow \emptyset$
3.      for each $v_i \in V$ do
3.1         $V' = \{v_i\}$ ; done $\leftarrow$ FALSE
3.2         while $\big( (V \setminus V' \neq \emptyset)$ AND (NOT done) $\big)$ do
3.2.1           compute $\mu\left(\mathcal{D}_{V \setminus V', -V'}\right)$
3.2.2           if $\Big( \big( \mu\left(\mathcal{D}_{V \setminus V', -V'}\right) \geq k \big)$ and $\big( |V'| < \widehat{\mathcal{L}_{\text{opt}}^{\geq k}} \big) \Big)$
3.2.3               then    $\widehat{\mathcal{L}_{\text{opt}}^{\geq k}} \leftarrow |V'|$ ; $\widehat{V_{\text{opt}}^{\geq k}} \leftarrow V'$ ; done $\leftarrow$ TRUE
3.2.4               else    let $V_1, V_2, \ldots, V_\ell$ be the only $\ell > 0$ equivalence classes
                                in $\Pi^{\equiv}_{V \setminus V', -V'}$ such that
                                $|V_1| = \cdots = |V_\ell| = \mu\left(\mathcal{D}_{V \setminus V', -V'}\right)$
3.2.5                       $V' \leftarrow V' \cup \left( \cup_{t=1}^{\ell} V_t \right)$
4.      return $\widehat{\mathcal{L}_{\text{opt}}^{\geq k}}$ and $\widehat{V_{\text{opt}}^{\geq k}}$ as our solution
```

We obtain exact solutions for Problem 1 and find k_{opt} by using Algorithm I and doing a binary search for the parameter k over the range $\{1, 2, \ldots, n\}$ to find the largest k such that $V_{\text{opt}}^{\geq k} \neq \emptyset$. This requires using Algorithm I $O(\log n)$ times.

Although $\textsc{Adim}_{=k}$ is NP-hard for almost all k, for $k = 1$ we implement the following logarithmic-approximation algorithm devised in [9] by Chatterjee *et al.* for $\textsc{Adim}_{=1}$ computing $\mathcal{L}_{\mathrm{opt}}^{=1}$ and $V_{\mathrm{opt}}^{=1}$.

```
(* Algorithm II *)
1.  Compute $\mathbf{d}_{v_i}$ for all $i = 1, \ldots, n$ using any algorithm that solves
        all-pairs-shortest-path problem [12].
2.  $\widehat{\mathcal{L}_{\mathrm{opt}}^{=1}} \leftarrow \infty$ ; $\widehat{V_{\mathrm{opt}}^{=1}} \leftarrow \emptyset$
3.  for each node $v_i \in V$ do
    3.1  create the following instance of the set-cover problem [28]
         containing $n-1$ elements and $n-1$ sets:
           $\mathcal{U} = \left\{ a_{v_j} \,|\, v_j \in V \setminus \{v_i\} \right\}$,
           $S_{v_j} = \left\{ a_{v_j} \right\} \cup \left\{ a_{v_\ell} | \mathrm{dist}_{v_i,v_j} \neq \mathrm{dist}_{v_\ell,v_j} \right\}$ for $j \in \{1, \ldots, n\} \setminus \{i\}$
    3.2  if $\cup_{j \in \{1,\ldots,n\} \setminus \{i\}} S_{v_j} = \mathcal{U}$ then
         3.2.1  run the algorithm of Johnson in [28] for this instance of
                    set-cover giving a solution $\mathcal{I} \subseteq \{1, \ldots, n\} \setminus \{i\}$
         3.2.2  $V' = \{ v_j \,|\, j \in \mathcal{I} \}$
         3.2.3  if $\left( |V'| < \widehat{\mathcal{L}_{\mathrm{opt}}^{=1}} \right)$ then $\widehat{\mathcal{L}_{\mathrm{opt}}^{=1}} \leftarrow |V'|$ ; $\widehat{V_{\mathrm{opt}}^{=1}} \leftarrow V'$
4.  return $\widehat{\mathcal{L}_{\mathrm{opt}}^{=1}}$ and $\widehat{V_{\mathrm{opt}}^{=1}}$ as our solution
```

3.3. Run-time analyses and implementations of Algorithms I and II

Both Algorithm I and Algorithm II use the all-pairs-shortest-path ($\textsc{Apsp}$) computation, and this is the step that dominates the theoretical worst-case running time of both the algorithms. The following algorithmic approaches are possible for the all-pairs-shortest-path step:

- For the classical Floyd-Warshall algorithm for $\textsc{Apsp}$ [12], the theoretical worst-case running time of is $O(n^3)$ when n is the number of nodes in the network. In practice, for larger networks the running time of the Floyd-Warshall algorithm for $\textsc{Apsp}$ can often be improved by using algorithmic engineering tricks such as early termination criteria that are known in the algorithms community.

For our networks, we found the Floyd-Warshall algorithm with appropriate data structures and algorithmic engineering techniques to be sufficient; one reason for this could be that most of our networks, like many other real-world networks, have a small diameter and thus some computational steps in the Floyd-Warshall algorithm can often be skipped (the diameter of a network can be computed in worst-case $o(n^3)$ time [47] and in just $O(m)$ time in practice for many real-world networks [13]).

- Repeatedly running *breadth-first-search* [12] from each node gives a solution of APSP with a worst-case running time of $O(mn)$, which is better than $O(n^3)$ if $m = o(n^2)$, *i.e.*, the network is sparse.

- For specific types of networks, practitioners also consider using other algorithmic approaches, such as repeated use of Dijkstra's single-source shortest path or Johnson's algorithm [12], if they are run faster. Both these algorithms have a worst-case running time of $O(n^2 \log n + nm)$ where m is the number of edges, and therefore run faster than Floyd-Warshall algorithm in the worst case if $m = o(n^2)$.

- Using graph compression techniques, it is possible to design a $O(n^3/\log n)$ worst-case time algorithm for APSP [16].

- Using fast matrix multiplication algorithms, APSP can be solved in $O(n^{2.376})$ time [19, 20, 41] using Coppersmith and Winograd's matrix multiplication result [11].

For increasing the efficiency and speed of the algorithms we used various data structures such as *STL nested maps* and *vectors* to improve comparisons and lookup operations. Furthermore, for Algorithm I, we prematurely terminate the algorithm if $|V_{\mathrm{opt}}|$ reaches 1 as 1 is the smallest value of the size of attacker nodes.

Finally, just like the measures in this article, the APSP computation is *unavoidable* for a large variety of other geodesic-based network properties that are often used for real networks such as the *betweenness centrality*, *closeness centrality* or *Gromov-hyperbolicity* measure, and there is a vast amount of literature that apply such measures to large networks (*e.g.*, see [7, 46, 3, 35, 36, 27]).

3.4. Scalability of the privacy measure with respect to the size of network

We have tested computation of the privacy measures for graphs up to 1000 nodes. For Algorithm I, we found that the running time for computing the measure for an individual network ranges from 1 minute or less (for smaller sparser networks) to about 10 to 20 minutes (for larger denser networks). For Algorithm-II the running time was mostly in the order of a few minutes.

However, for much larger networks than what has been used in this paper, we would recommend a more careful implementation, specially for Algorithm I, to achieve a more time efficient implementation. Towards this goal, we provide the following suggestions in relation to computing the measures for larger networks:

- For larger networks, it would be advisable to use the fastest possible implementation of the all-pairs-shortest-paths algorithm. This is a well-known problem that admits a variety of algorithms some of which are especially more efficient on non-dense networks and moreover in practice the running times of many of these algorithms can be significantly improved by using several algorithmic engineering tricks (early termination criteria, efficient data structures etc.) that are known in the algorithmic implementation community. Also, if the same network is used for more than one privacy measure computation, it is certainly advisable to store the all-pairs-shortest-path data and re-use them instead of computing them afresh every time.

- Although our simulation did not need it, for larger networks the relevant set operations needed in Algorithms I and II can be implemented more efficiently, for example using the well-known data structures for disjoint sets (*e.g.*, see [18] for a survey).

- For extremely large networks, say dense networks containing millions of nodes, it may be advisable to use a suitable sampling method such as in [31] to sample appropriate sub-graphs of smaller size, and use the measures computed on these sub-graphs to statistically estimate the value of the measures on the entire graph.

3.4.1. Synthetic networks: models and algorithmic generations

Unfortunately, there is no *single universally agreed upon synthetic network model that faithfully reproduces all networks in various application domains (e.g., see [42, 29, 1]). In fact, there are some results that cast doubt if a true generative network model can even be known unambiguously.* Thus, it is very customary in the network research community to draw conclusions of the following type:

> "For those real-world networks generated by such-and-such model,
> we can conclude that ......"

We use two major types of synthetic networks, namely the *Erdös-Rényi random networks* and the *scale-free random networks* generated by the Barábasi-Albert *preferential-attachment* model [6]. Although the Erdös-Rényi network model has been used by prior network researchers as a real-network model in several application domains (*e.g.*, see [39, 17, 33, 8]) it is also known that this particular model is probably not very good a model for real networks in many other application domains. Thus, we also consider networks generated by the scale-free random network model which is more widely considered to be a real-network model in many network applications (*e.g.*, see [6, 4, 10, 45, 2]).

Erdös-Rényi model This is the classical undirected Erdös-Rényi model $G(n, p)$, where n is the number of nodes and every possible edge in the network is selected independently with a probability of p. The average degree of any node in $G(n, p)$ is $(n-1)p \approx np$, leading to $\frac{n(n-1)p}{2} \approx \frac{n^2 p}{2}$ as the average number of edges in the network. Our privacy measures assume that the given graph is connected since one connected component has no influence on the privacy of another connected component. Thus, it is imperative to select only those combinations of n and p that keeps the graph connected by keeping the average degree of every node to be at least 1. However, we actually need to make sure that the average degree is *at least* 2 since, for example, $\mathcal{L}_{\text{opt}}^{=1}$ is trivially equal to 1 otherwise. This implies that at the very least we must ensure that $(n-1)p \geq 2$, or *roughly* $np \geq 2$. However, in practice, while generating the actual random networks one may need to select a p that is slightly higher (**in our case,** $np \geq 2.5$). Note that the giant-component formation in ER networks happens around $np \approx 1$, so we are indeed further away from this phenomenon where slight variations in p cause abrupt changes in topological behavior of the network. We used the following four combinations of n and p to generate our synthetic networks to capture a smaller average degree of 2.5, a modest average degree of 5 and a larger average degree of 10:

$$\begin{array}{rcl} n & = & 500 \\ p & = & 0.005 \\ np & = & 2.5 \end{array} \qquad \begin{array}{rcl} n & = & 500 \\ p & = & 0.01 \\ np & = & 5 \end{array} \qquad \begin{array}{rcl} n & = & 1000 \\ p & = & 0.005 \\ np & = & 5 \end{array} \qquad \begin{array}{rcl} n & = & 1000 \\ p & = & 0.01 \\ np & = & 10 \end{array}$$

For $n = 500$ (respectively, for $n = 1000$) we generated 1000 random networks (respectively, 100 random networks) for each corresponding value of p, and then calculated relevant statistics using Algorithms I and II.

Scale-free model We use the Barábasi-Albert *preferential-attachment* model [6] to generate random scale-free networks. The algorithm for generating a random scale-free $G(n, q)$,where n is number of nodes and $q \ll n$ is the number of connections each new node makes, is as follows:

- Initialize G to have q nodes and *no* edges. Add these nodes to a "*list of repeated nodes*".
- Repeat the following steps till G has n nodes:

- Randomly select q distinct nodes, say $u_1, \ldots, u_q$, from the *list of repeated nodes*.
- Add a new node w and undirected edges $\{w, u_1\}, \ldots, \{w, u_q\}$ in G.
- Add w and $u_1, \ldots, u_q$ to the current *list of repeated nodes*.

The larger the q is, the more dense is the network $G(n, q)$. We used the following four combinations of n and q to generate our synthetic scale-free networks:

$$\begin{array}{lllllllllllll} n & = & 500 & \quad & n & = & 500 & \quad & n & = & 1000 & \quad & n & = & 1000 \\ q & = & 5 & & q & = & 10 & & q & = & 5 & & q & = & 10 \end{array}$$

For $n = 500$ (respectively, for $n = 1000$) we generated 1000 random networks (respectively, 100 random networks) for each corresponding value of q, and then calculated relevant statistics using Algorithms I and II.

3.4.2. Real networks

Table 3 shows the list of eight well-known unweighted social networks that we investigated. All the networks except one were undirected; for the only directed *UC Irvine College Message platform* network, we ignored the direction of edges. For each network the *largest* connected component was selected and tested.

3.4.3. Results for real networks in Table 3

Results for Adim **and** Adim$_{\geq k}$ Table 4 shows the results for Adim via applying Algorithm I to these networks. From these results we may conclude:

① For all networks *except* the "Enron Email Data" network, an attacker needs to control *only one* suitable node of the network to uniquely re-identify (based on the metric representation) a significant percentage of nodes in the network (ranging from 2.6% of nodes for the "University Rovira i Virgili emails" network to 26.5% of nodes for the "Zachary Karate Club" network).

Table 3: List of real social networks studied in this paper.

Name	**# of**		**Description**
	nodes	**edges**	
(A) Zachary Karate Club [48]	34	78	Network of friendships between 34 members of a karate club at a US university in the 1970s
(B) San Juan Community [32]	75	144	Network for visiting relations between families living in farms in the neighborhood San Juan Sur, Costa Rica, 1948
(C) Jazz Musician Network [22]	198	2842	A social network of Jazz musicians
(D) University Rovira i Virgili emails [23]	1133	10903	the network of e-mail interchanges between members of the University Rovira i Virgili
(E) Enron Email Data set [15]	1088	1767	Enron email network
(F) Email Eu core [37]	986	24989	Emails from a large European research institution
(G) UC Irvine College Message platform [38]	1896	59835	Messages on a Facebook-like platform at UC-Irvine
(H) Hamsterster friendships [24]	1788	12476	This Network contains friendships between users of the website `hamsterster.com`

② For all networks *except* the "Enron Email Data" network, the minimum privacy violation probability guarantee is significantly further from zero (ranging from 0.019 for the "UC Irvine College Message platform" network to 0.25 for the "Hamsterster friendships" network). The minimum privacy violation probability guarantee for the "Hamsterster friendships" network is significantly higher than all other networks.

③ The "Zachary Karate Club" and the "San Juan Community" networks are *more* vulnerable to privacy attacks in terms of the percentage of nodes in the networks whose privacy can be violated by the adversary.

Table 4: Results for ADIM using Algorithm I. n is the number of nodes and k_{opt} is the largest value of k such that $V_{\text{opt}}^{\geq k} \neq \emptyset$ (*cf.* Problem 1).

Name	n	k_{opt}	$p_{\text{opt}} = {}^{1}/_{k_{\text{opt}}}$	$\mathcal{L}_{\text{opt}}^{\geq k_{\text{opt}}} = \mathcal{L}_{\text{opt}}^{=k_{\text{opt}}}$	$\frac{k_{\text{opt}}}{n}$
(A) Zachary Karate Club	34	9	0.111	1	26.5%
(B) San Juan Community	75	7	0.143	1	9.3%
(C) Jazz Musician Network	198	12	0.084	1	6.0%
(D) University Rovira i Virgili emails	1133	29	0.035	1	2.6%
(E) Enron Email Data set	1088	153	0.007	935	14.1%
(F) Email Eu core	986	39	0.026	1	3.4%
(G) UC Irvine College Message platform	1896	55	0.019	1	2.9%
(H) Hamsterster friendships	1788	4	0.25	1	0.22%

For the "Enron Email Data" network, $\mathcal{L}_{\text{opt}}^{\geq k_{\text{opt}}} = 935$ implies that even to achieve a modest value of $p_{\text{opt}} = 0.007$ an adversary needs to control a large percentage (at least $\frac{935 \times 100}{1088}\% \approx 86\%$) of its nodes, a possibility unlikely to happen in practice. Thus, we continue further investigation about this network to check if a value of k *somewhat* smaller than k_{opt} may allow a *sufficiently steep* decline in the number of nodes that the attacker need to control, and report the values of $\mathcal{L}_{\text{opt}}^{\geq k}$ corresponding to relevant values of $k > 1$ in Table 5. As can be seen, the values of $\mathcal{L}_{\text{opt}}^{\geq k}$ does not decline unless k is really further away from k_{opt}, leading us to conclude the following:

> ④ For the "Enron Email Data" network, privacy violation of a large number of nodes of the network by an attacker cannot be guaranteed in a *practical* sense (*i.e.*, without gaining control of a large number of nodes).

Results for ADIM$_{=1}$ Algorithm II returns $\mathcal{L}_{\text{opt}}^{=1} = 1$ for all of our networks except the "Hamsterster friendships" network. For the "Hamsterster friendships" network, Algorithm II returns $\mathcal{L}_{\text{opt}}^{=1} = 2$. Thus, we conclude:

Table 5: Values of $\mathcal{L}_{\text{opt}}^{\geq k}$ corresponding to values for $k > 1$ for "Enron Email Data" network. Only those values of $k > 1$ for which $\mathcal{L}_{\text{opt}}^{\geq k} \neq \mathcal{L}_{\text{opt}}^{\geq k-1}$ are shown.

(E) Enron Email Data set	k	4	5	10	20	40	60	100	120	153
	$p_k = 1/k$	0.25	0.2	0.1	0.05	0.025	0.017	0.01	0.009	0.007
	$\mathcal{L}_{\text{opt}}^{\geq k}$	1	334	463	567	683	842	935	935	935

⑤ For all the real networks except the "Hamsterster friendships" network, an adversary controlling *just one* suitable node may uniquely re-identify (based on the metric representation) one other node in the network with certainty (*i.e.*, with a probability of 1). For the "Hamsterster friendships" network, the same conclusion holds provided the adversary controls two suitable nodes.

3.4.4. Results for Erdös-Rényi synthetic networks

Results for $\textsc{Adim}_{\geq k}$ Table 6 shows the results for $\textsc{Adim}_{\geq k}$ via applying Algorithm I to these networks. From these results we may conclude:

⑥ For *most* synthetic Erdös-Rényi networks, k_{opt} is a value that is *much smaller* compared to the number of nodes n. Thus, for our synthetic Erdös-Rényi networks, with high probability privacy violation of a large number of nodes of the network by an attacker *cannot* be achieved.

⑦ The values of $\frac{k_{\text{opt}}}{n}$ for denser Erdös-Rényi networks (corresponding to $p = 0.01$) is about 75% higher that those for sparser Erdös-Rényi networks (corresponding to $p = 0.005$) irrespective of the number of nodes. Thus, we conclude that our sparser synthetic Erdös-Rényi networks are more privacy-secure compared to their denser counter-parts.

Results for $\textsc{Adim}_{=1}$ Table 7 shows the result of our experiments of computation

Table 6: Results for $\text{ADIM}_{\geq k}$ using Algorithm I for classical Erdös-Rényi model $G(n,p)$. k_{opt} is the largest value of k such that $V^{\geq k}_{\text{opt}} \neq \emptyset$ (cf. Problem 1). The %-values indicate the percentage of the generated networks for those particular values of k_{opt} (*e.g.*, for $n = 500$ and $p = 0.005$, 980 out of the 1000 networks have $k_{\text{opt}} \geq 5$).

Network parameters										
n	p									
500	0.005	k_{opt}	≥ 4	≥ 5	≥ 6	≥ 7	≥ 8	≥ 9	≥ 10	> 10
		$p_{\text{opt}} = {}^{1}/{k_{\text{opt}}}$	≤ 0.25	≤ 0.2	≤ 0.166	≤ 0.142	≤ 0.125	≤ 0.111	≤ 0.1	< 0.1
		% of networks	100%	98%	81.8%	54.6%	21.5%	8%	3%	1%
			At least 90% of networks have $k_{\text{opt}} \leq 8$ and $\frac{k_{\text{opt}}}{n} \leq 0.016$							
500	0.010	k_{opt}	≥ 9	≥ 10	≥ 11	≥ 12	≥ 13	≥ 14	≥ 15	> 15
		$p_{\text{opt}} = {}^{1}/{k_{\text{opt}}}$	≤ 0.11	≤ 0.1	≤ 0.09	≤ 0.083	≤ 0.077	≤ 0.071	≤ 0.066	< 0.066
		% of networks	100%	98%	94%	81.4%	49.4%	21.4%	6.8%	0.6%
			At least 90% of networks have $k_{\text{opt}} \leq 14$ and $\frac{k_{\text{opt}}}{n} \leq 0.028$							
1000	0.005	k_{opt}	≥ 10	≥ 11	≥ 12	≥ 13	≥ 14	> 14		
		$p_{\text{opt}} = {}^{1}/{k_{\text{opt}}}$	≤ 0.1	≤ 0.09	≤ 0.083	≤ 0.077	≤ 0.071	< 0.066		
		% of networks	100%	99%	65%	16%	7%	1%		
			At least 90% of networks have $k_{\text{opt}} \leq 13$ and $\frac{k_{\text{opt}}}{n} \leq 0.013$							
1000	0.010	k_{opt}	≥ 18	≥ 19	≥ 20	≥ 21	≥ 22	≥ 23	≥ 24	> 24
		$p_{\text{opt}} = {}^{1}/{k_{\text{opt}}}$	≤ 0.055	≤ 0.052	≤ 0.05	≤ 0.047	≤ 0.045	≤ 0.043	≤ 0.041	< 0.041
		% of networks	100%	99%	90%	75%	47%	26%	9%	1%
			At least 90% of networks have $k_{\text{opt}} \leq 23$ and $\frac{k_{\text{opt}}}{n} \leq 0.023$							

of $\mathcal{L}^{=1}_{\text{opt}}$ using Algorithm II. From these results, we conclude:

⑧ For our synthetic Erdös-Rényi networks, with high probability an adversary controlling *at most two* nodes may uniquely re-identify (based on the metric representation) *at least* one other node in the network.

Table 7: Results for $\text{Adim}_{=1}$ using Algorithm II for classical Erdös-Rényi model $G(n, p)$. The %-values indicate the percentage of the generated networks that have the corresponding value of $\mathcal{L}^{=1}_{\text{opt}}$ (*e.g.*, for $n = 500$ and $p = 0.01$, 920 out of the 1000 networks have $\mathcal{L}^{=1}_{\text{opt}} = 1$).

Network parameters		$\mathcal{L}^{=1}_{\text{opt}}$		
n	p	1	2	> 2
500	0.01	92%	7%	1%
500	0.005	5.9%	89.3%	4.8%
1000	0.01	8%	90%	2%
1000	0.005	5%	93%	1%

3.4.5. Results for scale-free synthetic networks

Results for $\text{Adim}_{\geq k}$ Table 8 shows the results for $\text{Adim}_{\geq k}$ via applying Algorithm I to these networks. From these results we may conclude:

⑨ The value of k_{opt} relative to the size n of the network is much larger for synthetic scale-free networks compared to those for the synthetic Erdös-Rényi networks. Thus, compared to synthetic Erdös-Rényi networks, synthetic scale-free networks may allow privacy violation of a larger number of nodes of the network by an attacker.

⑩ Unlike the synthetic Erdös-Rényi networks, the values of $\frac{k_{\text{opt}}}{n}$ for denser scale-free networks (corresponding to $q = 10$) may be smaller or larger than those for sparser scale-free networks (corresponding to $q = 5$). Thus, density of scale-free networks does not seem to be well-correlated to privacy-security of these networks.

Results for $\text{Adim}_{=1}$ Table 9 shows the result of our experiments of computation of $\mathcal{L}^{=1}_{\text{opt}}$ using Algorithm II. From these results, we conclude:

⑪ Similar to synthetic synthetic Erdös-Rényi networks, for synthetic scale-free networks also with high probability an adversary controlling *at most two* nodes may uniquely re-identify

Table 8: Results for $\textsc{Adim}_{\geq k}$ using Algorithm I for the Barábasi-Albert preferential-attachment scale-free model $G(n,q)$. $k_{\rm opt}$ is the largest value of k such that $V_{\rm opt}^{\geq k} \neq \emptyset$ (cf. Problem 1). The %-values indicate the percentage of the generated networks for those particular values of $k_{\rm opt}$ (*e.g.*, for $n = 500$ and $q = 5$, 990 out of the 1000 networks have $k_{\rm opt} \geq 50$).

Network parameters										
n	q									
500	5	$k_{\rm opt}$	≥ 49	≥ 50	≥ 55	≥ 60	≥ 65	≥ 70	> 70	
		$p_{\rm opt} = {}^1\!/_{k_{\rm opt}}$	≤ 0.0204	≤ 0.02	≤ 0.018	≤ 0.016	≤ 0.015	≤ 0.014	< 0.014	
		% of networks	100%	99%	97%	89%	42%	10%	6%	
		At least 90% of networks have $k_{\rm opt} \leq 65$ and $\frac{k_{\rm opt}}{n} \leq 0.13$								
500	10	$k_{\rm opt}$	≥ 45	≥ 60	≥ 80	≥ 100	≥ 120	≥ 140	> 140	
		$p_{\rm opt} = {}^1\!/_{k_{\rm opt}}$	≤ 0.022	≤ 0.016	≤ 0.0125	≤ 0.001	≤ 0.008	≤ 0.007	< 0.007	
		% of networks	100%	50%	48%	47%	27%	5%	4%	
		At least 95% of networks have $k_{\rm opt} \leq 120$ and $\frac{k_{\rm opt}}{n} \leq 0.24$								
1000	5	$k_{\rm opt}$	≥ 88	≥ 90	≥ 100	≥ 110	≥ 120	≥ 130	≥ 135	
		$p_{\rm opt} = {}^1\!/_{k_{\rm opt}}$	≤ 0.011	≤ 0.010	≤ 0.001	≤ 0.009	≤ 0.008	≤ 0.007	≤ 0.0074	
		% of networks	100%	98%	94%	66%	32%	11%	1%	
		At least 89% of networks have $k_{\rm opt} \leq 120$ and $\frac{k_{\rm opt}}{n} \leq 0.12$								
1000	10	$k_{\rm opt}$	≥ 86	≥ 88	≥ 90	≥ 92	≥ 94	≥ 96	≥ 98	> 100
		$p_{\rm opt} = {}^1\!/_{k_{\rm opt}}$	≤ 0.0116	≤ 0.0113	≤ 0.0111	≤ 0.0108	≤ 0.0106	≤ 0.0104	≤ 0.0102	< 0.001
		% of networks	100%	77%	67%	56%	43%	30%	13%	3%
		At least 87% of networks have $k_{\rm opt} \leq 96$ and $\frac{k_{\rm opt}}{n} \leq 0.096$								

(based on the metric representation) *at least* one other node in the network.

4. Conclusion

Rapid evolution of popular social networks such as Facebook and Twitter have rendered modern society heavily dependent on such virtual platforms for their day-to-day operation. However, the many benefits accrued by such online

Table 9: Results for Adim$_{=1}$ using Algorithm II for the Barábasi-Albert preferential-attachment scale-free model $G(n, q)$. The %-values indicate the percentage of the generated networks that have the corresponding value of $\mathcal{L}_{\text{opt}}^{=1}$ (*e.g.*, for $n = 500$ and $q = 5$, 990 out of the 1000 networks have $\mathcal{L}_{\text{opt}}^{=1} = 2$).

Network parameters		$\mathcal{L}_{\text{opt}}^{=1}$	
n	q	2	> 2
500	5	99%	1%
500	10	99.5%	0.5%
1000	5	99%	1%
1000	10	99%	1%

networked systems are not necessarily cost-free since a malicious entity may compromise privacy of users of these social networks for harmful purposes that may result in the disclosure of sensitive attributes of these networks. In this article, we investigated, both theoretically and empirically, quantifications of privacy violation measures of large networks under active attacks. Our theoretical result indicates that the network manager responsible for prevention of privacy violation must be very careful in designing the network if its topology does not contain a cycle, while our empirical results shed light on privacy violation properties of eight real social networks as well as synthetic networks generated by the classical Erdö-Rènyi model. We believe that our results will stimulate much needed further research on quantifying and computing privacy measures for networks.

5. Acknowledgements

We thank the anonymous reviewers for their helpful comments. B.D. and N.M. thankfully acknowledges partially support from NSF grant IIS-1160995. This research was partially done while I.G.Y. was visiting the University of Illinois at Chicago, USA, supported by "Ministerio de Educación, Cultura y Deporte", Spain, under the "José Castillejo" program for young researchers (reference number: CAS15/00007).

References

[1] Y. Achiam, I. Yahav and D. G. Schwartz, *Why not scale free? Simulating company ego networks on Twitter*. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, San Francisco, CA, 174-177, 2016.

[2] R. Albert and A. L. Barabási, *Statistical mechanics of complex networks.* Reviews of Modern Physics, 74(1), 47-97, 2002.

[3] R. Albert, B. DasGupta and N. Mobasheri, *Topological implications of negative curvature for biological and social networks.* Physical Review E, 89(3), 032811, 2014.

[4] H. Amini, R. Cont and A. Minca, *Resilience to contagion in financial networks.* Mathematical Finance, 26(2), 329-365, 2016.

[5] L. Backstrom, C. Dwork and J. Kleinberg, *Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography.* Proc. 16th International Conference on World Wide Web, 181-190, New York, NY, USA, 2007.

[6] A. L. Barábasi and R. Albert, *Emergence of scaling in random networks.* Science, 286, 509-512, 1999.

[7] C. Biscaro and C. Giupponi, *Co-Authorship and Bibliographic Coupling Network Effects on Citations.* PLoS ONE 9(6): e99502, 2014.

[8] D. S. Callaway, M. E. J. Newman, S. H. Strogatz and D. J. Watts, *Network robustness and fragility: percolation on random graphs.* Physical Review Letters, 85, 5468-5471, 2000.

[9] T. Chatterjee, B. DasGupta, N. Mobasheri, V. Srinivasan and I. G. Yero, *On the computational complexities of three privacy measures for large networks under active attack.* arXiv:1607.01438 [cs.CC], 2016.

[10] R. Cont, A. Moussa and E. B. Santos, *Network Structure and Systemic Risk in Banking Systems*. In J. Fouque and J. Langsam (Eds.), Handbook on Systemic Risk, Cambridge University Press, 327-368, 2013.

[11] D. Coppersmith and S. Winograd, *Matrix multiplication via arithmetic progressions*. Journal of Symbolic Computation, 9, 251-280, 1990.

[12] T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, *Introduction to algorithms*. The MIT Press, 2001.

[13] P. Crescenzi, R. Grossi, M. Habib, L. Lanzi and A. Marino, *On computing the diameter of real-world undirected graphs*. Theoretical Computer Science, 514, 84-95, 2013.

[14] B. DasGupta B and N. Mobasheri, *On optimal approximability results for computing the strong metric dimension*. Discrete Applied Mathematics, 221, 18-24, 2017.

[15] Enron email network, available from UC Berkeley Enron Email Analysis website `http://bailando.sims.berkeley.edu/enron_email.html` (see also `https://www.cs.uic.edu/~dasgupta/network-data/`).

[16] T. Feder and R. Motwani, *Clique partitions, graph compression and speeding-up algorithms*. Journal of Computer and System Sciences, 51, 261-272, 1995.

[17] P. Gai and S. Kapadia, *Contagion in financial networks*. Proc. R. Soc. A, 466(2120), 2401-2423, 2010.

[18] Z. Galil and G. Italiano, *Data structures and algorithms for disjoint set union problems*. ACM Computing Surveys, 23, 319-344, 1991.

[19] Z. Galil and O. Margalit, *All pairs shortest distances for graphs with small integer length edges*. Information and Computation, 134, 103-139, 1997.

[20] Z. Galil and O. Margalit, *All pairs shortest paths for graphs with small integer length edges.* Journal of Computer and System Sciences, 54, 243-254, 1997.

[21] M. Gast, M. Hauptmann and M. Karpinski, *Inapproximability of dominating set on power law graphs.* Theoretical Computer Science, 562, 436-452, 2015.

[22] P. Gleiser and L. Danon, *Community structure in Jazz.* Advances in Complex Systems, 6(4), 565-573, 2003.

[23] R. Guimera, L. Danon, A. Diaz-Guilera, F. Giralt and A. Arenas, *Self-similar community structure in a network of human interactions.* Physical Review E, 68, 065103, 2003.

[24] *Hamsterster friendships network dataset* — KONECT, 2017, see `http://konect.uni-koblenz.de/networks/petster-friendships-hamster`.

[25] M. Hauptmann, R. Schmied and C. Viehmann, *Approximation complexity of metric dimension problem.* Journal of Discrete Algorithms, 14, 214-222, 2012.

[26] M. Hay, G. Miklau, D. Jensen, D. Towsley and P. Weis, *Resisting structural re-identification in anonymized social networks.* VLDB Journal, 1(1), 102-114, 2008.

[27] P. Holme, B. J. Kim, C. N. Yoon and S. K. Han, *Attack vulnerability of complex networks.* Physical Review E, 65, 056109, 2002.

[28] D. S. Johnson, *Approximation algorithms for combinatorial problems.* Journal of Computer and System Sciences, 9, 256-278, 1974.

[29] R. Khanin and E. Wit, *How scale-free are biological networks.* Journal of Computational Biology, 13(3), 810-818, 2006.

[30] S. Khuller, B. Raghavachari and A. Rosenfeld, *Landmarks in graphs.* Discrete Applied Mathematics, 70(3), 217-229, 1996.

[31] J. Leskovec and C. Faloutsos, *Sampling from Large Graphs.* 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 631-636, 2006.

[32] C. P. Loomis, J. O. Morales, R. A. Clifford and O. E. Leonard, *Turrialba: social systems and the introduction of change.* The Free Press, Glencoe, IL, p. 45 and 78, 1953.

[33] S. Markose, S. Giansante, M. Gatkowski and A. R. Shaghaghi, *Too interconnected to fail: financial contagion and systemic risk in network model of CDS and other credit enhancement obligations of US banks.* Economics Discussion Papers, Department of Economics, University of Essex, 683, 2009.

[34] S. Mauw, R. Trujillo-Rasua and B. Xuan, *Counteracting active attacks in social network graphs.* Proceedings of the 30th IFIP Annual Conference on Data and Applications Security and Privacy, 9766, 233-248, 2017.

[35] M. E. J. Newman, *The structure and function of complex networks.* SIAM Review, 45, 167-256, 2003.

[36] M. E. J. Newman, *Scientific collaboration networks: II. Shortest paths, weighted networks, and centrality.* Physical Review E, 64, 016132, 2001.

[37] A. Paranjape, A. R. Benson and J. Leskovec, *Motifs in temporal networks.* Proceedings of the Tenth ACM International Conference on Web Search and Data Mining, 2017.

[38] P. Panzarasa, T. Opsahl and K. M. Carley, *Patterns and dynamics of users' behavior and interaction: network analysis of an online community.* Journal of the American Society for Information Science and Technology, 60(5), 911-932, 2009.

[39] A. Sachs, *Completeness interconnectedness and distribution of interbank exposures - a parameterized analysis of the stability of financial networks.* Quantitative Finance, 14(9), 1677-1692, 2014.

[40] A. Salem, Y. Zhang, M. Humbert, M. Fritz and M. Backes, *ML-Leaks: Model and Data Independent Membership Inference Attacks and Defenses on Machine Learning Models*. arXiv:1806.01246, 2018.

[41] R. Seidel, *On the all-pairs-shortest-path problem in unweighted undirected graphs*. Journal of Computer and System Sciences, 51, 400-403, 1995.

[42] M. P. H. Stumpf, C. Wiuf and R. M. May, *Subnets of scale-free networks are not scale-free: Sampling properties of networks*. Proceedings of the National Academy of Sciences, 102(12), 4221-4224, 2005.

[43] R. Trujillo-Rasua and I. G. Yero, *k-metric antidimension: a privacy measure for social graphs*. Information Sciences, 328, 403-417, 2016.

[44] R. Trujillo-Rasua and I. G. Yero, *Characterizing* 1*-metric antidimensional trees and unicyclic graphs*. The Computer Journal, 59(8), 1264-1273, 2016.

[45] A. Wagner, *Estimating coarse gene network structure from large-scale gene perturbation data*. Genome Research, 12, 309-315, 2002.

[46] S. Wasserman and K. Faust, *Social Network Analysis*. Cambridge University Press, Cambridge, 1994.

[47] R. Yuster, *Computing the diameter polynomially faster than APSP*. arXiv:1011.6181v2, 2011.

[48] W. W. Zachary, *An information flow model for conflict and fission in small groups*. Journal of Anthropological Research, 33, 452-473, 1977.

[49] C. Zhang and Y. Gao, *On the Complexity of k-Metric Antidimension Problem and the Size of k-Antiresolving Sets in Random Graphs*. In Y. Cao and J. Chen (Eds.), COCOON 2017, LNCS 10392, 555-567, Springer, 2017.

[50] T. Zhang, Z. He and R. B. Lee, *Privacy-preserving Machine Learning through Data Obfuscation*. arXiv:1807.01860, 2018.

[51] M. Zito, *Greedy Algorithms for Minimisation Problems in Random Regular Graphs.* Proc. 9th Annuual European Symposium on Algorithms, 525-536, 2001.