上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

学士学位论文

BACHELOR'S THESIS

论文题目 基于社区结构的社交网络去匿名化

学生姓名 傅新喆

学生学号 5130309409

指导教师 傅洛伊

专　　业 计算机科学与技术

学院（系）电子信息与电气工程学院

Submitted in total fulfilment of the requirements for the degree of

Bachelor

in Computer Science and Technology

De-anonymization of Social Networks with Communities

Xinzhe Fu

Supervisor

Prof. Luoyi Fu

Depart of Computer Science and Engineering, SEIEE

Shanghai Jiao Tong University

Shanghai, P.R.China

May 28th, 2017

基于社区结构的社交网络去匿名化

摘　　要

通过在跨领域社交网络间建立映射从而对社交网络进行去匿名化已经成为当前的一个重要隐私问题。前人工作通常基于将社交网络建模为随机图来表示其中的节点和节点间的关系，之后通过目标函数来刻画映射的质量。但是这些目标函数的提出往往缺乏理论依据。另外，如何在算法层面上解决目标函数带来的疑问，即寻找目标函数的最小值点，仍然是一个开放的问题。

我们通过更实际的基于社区的社交网络建模来解决上述问题，同时，社交网络的社区信息也可作为去匿名化的辅助信息。通过最大后验估计，我们首先提出了一个具有充分理论依据的新目标函数。此目标函数的优势在于其最小值点与正确映射重合的概率最高。之后，我们首次从算法的角度探究此目标函数的可行性，即目标函数引出的优化问题。我们证明优化问题在一般情况下的不可近似性。尽管如此，我们仍提出了两个具有理论性能保证的近似算法，一个具有 ϵ-加性近似最优特性，另一个具有条件最优性。我们之后通过实验验证了理论结果的合理性。其中一个数据集提取自跨领域学术网络，它能够真实再现社交网络去匿名化的实际场景。我们的理论和实验结果同时还佐证了社区信息在隐私保护与推断中的重要性。

关键词： 社交网络，隐私，算法，图论

De-anonymization of Social Networks with Communities

ABSTRACT

A crucial privacy-driven issue nowadays is re-identifying ano-nymized social networks by mapping them to correlated cross-domain auxiliary networks. Prior works are typically based on modeling social networks as random graphs representing users and their relations, and subsequently quantify the quality of mappings through cost functions that are proposed without sufficient rationale. Also, it remains unknown how to algorithmically meet the demand of such quantifications, i.e., to find the minimizer of the cost functions.

We address those concerns in a more realistic social network modeling parameterized by community structures that can be leveraged as side information for de-anonymization. By Maximum A Posteriori (MAP) estimation, our first contribution is new and well justified cost functions. The new cost function enjoy superiority to previous ones in finding the correct mapping with the highest probability. The feasibility of the cost functions is then for the first time algorithmically characterized. While proving the general multiplicative inapproximability, we are able to propose two algorithms, which, respectively, enjoy an ϵ-additive approximation and a conditional optimality in carrying out successful user re-identification. Our theoretical findings are empirically validated, with a notable dataset extracted from rare true cross-domain academic networks that reproduce genuine social network de-anonymization. Both theoretical and empirical observations also manifest the importance of community information in enhancing privacy inferencing.

KEY WORDS: Social Networks, Privacy, Algorithms, Graph Theory

Contents

Table Index

Figure Index

Chapter 1 Introduction and Related Work

1.1 Introduction

The proliferation of social networks has led to generation of massive network data. Although users can be anonymized in the released data through removing personal identifiers [1–4], with their underlying relations preserved, they may still be re-identified by adversaries from correlated cross domain auxiliary networks where user identities are known [5–7].

Such idea of unveiling hidden users by leveraging their information collected from other domains, or alternatively called social network de-anonymization [7], is a fundamental privacy issue that has received considerable attention. Inspired by Pedarsani and Grossglauser [8], a large body of existing de-anonymization work shares a basic common paradigm: with an underlying network representing social relations between users, both the *published anonymized network* and the *auxiliary un-anonymized network* are generated from that network based on graph sampling that captures their correlation, as observed in many real cross-domain networks. The equivalent node sets they share are corresponded through an unknown correct mapping. With the availability of only structural information, adversaries attempt to re-identify users by establishing a mapping between networks. To quantify the quality of such mappings, several global cost functions have been proposed [8–10] in favor of exploring the conditions under which the correct matching can be unraveled from the mapping that minimizes the cost function.

Despite those dedications to de-anonymization, it is still not entirely understood how the privacy of anonymized social network can be guaranteed given that adversaries have no access to side information other than network structure, primarily for three reasons. First, the widely adopted Erdős-Rényi graph or Chung-Lu graph [11, 12] for the modeling of underlying social networks [8–10], though facilitating analysis, falls short

of well capturing the clustering effects that are prevalent in realistic social networks; Second, the cost functions [8, 9] in measuring mapping qualities not only lack sufficient rationale in analytical aspects, but most importantly, it remains unclear whether the feasibility of minimizing such cost functions could be theoretically characterized from an algorithmic aspect [13–15]; Last but not least, due to the rarity of true cross-domain datasets, current empirical observations of social network de-anonymization are either based on synthetic data, or real social networks with artificial sampling in construction of correlated published and auxiliary networks, and consequently do not well represent the genuine practical de-anonymization [13, 16, 17]. While a thorough understanding of this issue may better inform us on user privacy protection, this paper is particularly concerned about the following question: **Is it possible to quantify de-anonymization in a more realistic modeling, and meanwhile algorithmically meet the demand brought by such quantifications?**

The answer to this question entails appropriate modeling of social networks, well-designed cost functions as metrics of mappings and elaborated algorithms of finding the mapping that is optimal according to the metric, along with data collection that can empirically validate the related claims. To present a more reasonable model of underlying social network that incorporates the clustering effect, we adopt the stochastic block model [18] where nodes are partitioned into disjoint sets representing different communities [19]. Based on that, we investigate the problem following the paradigm, as noted earlier, where the published and auxiliary networks serve as two sampled subnetworks. Both of them inherit from the underlying network the community structures that can be leveraged as side structural information for adversaries. Similarly, we assume that other than network structure, there is no additional availability of side information to adversaries as it will only further benefit them. Varying the amount of availability of community information, here we classify our de-anonymization problem into two categories, i.e., bilateral case, and its counterpart, unilateral case, literally meaning that adversaries have access to community structure of both or only one network. A more formal definition of the two cases information is deferred to Section 2.1. Subsequently, we summarize, built on the model, our results on metrics, algorithms and empirical validations into three aspects answering the question raised.

Analytical aspect: For both cases, our first contribution is to derive the cost func-

tions as metrics quantifying the structural mismappings between networks based on Maximum A Posteriori (MAP) estimation. The virtue of MAP estimation ensures the superiority of our metrics to the previous ones in the sense that the minimizers of our cost functions equal to the underlying correct mappings with the highest probability. Also, as we will rigorously prove later, under fairly mild conditions on network density and the closeness between communities, through minimizing the cost function we can perfectly recover the correct mapping.

Algorithmic aspect: Following the derived quantifications, our next significant contribution is to take a first algorithmic look into the demand imposed by the quantifications, i.e., the optimization problems of minimizing such cost functions. We find that opposed to the simplicity of the cost functions in form, the induced optimization problems are computationally intractable and highly inapproximable. Therefore, we circumvent pursing exact or multiplicative approximation algorithms, but instead seek for algorithms with other types of guarantees. However, the issue is still made particularly challenging by the intricate tension among cost function, mappings, network topology as well as the super-exponentially large number of candidate mappings. Our main idea to resolve the tension is converting the problems into equivalent formulations that enable some relaxations, through bounding the influence of which, we demonstrate that the proposed algorithms have their respective performance guarantees. Specifically, one algorithm enjoys an ϵ-additive approximation guarantee in both cases, while the other yields optimal solutions for bilateral de-anonymization when the two sub-networks are highly structurally similar but fails to provide such guarantee for the unilateral case due to its lack of sufficient community information. Further comparisons of algorithmic results between the two cases also manifest the importance of community as side information in privacy inferencing.

Experimental aspect: Finally, we empirically verified all our theoretical findings under both synthetic and real datasets. We remark that one dataset, as never appeared in this context previously, is extracted from true cross-domain co-authorship networks [20] serving as published and auxiliary networks. As a result, it leads to no prior work, other than ours, that reproduces genuine scenarios of social network de-anonymization without artificial modeling assumptions. The experimental results demonstrate the effectiveness of our algorithms as they correctly re-identify more than 40% of users even

in the co-authorship networks that possess the largest deviation from our assumptions. Also, it empirically consolidates our argument that community information can increase the de-anonymization capability.

The rest of this paper is organized as follows: In Section 1.2 of Chapter 1, we briefly survey the related works. In Chapter 2, we introduce our model for de-anonymization problem of social networks with community structure and characterize the cases of bilateral and unilateral information. In Chapter 3, we present our results on analytical and algorithmic aspects of bilateral de-anonymization. Following the path of bilateral case, we introduce our results on unilateral de-anonymization and make comparisons between the two cases in Chapter 4. We present our experiments in Chapter 5 and conclude the paper in Chapter 6.

1.2 Related Works

The issue of social network de-anonymization, which has received considerable attention, was pioneeringly investigated by Narayanan and Shimatikov [7], who proposed the idea that users in anonymized networks can be re-identified through utilizing auxiliary networks with the same set of users from other domains. In that regard, they designed practical de-anonymization schemes that rely on side information in the form of a seed set of "pre-mapped" node pairs, i.e., a subset of nodes that are identified priorly across the two networks. Then the mapping is generated incrementally, starting from the seeds and percolating to the whole node sets.

Following this framework, Pedarsani and Grossglauser developed a succinct modeling that is amiable to theoretical analysis and serves as the paradigm for a family of subsequent related works on social network de-anonymization [8]. They assumed that the published and auxiliary networks are two graphs that share the same node sets with the edge sets resulted from independent samples of an underlying social network. Additionally, they studied a more challenging but practical version of de-anonymization that are free of prior seed information.

The two seminal works triggered a flurry of subsequent attempts that all fall into the categories of either seeded or seedless de-anonymization, tuning the model of the

underlying social networks. Specifically, in terms of seeded de-anonymization, current literature focuses on designing efficient de-anonymization algorithms that are executed by percolating the mapping to the whole node sets starting from the seed set. Yartseva et al. [21], Kazemi et al. [22], and later Fabiana et al. [23] proposed percolation graph matching algorithms for de-anonymization on Erdős-Rényi graph and scale-free network, respectively. Assuming that the underlying social network is generated following the preferential attachment model, Korula and Lattenzi [24] designed a correspnding efficient de-anonymizaiton algorithm. Chiasserini et al. [25] characterized the impact that clustering imposes on the performance of seeded de-anonymization. Under the classification of both perfect and imperfect seeded de-anonymization, Ji et al. [16] analyzed the two cases both qualitatively through theoretical characterization and empirically through experiments on real and synthetic datasets.

While this type of seed-based de-anonymizing methods works well in analysis, it is rather difficult or even impossible to acquire pre- identified user pairs across different networks as many real situations limit the access to user profiles. Therefore, more often we are faced with adversaries without seeds as side information, which is also the case considered in the present work. A natural alternative, under such circumstance, is to define a global cost function of mappings and unravel the correct mapping through the minimizer of the cost function. For instance, Pedarsani and Grossglauer [8] studied the seedless de-anonymization problem where the underlying social network is an Erdős-Rényi graph, the results of which were further improved by Cullina and Kiyavash [10]. Ji et al. analyzed perfect and partial de-anonymization on Chung-Lu graph [19] in this seedless de-anonymization setting. Kazemi et al. [9] focused on the case of de-anonymization problem on Erdős-Rényi graph where the published network and auxiliary network exhibit partial overlapping. A very recent work that shares the highest correlation with ours, belongs to that of Onaran et al. [15], who study the situation where there are only two communities in networks, a special case that can be embodied in our bilateral de-anonymization case.

Chapter 2 Models and Definitions

2.1 Network Models

In this section, we introduce the models and definitions of the social network de-anonymization problem. We first present the network models and then formally define the problem of social network de-anonymization. The network models consist of the underlying social networks G, the published network G_1 and the auxiliary network G_2 as incomplete observations of G. In reality, the edges of G, for example, might represent the true relationships between a set of people, while G_1 and G_2 characterize the observable interactions between these people such as communication records in cell phones or "follow" relationships in online social networks such as Tweeter and Facebook.

2.1.0.1 Underlying Social Network

To elaborate this, let $G = (V, E, \boldsymbol{M})$[1] be the graph representing the underlying social relationships between network nodes, where V is the set of nodes, E is the set of edges and $\boldsymbol{M}$[2] denotes the adjacency matrix of G. We treat G as an undirected graph and define the number of nodes as $|V| = n$. We assume that G is generated according to the *stochastic block model* [18]. Specifically, the model is interpreted as follows: the set of nodes in V are partitioned into κ disjoint subsets denoted as $C_1, C_2, \ldots, C_\kappa$ indicating their communities with $|C_i| = n_i$ and $\sum_i n_i = n$. The edges between nodes in different communities are drawn independently at random with certain probabilities. Let $c : V \mapsto \{1 \ldots \kappa\}$ be the community assignment function that assigns to each node

[1] For a matrix $\boldsymbol{M}$, we use $\mathbf{M}_{ij}$ to denote the element on its ith row and jth column and $\boldsymbol{M}_i$ to denote its ith row vector.

[2] $\boldsymbol{M}_{ij} = 1$ if $(i, j) \in E$ and $\boldsymbol{M}_{ij} = 0$ otherwise.

the label of the community it belongs to, we have

$$Pr\{(u,v) \in E\} = Pr\{\boldsymbol{M}_{uv} = 1\} = p_{c(u)c(v)},$$

where affinity values $\{p\}_{ab}$ $(1 \leq a, b \leq \kappa)$ are pre-defined parameters that indicate the edge existence probabilities and capture the closeness between communities. It has been shown that this model well captures the community structures in social networks and can generate graphs with various degree distributions by tuning the community affinity values $\{p\}$ [26].

2.1.0.2 Published Network and Auxiliary Network

We define $G_1(V_1, E_1, \boldsymbol{A})$ as the graph representing the published network and $G_2(V_2, E_2, \boldsymbol{B})$ as the graph representing the auxiliary network with E_1, E_2 denoting their edge sets and $\boldsymbol{A}, \boldsymbol{B}$ denoting their adjacency matrices respectively. In correspondence to real situations, G_1 represents the publicly available anonymized network where user identities are removed for privacy concern. In contrast, G_2 represents the auxiliary cross-domain un-anonymized network where those users' identities are known, and can be collected by the adversary to re-identify the users in G_1. Following previous literature [8, 16], we assume the node sets in G_1 and G_2 are equivalent and that the published network and the auxiliary network are independent samples obtained from the underlying social network G with sampling probabilities s_1 and s_2, respectively. Specifically, for $i = 1, 2$, we have

$$Pr\{(u,v) \in E_i\} = \begin{cases} s_i & \text{if } (u,v) \in E, \\ 0 & \text{otherwise.} \end{cases}$$

Technically, G, G_1 and G_2 are defined as the random graph variables for the networks. However, for ease of representation, we will also use them to denote the realizations of the random graph variables without loss of clearance. In the sequel, we will also use $\boldsymbol{\theta}$ as a shorthand of the set of parameters including affinity values $\{p\}$ and sampling probabilities s_1, s_2 in the models of G, G_1, G_2.

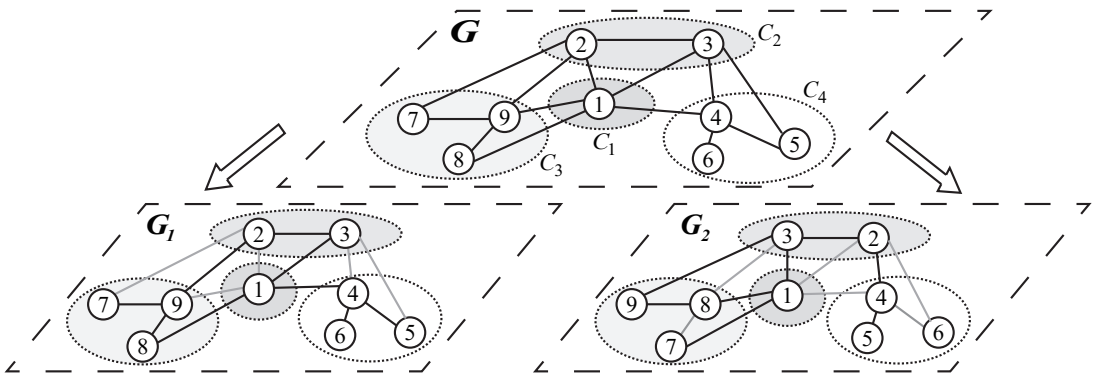


Figure 2–1: **An example of underlying social network (G), the published network (G_1) and the auxiliary network (G_2) sampled from G. C_1, C_2, C_3, C_4 represent the four communities in the networks. The correct mapping $\pi_0 = \{(1,1),(2,3),(3,2),(4,4),(5,6),(6,5),(7,9),(8,7),(9,8)\}$.**

2.2 Social Network De-anonymization

Given the published network G_1 and the auxiliary network G_2, the problem of social network de-anonymization aims to find a bijective mapping $\pi : V_1 \mapsto V_2$ that reveals the correct correspondence of the nodes in the two networks. Equivalently, a mapping π[3] can be represented as a permutation matrix $\mathbf{\Pi}$ where $\mathbf{\Pi}_{ij} = 1$ if $\pi(i) = j$ and $\mathbf{\Pi}_{ij} = 0$ otherwise. We naturally extend the definition of mapping of node set to the mapping of edge set, as $\pi(e = (i,j)) = (\pi(i), \pi(j))$.

We define π_0 (or equivalently $\mathbf{\Pi}_0$) to be the correct mapping between the node sets of G_1 and G_2. Note that we do not have access to π_0 or the generator G of G_1 and G_2. In other words, although the node sets of G_1 and G_2 are equivalent, the labeling of the nodes does not reflect their underlying correspondence. We interpret this in the way that the published network G_1 has the same node labeling as the underlying network G while the node labeling of G_2 is permuted. Following this interpretation, the community assignment function of G_1 equals to c. However the community assignment function of G_2, which we further define as c', may be different. We illustrate an example of our network models in Figure 2–1.

The community assignment functions of the two networks may serve as important

[3] In this paper, all the mappings are assumed to be bijective. Hence, we simply refer to them as mappings for brevity.

structural side information for de-anonymization, which naturally divide the social network de-anonymization problem into two types where the adversary possesses different amount of information on the community assignment. In the first type, the adversary possesses the community assignments of both G_1 and G_2. The corresponding problem is formally defined as follows.

Definition 2.2.1. (De-anonymization with Bilateral Community Information) Given the published network G_1, the auxiliary network G_2, the parameters $\boldsymbol{\theta}$, as well as the community assignment function c for G_1 and c' for G_2, the goal is to construct a mapping π that satisfies $\forall i, c(i) = c'(\pi(i))$ and is closest to the correct mapping π_0.

Since in this case, we have the community assignment of G_2, we can perform a relabeling on nodes in G_2 to make its community assignment equals to that of G_1. Hence, without loss of generality, for the case of de-anonymization with bilateral information, we denote c as the community assignment function of both G_1 and G_2 in the sequel.

The second variant corresponds to the case where the adversary only possesses the community assignment of the published network, which is formally stated as follows.

Definition 2.2.2. (**De-anonymization with Unilateral Community Information**) Given the published network G_1, the auxiliary network G_2, parameters $\boldsymbol{\theta}$, as well as the community assignment function c for G_1, the goal is to construct a mapping that is closest to the correct mapping π_0.

Intuitively, de-anonymization with unilateral information is harder than that with bilateral information due to the lack of side information. We will validate this argument with subsequent theoretical analysis and experiments. In addition, for brevity, we may refer to de-anonymization problem with bilateral community information and with unilateral community information as bilateral de-anonymization and unilateral de-anonymization respectively.

Remark: Till now, we have not given the quantifying metric of the closeness to the correct mapping π_0. A natural choice would be the mapping accuracy, i.e., percentage of nodes that are mapped identically as in π_0. However, as we have no knowledge of π_0, such ground-truth-based metrics do not apply. To tackle this, we leverage the Maximum A Posteriori (MAP) estimator to construct cost functions for measuring the

Table 2–1: **Notions and Definitions**

Notation	Definition
G	Underlying social network
G_1, G_2	Published and auxiliary networks
V, V_1, V_2	Vertex sets of graphs G, G_1 and G_2
E, E_1, E_2	Edge sets of graphs G, G_1, G_2
s_1, s_2	Edge sampling probabilities of graphs G_1, G_2
$\boldsymbol{M}, \boldsymbol{A}, \boldsymbol{B}$	Adjacency matrices of graphs G, G_1, G_2
c	Community assignment function
C_i	Vertex set of community i
n	Total number of vertices
κ	Total number of communities
n_i	Number of vertices in community i
p_{ab}	Affinity value indicating the edge existence probability between communities a and b
$\boldsymbol{\theta}$	Set of parameters in the models of G, G_1 and G_2
π_0	Correct mapping between vertices in G_1 and G_2
π	Mapping between vertices in G_1 and G_2
$\mathbf{\Pi}$	Permutation matrix of mapping π
Δ_π	Cost function of the mappings
$\{w\}$	Set of weights in the cost function

quality of mappings based solely on observable information. The main notations used throughout the paper are summarized in Table 2–1.

Chapter 3 Bilateral De-anonymization

3.1 Analytical Aspect of Bilateral De-anonymization

First, we investigate the de-anonymization problem with bilateral information, starting with an appropriate metric measuring the quality of mappings. We define our proposed metric in the form of a cost function that derived from Maximum A Posteriori (MAP) estimation.

3.1.1 MAP-based Cost Function

According to the definition of MAP estimation, given the published network G_1, auxiliary network G_2, parameters $\boldsymbol{\theta}$ and the community assignment function c, the MAP estimate $\hat{\pi}$ of the correct mapping π_0 is defined as:

$$\hat{\pi} = \arg\max_{\pi \in \Pi} Pr(\pi_0 = \pi \mid G_1, G_2, c, \boldsymbol{\theta}), \tag{3–1}$$

where $\Pi = \{\pi : V_1 \mapsto V_2 \mid \forall i, c(i) = c(\pi(i))\}$, i.e. the set of bijective mappings that observe the community assignment.

From the results in [15], the MAP estimator in Equation (3–1) can be computed as

$$\begin{aligned} \hat{\pi} &= \arg\min_{\pi \in \Pi} \sum_{i \le j}^{n} w_{ij} \left| \mathbb{1}\{(i,j) \in E_1\} - \mathbb{1}\{(\pi(i), \pi(j)) \in E_2\} \right| \\ &\triangleq \arg\min_{\pi \in \Pi} \Delta_\pi, \end{aligned} \tag{3–2}$$

where $w_{ij} = \log\left(\frac{1 - p_{c(i)c(j)}(s_1 + s_2 - s_1 s_2)}{p_{c(i)c(j)}(1 - s_1)(1 - s_2)}\right)$. Based on Equation (3–2), we have our cost function Δ_π as the metric for the quality of mappings, which can also be interpreted as weighted edge disagreements induced by mappings.

3.1.2 Validity of the Cost Function

Since our cost function Δ_π is derived using the MAP estimation, the minimizer of Δ_π, being the MAP estimate of π_0, coincides with the correct mapping with the highest probability [27, 28]. Aside from this, we proceed to justify the use of MAP estimation in de-anonymization problem from another perspective. Specifically, we prove that if the model parameters satisfy certain conditions, then the MAP estimate $\hat{\pi}$ *asymptotically almost surely*[1] coincides with the correct mapping π_0, which means that we can perfectly recover the correct mapping through minimizing Δ_π.

Theorem 3.1.1. *Let* $\alpha = \min_{ab} p_{ab}, \beta = \max_{ab} p_{ab}$, $\overline{w} = \max_{ij} w_{ij}$ *and* $\underline{w} = \min_{ij} w_{ij}$. *Assume that* $\alpha, \beta \to 0$, s_1, s_2 *do not go to 1 as* $n \to \infty$ *and* $\frac{\log \alpha}{\log \beta} \leq \gamma$. *Suppose that*

$$\frac{\alpha(1-\beta)^2 s_1^2 s_2^2 \log(1/\alpha)}{s_1 + s_2} = \Omega\left(\frac{\gamma \log^2 n}{n}\right) + \omega\left(\frac{1}{n}\right)^2,$$

then $\hat{\pi} = \pi_0$ *holds almost surely as* $n \to \infty$.

Proof. Due to space limitations, here we only presenting an outline of the proof and defer the details to **Appendix A.1**. Recall that for a mapping π, we define $\Delta_\pi = \sum_{i \leq j}^{n} w_{ij} |\mathbb{1}\{(i,j) \in E_1\} - \mathbb{1}\{\pi(i), \pi(j) \in E_2\}|$. Also, we denote Π_k as the set of mappings that map k nodes incorrectly and S_k as a random variable representing the the number of mappings $\pi \in \Pi_k$ with $\Delta_\pi \leq \Delta_{\pi_0}$. We then define $S = \sum_{k=2}^{n} S_k$ as the total number of incorrect mappings π with $\Delta_\pi \leq \Delta_{\pi_0}$ and derive an upper bound on the mean of S as $\mathbb{E}[S] \leq \sum_{k=2}^{n} n^k \max_{\pi \in \Pi_k} Pr\{\Delta_\pi - \Delta_{\pi_0} \leq 0\}$. We further show that under the conditions stated in the theorem, this upper bound, and consequently the value of $\mathbb{E}[S]$, go to 0 as $n \to \infty$, which implies that π_0 is the unique minimizer of Δ_π and concludes the proof.

□

Remark: We now present two further notes regarding Theorem 3.1.1. (i) *Applicability of the Theorem:* Recall that for a random Erdős-Rényi graph $G(n,p)$ to be

[1] An event *asymptotically almost surely* happens if it happens with probability $1 - o(1)$.

[2] We use standard Knuth's notations in this paper.

connected and free of isolated nodes with high probability, it must satisfy $p = \Omega(\frac{\log n}{n})$ [11], and the absence of isolated nodes is necessary for successful de-anonymization since there is no way that we can distinguish the isolated nodes in G_1 and G_2. Conventionally setting the sampling probabilities s_1, s_2 as constants, it is easy to verify that the conditions in Theorem 3.1.1 only have constant gap from the graph connectivity conditions even when the expected degree distributions (or equivalently, the closeness between the communities) of G_1 and G_2 are non-uniform (e.g. power law distribution where $\alpha/\beta = O(n)$ and $\log \alpha / \log \beta = O(\log n)$). From this aspect, the conditions are quite mild and thus make Theorem 3.1.1 fairly general; (ii) *Extension of the Theorem:* The cost function we design is robust, in the sense that any approximate minimizer Δ_π can map most of the nodes correctly. We formally present the claim in Corollary 3.2.

Corollary 3.2. *Let $\alpha, \beta, \overline{w}, \underline{w}$ be the same parameters defined in Theorem 3.1.1. Assume that α, β, s_1, s_2 do not go to 0 and $\frac{\log \alpha}{\log \beta} \leq \gamma$. Additionally, let δ, ϵ be two real numbers with $0 \leq \delta, \epsilon \leq 1$ with $\epsilon = O(\delta - \frac{\delta^2}{2})\alpha(1-\beta)s_1 s_2 \log(1/\alpha)$. If*

$$\frac{\alpha(1-\beta)^2 s_1^2 s_2^2 \log(1/\alpha)}{s_1 + s_2} = \Omega\left(\frac{\gamma \log^2 n}{(1-\delta/2)n}\right) + \omega\left(\frac{1}{n}\right),$$

then for all π^* with $\Delta_{\pi^*} - \min_{\pi \in \Pi} \Delta_\pi \leq \epsilon n^2$, π^* is guaranteed to map at least $(1-\delta)n$ nodes correctly as $n \to \infty$.

Proof. The proof is similar to that of Theorem 3.1.1. Instead of bounding $\sum_{k=2}^{n} \sum_{\pi \in \Pi_k} Pr\{\Delta_\pi - \Delta_{\pi_0} \leq 0\}$, we upper bound $\sum_{k=\delta n}^{n} \sum_{\pi \in \Pi_k} Pr\{\Delta_\pi - \Delta_{\pi_0} \leq \epsilon n^2\}$. Using similar technique as in Theorem 3.1.1, we have that under the conditions stated in the corollary, $\sum_{k=\delta n}^{n} \sum_{\pi \in \Pi_k} Pr\{\Delta_\pi - \Delta_{\pi_0} \leq \epsilon n^2\} \to 0$ as $n \to \infty$. Therefore, for a mapping π^* with $\Delta_{\pi^*} - \Delta_{\pi_0} \leq \epsilon n^2$, it maps at most $k = \delta n$ nodes incorrectly. Since $\Delta_{\pi_0} \geq \arg\min_{\pi \in \Pi} \Delta_\pi$, we conclude that all π^* with $\Delta_{\pi^*} - \min_{\pi \in \Pi} \Delta_\pi \leq \epsilon n^2$ are guaranteed to map at least $(1-\delta)n$ nodes correctly as $n \to \infty$. □

3.2 Algorithmic Aspect of Bilateral De-anonymization

The quantification in Section 3.1 justified that, under mild conditions, we can unravel the correct mapping through computing its MAP estimate, i.e., the minimizer

of Δ_π. This naturally puts forward the optimization problem of computing the minimizer of Δ_π, which reasonably serves as the instantiation of the social network de-anonymization problem (Definition 3.1). To meet the demand of the quantification, in this section, we formally define and investigate this optimization problem, presenting a first look into the algorithmic aspect of social network de-anonymization.

3.2.1 The Bilateral MAP-ESTIMATE Problem

Naturally, with some previously defined notations inherited, the optimization problem induced by the cost function can be formulated as follows.

Definition 3.2.1. (The BI-MAP-ESTIMATE Problem) Given two graphs $G_1(V_1, E_1, \boldsymbol{A})$ and $G_2(V_2, E_2, \boldsymbol{B})$, community assignment function c and a set of weights $\{w\}$, the goal is to compute a mapping $\hat{\pi} : V_1 \mapsto V_2$ that satisfies

$$\begin{aligned} \boldsymbol{P1}: \qquad \hat{\pi} &= \arg\min_{\pi\in\Pi} \sum_{i\le j}^{n} w_{ij} \left|\mathbb{1}\{(i,j)\in E_1\} - \mathbb{1}\{\pi(i),\pi(j)\in E_2\}\right| \\ &\triangleq \arg\min_{\pi\in\Pi} \Delta_\pi, \end{aligned}$$

where $\Pi = \{\pi \mid \forall i, c(i) = c(\pi(i))\}$.

Note that we require the weights $\{w\}$ to be induced by implicit and well-defined community affinity values and sampling probabilities. Also, the BI-MAP-ESTIMATE Problem denoted as $\boldsymbol{P1}$ above has several equivalent formulations, which will be presented later.

The BI-MAP-ESTIMATE seems to be easy at first glance due to the simplicity of its objective function Δ_π, but as justified by the following proposition, it is not only computationally intractable but also highly inapproximable.

Proposition 3.3. *BI-MAP-ESTIMATE problem is NP-hard. And there is no polynomial time (pseudo-polynomial time) approximation algorithm for BI-MAP-ESTIMATE with any multiplicative approximation guarantee unless* $GI \in P$ *(*$GI \in DTIME(n^{\text{polylog}n})$*).*[3]

[3] GI denotes the complexity class Graph Isomorphsim. $DTIME(T(n))$ denotes the set of problems that are solvable by deterministic Turing machine in $O(T(n))$ steps.

Proof. The proof can be easily constructed by reduction from the graph isomoprhism problem. The reduction is completed by just setting the two graphs in the instance of the graph isomorphism as G_1 and G_2, as well as assigning all $w_{ij} = 1$ and $c(v) = 1$ for all $v \in V_1, V_2$. Obviously, if the two graphs are isomorphic, the value $\Delta_{\hat{\pi}}$ of the optimal mapping $\hat{\pi}$ will be zero. Therefore, in this case, any algorithm with multiplicative approximation guarantee must find a mapping π with $\Delta_\pi = 0$. Furthermore, if G_1 and G_2 are not isomorphic, then any mapping π must induce a Δ_π strictly larger than 0. Hence, a polynomial time approximation algorithm for BI-MAP-ESTIMATE with multiplicative guarantee implies a polynomial time algorithm for the graph isomorphism problem. Note that the result can be further extended as there is no pseudo-polynomial time algorithm with multiplicative approximation guarantee unless $GI \in DTIME(n^{\text{polylog}n})$. □

3.2.2 Approximation Algorithms

As demonstrated above, the BI-MAP-ESTIMATE problem bears high computational complexity and approximation hardness. It is thus unrealistic to pursue exact or even multiplicative approximation algorithms. To circumvent this obstacle and still find solutions with provable theoretical properties, we propose two algorithms with their respective advantages: one has an ϵ-additive approximation guarantee and the other has lower time complexity and yields optimal solutions under certain conditions. The main idea behind them is to convert **P1** to equivalent formulations which are more amenable to relaxation techniques.

3.2.2.1 Additive Approximation Algorithm

The additive approximation algorithm we propose is based on the following quadratic assignment formulation of the BI-MAP-ESTIMATE Problem which we denote as $\boldsymbol{P2}$.

$$\begin{aligned}
\boldsymbol{P2}: \quad \text{maximize} \quad & \textstyle\sum_{i,j,k,l} q_{ijkl} x_{ik} x_{jl} && (3\text{–}3)\\
\textbf{s.t.} \quad & \textstyle\sum_i x_{ij} = 1, \quad \forall i \in V_1 && (3\text{–}4)\\
& \textstyle\sum_j x_{ij} = 1, \quad \forall j \in V_2 && (3\text{–}5)\\
& x_{ij} \in \{0, 1\} && (3\text{–}6)
\end{aligned}$$

The coefficients $\{q\}_{ijkl}$ of $\boldsymbol{P2}$ are defined as:

$$q_{ijkl} = \begin{cases} w_{ij}, & \text{if } (i,j) \in E_1, (k,l) \in E_2 \text{ and} \\ & c(i) = c(k), c(j) = c(l), \\ -1 & \text{if } c(i) \neq c(k) \text{ or } c(j) \neq c(l), \\ 0 & \text{otherwise.} \end{cases}$$

The solutions to $\boldsymbol{P2}$ are a set of integers $\{x\}$. We will refer to the value of $\sum_{i,j,k,l} q_{ijkl} x_{ik} x_{kl}$ as the value of $\{x\}$. Based on a solution $\{x\}$, we can construct its equivalent mapping for the BI-MAP-ESTIMATE problem by setting $\pi(i) = j$ iff $x_{ij} = 1$. The following proposition shows the correspondence between $\boldsymbol{P1}$ and $\boldsymbol{P2}$.

Proposition 3.3. *Given G_1, G_2, c and $\{w\}$, the optimal solutions of $\boldsymbol{P1}$ and $\boldsymbol{P2}$ are equivalent.*

Proof. We write the equivalent set of integers $\{x\}$ of a mapping π as $\{x^\pi\}$. First, we prove that the optimal solution $\{x^*\}$ to $\boldsymbol{P2}$ must observe the community assignment, i.e., if $x^*_{ij} = 1$, then $c(i) = c(j)$. Indeed, for a solution $\{x\}$ having some $x_{i_0 i_1} = 1$ but $c(i_0) \neq c(i_1)$, we can find a "cycle of community assignment violations" starting from i with $x_{i_0 i_1} = x_{i'_1 i_2} = x_{i'_2 i_3} = \ldots x_{i'_\rho i'_0}$ and $c(i_0) = c(i'_0), c(i_1) = c(i'_1), \ldots, c(i_\rho) = c(i'_\rho)$. Due to the special structure of the coefficients $\{q\}$, this cycle only contributes negative value to the objective function of $\boldsymbol{P2}$. Therefore, by "reversing" the cycle, we obtain a new solution $\{x'\}$ from $\{x\}$ with $x'_{i_0 i'_0} = x'_{i'_1 i_1} = x'_{i'_2 i_2} = \ldots = x'_{i'_\rho i_\rho} = 1$ and $\sum_{i,j,k,l} q_{ijkl} x'_{ij} x'_{kl} > \sum_{i,j,k,l} q_{ijkl} x_{ij} x_{kl}$.The process of reversing cycles of community assignment violations is demonstrated in Figure 2. If follows that the optimal solution to $\boldsymbol{P2}$ must observe the community assignment. Then, we proceed to show that the optimal solution to $\boldsymbol{P1}$ is equivalent to the optimal solution to $\boldsymbol{P2}$. Notice that for all $\{x^\pi\}$ that observe the community assignment, we have $\sum_{ij} w_{ij} = \sum_{ijkl} q_{ijkl} x^\pi_{ik} x^\pi_{jl} + \Delta_\pi$. Therefore, the corresponding $\{x^{\hat{\pi}}\}$ of the optimal solution $\hat{\pi}$ to $\boldsymbol{P1}$ is also optimal for $\boldsymbol{P2}$ and vice versa. □

The proof of Proposition 3.3 also provides the two main stages in our additive approximation algorithm: (i) Convert the instance of the BI-MAP-ESTIMATE prob-

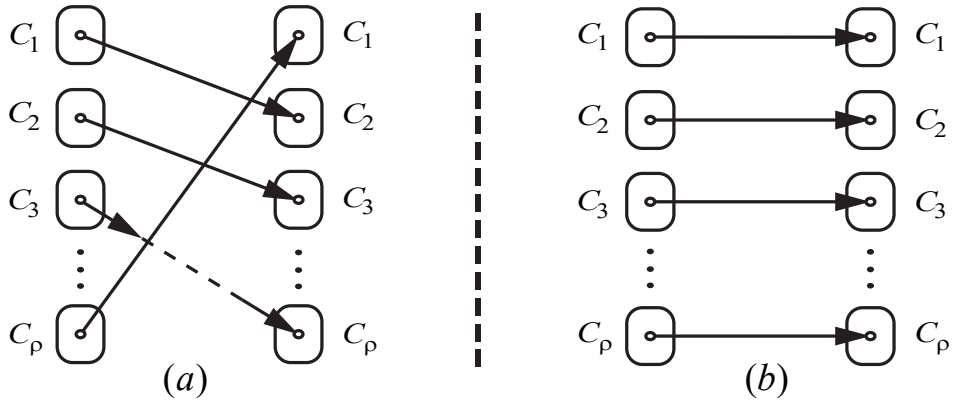


Figure 3–1: **Illustration of the reversal of a cycle of community assignment violations: (a) a cycle of community assignment violations in a mapping; (b) reversal of the cycle of violations.**

lem into its corresponding quadratic assignment formulation $\boldsymbol{P2}$ where the solution is then computed. (ii) Reverse all the "cycles of community assignment violations" in the solution and construct the desired mapping based on it.

For the first stage, we adopt the relaxing-rounding based algorithm proposed by Arora at al. [29] as a sub-procedure referred to as "QA-Rounding" to solve the converted instances of $\boldsymbol{P2}$. QA-Rounding has additive approximation guarantee when the instances have coefficients $\{q\}$ that do not scale with the size of the problem [29]. Note that the requirement for the coefficients to be independent of the size of the problem is one of the key factors for the seemingly unnatural formulation of $\boldsymbol{P2}$. For the sake of completeness, we state in the following lemma the related result from [29].

Lemma 3.4. *(Theorem 3 in [29]) Given an instance of $\boldsymbol{P2}$ with $-C \leq q_{ijkl} \leq C$ for all $i, j, k, l \in \{1 \dots n\}$ where C is a constant that is independent of n, then for any $\epsilon > 0$, QA-Rounding finds a solution $\{x\}$ with*

$$\sum_{i,j,k,l} q_{ijkl} x_{ik} x_{jl} \geq \sum_{ijkl} q_{ijkl} x^*_{ijkl} - \epsilon n^2$$

in $n^{O(\log n/\epsilon^2)}$ time, where $\{x^*\}$ is the optimal solution.

The second stage can be completed by repeatedly traversing the solution $\{x\}$ to

identify all the cycles of community assignment violations and reversing them. **Algorithm 1** illustrates a whole diagram of our proposed additive approximation algorithm.

Approximation Guarantee: By Lemma 3.4, QA-Rounding yields a solution whose value has a gap of less than ϵn^2 from the optimal. Combined with the equality $\sum_{i,j} w_{ij} = \Delta_\pi + \sum_{i,j,k,l} q_{ijkl} x_{ik} x_{jl}$ and the fact that the reversal of all the cycles of community assignment violations only incurs an increase on the value of the computed solution $\{x\}$, we have that the mapping π given by **Algorithm 1** has an ϵ-additive approximation guarantee and satisfies $c(i) = c(\pi(i))$ for all i. Moreover, by Corollary 3.2, we know that when ϵ, δ satisfy the conditions in the corollary, the mappings yielded by **Algorithm 1** map at least $(1-\delta)n$ nodes correctly.

Input: Graphs G_1, G_2, weights $\{w\}$,
community assignment function c.
Output: mapping π.
Initialize: $\pi = \emptyset$, $\forall i, j, k, l \in \{1 \dots n\}, x_{ijkl} = 0$, $i', j' = 0$
Compute the set of coefficients $\{q\}_{ijkl}$ and
form an instance $\mathcal{I}$ of $\boldsymbol{P2}$.
$\{x\}$:=QA-Rounding($\mathcal{I}$).
for $i = 1$ *to* n **do**
  for $j = 1$ *to* n **do**
    if $x_{ij} = 1$ *and* $c(i) \neq c(j)$ **then**
      $x_{ij} := 0$.
      while $c(j') \neq c(i)$ **do**
        Find i', j' with $x_{i'j'} = 1$ and $c(i') = c(j)$.
        $x_{i'j'} := 0, x_{i'j} := 1, j := j'$.
      end
      $x_{ij'} := 1$.
    end
  end
end
Construct π based on $\{x\}$.
Return π

Algorithm 1: The Additive Approximation Algorithm

Time Complexity: The QA-Rounding has a time complexity of $n^{O(\log n/\epsilon^2)}$. The reversal of all the cycles can be completed in $O(n^2)$ time when $\{x\}$ is represented in the form of an adjacency list-like structure. Based on those, the time complexity of **Algorithm 1** is $O(n^{O(\log n/\epsilon^2)} + n^2)$.

3.2.2.2 Convex Optimization-Based Heuristic

Beside the algorithm that provides additive approximation guarantee under general case, it is also useful to pursue algorithms that have stronger guarantee in special cases. In this section, we present one such algorithm that can find the optimal solution in the cases where the structural similarity between the two networks are higher than certain threshold.

The algorithm is based on convex optimization, which relies on a matrix formulation of the BI-MAP-ESTIMATE problem. The main idea is to first solve a convex-relaxed version of the matrix formulation and then convert the solution back to a legitimate one. Specifically, the matrix formulation of the BI-MAP-ESTIMATE problem, which we denote by P3, is formally stated as follows:

$$
\begin{aligned}
\boldsymbol{P3}: \quad & \text{mininize } \|\boldsymbol{W} \circ (\boldsymbol{A} - \boldsymbol{\Pi}^{\mathrm{T}} \boldsymbol{B} \boldsymbol{\Pi})\|_{\mathrm{F}}^2 + \mu \|\boldsymbol{\Pi} \boldsymbol{m} - \boldsymbol{m}\|_{\mathrm{F}}^2 \\
& \textbf{s.t. } \forall i \in V_1,\ \textstyle\sum_i \boldsymbol{\Pi}_{ij} = 1 && (3\text{–}7) \\
& \quad \forall j \in V_2,\ \textstyle\sum_j \boldsymbol{\Pi}_{ij} = 1 && (3\text{–}8) \\
& \quad \forall i, j,\ \boldsymbol{\Pi}_{ij} \in \{0, 1\}, && (3\text{–}9)
\end{aligned}
$$

where $\boldsymbol{W}$ is a symmetric matrix with $\boldsymbol{W}_{ij} = \boldsymbol{W}_{ji} = \sqrt{w_{ij}}$, $\boldsymbol{m}$ represents the community assignment vector $(c(1), \ldots, c(n))^{\mathrm{T}}$, μ is a positive constant that is large enough, $\circ$ denotes the matrix Hadamard product with $(\boldsymbol{W} \circ \boldsymbol{A})_{ij} = \boldsymbol{W}_{ij} \cdot \boldsymbol{A}_{ij}$ and $\|\cdot\|_{\mathrm{F}}$ represents the Frobenius norm.

Note that $\boldsymbol{P3}$ is equivalent to $\boldsymbol{P1}$ from the perspective of the relation between a mapping and its corresponding permutation matrix. The claim is formally stated and proved in the following proposition.

Proposition 3.3. *Given G_1, G_2, c and $\{w\}$, the optimal solution of $\boldsymbol{P1}$ and $\boldsymbol{P3}$ are equivalent.*

Proof. The proof is similar to that of Proposition 3.3. First, due to the existence of the penalty factor $\mu \|\boldsymbol{\Pi} \boldsymbol{m} - \boldsymbol{m}\|_{\mathrm{F}}^2$, we have that the optimal solution of $\boldsymbol{P3}$ must observe the community assignment. Second, as for all the permutation matrices $\boldsymbol{\Pi}$'s and their corresponding mappings π's that observe the community assignment, it is easy to show

that $\Delta_\pi = \|\boldsymbol{W} \circ (\boldsymbol{A} - \boldsymbol{\Pi}^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\Pi})\|_{\mathrm{F}}^2 + \mu\|\boldsymbol{\Pi}\boldsymbol{m} - \boldsymbol{m}\|_{\mathrm{F}}^2$ (the second term equals to 0 in this case). Hence, the optimal solution of $\boldsymbol{P1}$ and $\boldsymbol{P3}$ are equivalent. □

Before introducing the algorithm, we further transform the objective function of $\boldsymbol{P3}$ into an equivalent but more tractable form. Lemma 3.4 gives the main idea of the transformation.

Lemma 3.4. *Let $\tilde{\boldsymbol{A}} = \boldsymbol{W} \circ \boldsymbol{A}$ and $\tilde{\boldsymbol{B}} = \boldsymbol{W} \circ \boldsymbol{B}$ be the weighted adjacency matrices of G_1 and G_2 respectively, then for all permutation matrices that observe the community assignment*[4]*,the following equality holds:*

$$\|\boldsymbol{W} \circ (\boldsymbol{A} - \boldsymbol{\Pi}^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\Pi})\|_{\mathrm{F}} = \|\boldsymbol{\Pi}\tilde{\boldsymbol{A}} - \boldsymbol{B}\tilde{\boldsymbol{\Pi}}\|_{\mathrm{F}}.$$

Proof. We prove the lemma by repeatedly using the symmetry of $\boldsymbol{A}$ and $\boldsymbol{B}$ and special properties of $\boldsymbol{W}$ and $\boldsymbol{\Pi}$. The detailed steps are presented as follows:

$$\begin{aligned}
\|\boldsymbol{W} \circ (\boldsymbol{A} - \boldsymbol{\Pi}^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\Pi})\|_{\mathrm{F}} &= \|\boldsymbol{W} \circ (\boldsymbol{\Pi}(\boldsymbol{A} - \boldsymbol{\Pi}^{\mathrm{T}}\boldsymbol{B}\boldsymbol{\Pi}))\|_{\mathrm{F}} && \text{(3–10)}\\
&= \|\boldsymbol{W} \circ (\boldsymbol{\Pi}\boldsymbol{A} - \boldsymbol{B}\boldsymbol{\Pi})\|_{\mathrm{F}} && \text{(3–11)}\\
&= \|\boldsymbol{W} \circ (\boldsymbol{\Pi}\boldsymbol{A}) - \boldsymbol{W} \circ (\boldsymbol{B}\boldsymbol{\Pi})\|_{\mathrm{F}} && \text{(3–12)}\\
&= \|\boldsymbol{\Pi}(\boldsymbol{W} \circ \boldsymbol{A}) - (\boldsymbol{W} \circ \boldsymbol{B})\boldsymbol{\Pi}\|_{\mathrm{F}} && \text{(3–13)}\\
&= \|(\boldsymbol{\Pi}\tilde{\boldsymbol{A}} - \tilde{\boldsymbol{B}}\boldsymbol{\Pi})\|_{\mathrm{F}}. && \text{(3–14)}
\end{aligned}$$

Note that Equation (3–10) holds because multiplying by a permutation matrix does not change the value of element-wise Frobenius norm. Equations (3–11), (3–12) and (3–14) hold due to the definition of Hadamard product and $\tilde{\boldsymbol{A}}, \tilde{\boldsymbol{B}}$. The validity of Equation (3–13) is less straightforward and can be interpreted in the following way: For the weight w_{ij} of a node pair (i, j), it is determined only by parameters $p_{c(i)c(j)}, s_1, s_2$. Therefore, if $c(i) = c(j), c(k) = c(l)$ for some nodes i, j, k, l, then we have $\boldsymbol{W}_{ik} = \boldsymbol{W}_{jl}$, i.e., the weight is invariant within communities. This crucial property, combined with the fact that $\boldsymbol{\Pi}$ is permutation matrix that observes the community assignment, makes the Hadamard products and normal matrix multiplication in Equation (3–13) interchangeable, which concludes the proof. □

[4] A permutation matrix $\boldsymbol{\Pi}$ observes community assignment if for all $\boldsymbol{\Pi}_{ij} = 1$, $c(i) = c(j)$.

Based on Lemma 3.4, we can rewrite the objective function of $\boldsymbol{P3}$ as $\|(\boldsymbol{\Pi}\tilde{\boldsymbol{A}} - \tilde{\boldsymbol{B}}\boldsymbol{\Pi})\|_{\mathrm{F}}^2 + \mu\|\boldsymbol{\Pi}\boldsymbol{m} - \boldsymbol{m}\|_{\mathrm{F}}^2$. Then, we further relax constraints (3–8) and (3–9) in $\boldsymbol{P3}$ and obtain the optimization problem $\boldsymbol{P3'}$ that can be formulated as:

$$\begin{aligned} \boldsymbol{P3'} \quad & \text{minimize } \|(\boldsymbol{\Pi}\tilde{\boldsymbol{A}} - \tilde{\boldsymbol{B}}\boldsymbol{\Pi})\|_{\mathrm{F}}^2 + \mu\|\boldsymbol{\Pi}\boldsymbol{m} - \boldsymbol{m}\|_{\mathrm{F}}^2 \\ & \textbf{s.t. } \forall i,\ \textstyle\sum_{i\in V_1} \boldsymbol{\Pi}_{ij} = 1 \end{aligned}$$

Obviously the objective function and the set of feasible solutions are both convex. Immediately we can conclude that $\boldsymbol{P3'}$ is a convex-relaxed version of $\boldsymbol{P3}$, which is stated in the following lemma.

Lemma 3.5. *$\boldsymbol{P3'}$ is a convex optimization problem.*

With all the prerequisites above, we are now ready to present our second convex optimization-based algorithm, which firstly solves for a fractional optimal solution of $\boldsymbol{P3'}$ and then projects that fractional solution into an integral permutation matrix (and its corresponding mapping). During the projection process, we use an n-dimensional array $Mapped$ to record the projected nodes and a set $Legal_i$ for each node i to record the remaining legitimate nodes to which it can be mapped. The details are illustrated in **Algorithm 2**.

Performance Guarantee: Generally, **Algorithm 2** can not yield the optimal solution to the BI-MAP-ESTIMATE problem and the gap between its solution and the optimal one may be large. However, we will demonstrate that when the similarity between G_1 and G_2 are high enough, or equivalently, the difference between the weighted adjacency matrices $\tilde{\boldsymbol{A}}$ and $\tilde{\boldsymbol{B}}$ is sufficiently small, **Algorithm 2** is guaranteed to find the optimal mapping.

Theorem 3.5.1. *Let $\tilde{\boldsymbol{B}}'$ be a symmetric matrix that is related with $\tilde{\boldsymbol{A}}$ by a unique $\hat{\boldsymbol{\Pi}}$ that observes the community assignment, i.e., $\tilde{\boldsymbol{B}}' = \hat{\boldsymbol{\Pi}}\boldsymbol{A}\hat{\boldsymbol{\Pi}}^{\mathbf{T}}$. Denote $\tilde{\boldsymbol{B}}' = \boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}^{\mathbf{T}}$ as its unitary eigen-decomposition with $\epsilon_2 \le \sum_j |\boldsymbol{U}_{ij}| \le \epsilon_1$ for all i. Define $\lambda_1, \lambda_2, \ldots, \lambda_n$ as the eigenvalues of $\tilde{\boldsymbol{B}}'$ with $\sigma = \max_i |\lambda_i|$ and $\delta \le |\lambda_i - \lambda_j|$ for all i, j. Assume that there exists a matrix $\boldsymbol{R}$ that satisfies $\tilde{\boldsymbol{B}} = \tilde{\boldsymbol{B}}' + \boldsymbol{R}$. We denote $\boldsymbol{E} = \boldsymbol{U}\boldsymbol{R}\boldsymbol{U}^{\mathbf{T}}$ with $\|\boldsymbol{E}\|_{\mathrm{F}} = \xi$ and $\boldsymbol{M} = \boldsymbol{m}^{\mathbf{T}}\boldsymbol{m}$ with $\|\boldsymbol{M}\|_{\mathrm{F}} = M$. Let $\boldsymbol{\Pi}^p$ be the solution obtained by*

Input: Graphs G_1, G_2, weights $\{w\}$,
community assignment function c.
Output: mapping π.
Initialize: $Mapped[i] = 0$. $Legal_i = \emptyset$ **for all** i**,**
$\pi = \emptyset$, $\mathbf{\Pi}^p, \mathbf{\Pi}^f = \mathbf{0}$.
Compute the weight matrix $\boldsymbol{W}$ and
form an instance $\mathcal{I}$ of $\boldsymbol{P3}$.
Relax $\mathcal{I}$ into an instance $\mathcal{I}'$ of $\boldsymbol{P3'}$. $\mathbf{\Pi}^f :=$ the optimal (fractional) solution to ($\mathcal{I}'$).
for $i = 1$ *to* n **do**
  $Legal_i := \{k \mid Mapped[k] = 0$ and $c(k) = c(i)\}$ $j := \arg\max_{k \in Legal_i} \mathbf{\Pi}^f_{ik}$.
  $\mathbf{\Pi}^p_{ij} := 1$. $Mapped[j]$:=1.
end
Construct π based on $\mathbf{\Pi}^p$.
Return π

Algorithm 2: Convex Optimization-Based Algorithm

Algorithm 2 *and* $\mathbf{\Pi}^*$ *be the optimal solution. If*

$$(\sigma^2 + 1)\xi^2 + \mu^2 M^2 \leq \left[\frac{\delta^2}{(2\sqrt{n}+1)(1+\sqrt{n}\epsilon_1/\epsilon_2)(1+2\epsilon_1/\epsilon_2)}\right]^2,$$

then $\mathbf{\Pi}^p = \mathbf{\Pi}^*$.

Proof. The proof is divided into three steps: (i) First, similar to the argument in [30], by constructing the Lagrangian function of $\boldsymbol{P3'}$ and setting its gradient to 0, we obtain the necessary conditions that the optimal fractional solution $\mathbf{\Pi}^f$ to $\boldsymbol{P3'}$ must satisfy; (ii) Then, combining these with the conditions stated in the theorem and the projection from $\mathbf{\Pi}^f$ to $\mathbf{\Pi}^p$, we show that $\mathbf{\Pi}^p = \hat{\mathbf{\Pi}}$; (iii) Finally, we prove that in this case $\hat{\mathbf{\Pi}} = \mathbf{\Pi}^*$, which concludes the proof.

1. Derivation of the Necessary Conditions: We start the first step with rewriting $\boldsymbol{P3'}$ as an optimization problem with respect to $\boldsymbol{Q} = \mathbf{\Pi}\hat{\mathbf{\Pi}}^{\mathbf{T}}$. Since

$$\mathbf{\Pi}\tilde{\boldsymbol{A}} - \tilde{\boldsymbol{B}}\mathbf{\Pi} = (\mathbf{\Pi}\hat{\mathbf{\Pi}}^{\mathbf{T}}\tilde{\boldsymbol{B}}' - \tilde{\boldsymbol{B}}\mathbf{\Pi}\hat{\mathbf{\Pi}}^{\mathbf{T}})\hat{\mathbf{\Pi}} = (\boldsymbol{Q}\tilde{\boldsymbol{B}}' - \tilde{\boldsymbol{B}}\boldsymbol{Q})\hat{\mathbf{\Pi}},$$

and $\mathbf{\Pi}\boldsymbol{m} - \boldsymbol{m} = (\boldsymbol{Q}\boldsymbol{m} - \boldsymbol{m})\hat{\mathbf{\Pi}}$, we can reformulate the objective function of $\boldsymbol{P3'}$ with $\boldsymbol{Q}$ as variable and divide it by two for ease of further manipulation as $\frac{1}{2}\|\boldsymbol{Q}\tilde{\boldsymbol{B}} - \boldsymbol{B}\boldsymbol{Q}\|_{\mathrm{F}}^2 + \frac{\mu}{2}\|\boldsymbol{Q}\boldsymbol{m} - \boldsymbol{m}\|_{\mathrm{F}}^2$. The constraint $\sum_j \mathbf{\Pi}_{ij}$ for all i can be expressed as $\boldsymbol{Q}\mathbf{1} = \mathbf{1}$. The solution of the reformulated version can be associated with the original one by $\mathbf{\Pi} = \boldsymbol{Q}\hat{\mathbf{\Pi}}$. Next, by introducing multiplier $\boldsymbol{\alpha}$ for the equality constraint of $\boldsymbol{P3'}$, we

construct its Lagrangian function as

$$L(\boldsymbol{Q}, \boldsymbol{\alpha}) = \frac{1}{2}\|\boldsymbol{Q}\tilde{\boldsymbol{B}} - \boldsymbol{B}\boldsymbol{Q}\|_{\mathrm{F}}^2 + \frac{\mu}{2}\|\boldsymbol{Q}\boldsymbol{m} - \boldsymbol{m}\|_{\mathrm{F}}^2 + \mathrm{tr}(\boldsymbol{Q}\mathbf{1} - \mathbf{1})\boldsymbol{\alpha}^{\mathrm{T}}.$$

The key element of the proof of the lemma is the sufficient conditions for $\boldsymbol{Q}$ to be the optimal (fractional) solution to $\boldsymbol{P3'}$. To yield the sufficient conditions, we take the gradient of $L(\boldsymbol{Q}, \boldsymbol{\alpha})$ with respect to $\boldsymbol{Q}$ and set it as 0. Then we have

$$\bigtriangledown_{\boldsymbol{Q}} L(\boldsymbol{Q}, \boldsymbol{\alpha}) = \boldsymbol{Q}\boldsymbol{B}^2 + \tilde{\boldsymbol{B}}^2\boldsymbol{Q} - 2\tilde{\boldsymbol{B}}\boldsymbol{Q}\boldsymbol{B} + \boldsymbol{\alpha}\mathbf{1}^{\mathrm{T}} + \mu(\boldsymbol{Q}\boldsymbol{M} - \boldsymbol{M}) = \mathbf{0}.$$

Multiplying $\boldsymbol{U}^{\mathrm{T}}$ to the left side of $\bigtriangledown_{\boldsymbol{Q}} L(\boldsymbol{Q}, \boldsymbol{\alpha})$ and $\boldsymbol{U}$ to the right side we get

$$\begin{aligned}(\boldsymbol{F}\boldsymbol{\Lambda}^2 + \boldsymbol{\Lambda}^{\mathbf{2}}\boldsymbol{F} - 2\boldsymbol{\Lambda}\boldsymbol{F}\boldsymbol{\Lambda}) + (\boldsymbol{F}\boldsymbol{E}\boldsymbol{\Lambda} + \boldsymbol{F}\boldsymbol{\Lambda}\boldsymbol{E} - 2\boldsymbol{\Lambda}\boldsymbol{F}\boldsymbol{E}) \\ + \boldsymbol{\gamma}\boldsymbol{v}^{\mathrm{T}} + \boldsymbol{F}\boldsymbol{G} + \mu\boldsymbol{F}\boldsymbol{M'} - \mu\boldsymbol{M'} = \mathbf{0},\end{aligned}$$

where $\boldsymbol{F} = \boldsymbol{U}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{U}$, $\boldsymbol{v} = \boldsymbol{U}^{\mathrm{T}}\mathbf{1}$, $\boldsymbol{\gamma} = \boldsymbol{U}^{\mathbf{T}}\boldsymbol{\alpha}$, $\boldsymbol{G} = \boldsymbol{E}^2$ and $\boldsymbol{M'} = \boldsymbol{U}^{\mathbf{T}}\boldsymbol{M}\boldsymbol{U}$.

Rewriting the equation coordinate-wise, we have

$$\begin{aligned}&\boldsymbol{F}_{ij}(\lambda_i - \lambda_j)^2 + \boldsymbol{v}_j\boldsymbol{\gamma}_i - \mu\boldsymbol{M}'_{ij} \\ &\quad + \textstyle\sum_k \boldsymbol{F}_{ik}(\boldsymbol{E}_{kj}(\lambda_j + \lambda_k - 2\lambda_i) + \boldsymbol{G}_{kj} + \mu\boldsymbol{M}'_{kj}) = 0\end{aligned}$$

Substituting $i = j$ into the above equation and plugging the results back to eliminate variables $\boldsymbol{\gamma}_i$'s, it follows that

$$\begin{aligned}\boldsymbol{F}_{ij}\boldsymbol{v}_i(\lambda_i - \lambda_j)^2 &+ \textstyle\sum_k \boldsymbol{F}_{ik}(\boldsymbol{v}_i\boldsymbol{G}_{kj} - \boldsymbol{v}_j\boldsymbol{G}_{ki} + \mu\boldsymbol{v}_i\boldsymbol{M}'_{kj} - \mu\boldsymbol{v}_j\boldsymbol{M}'_{ki}) \\ &+ \textstyle\sum_k \boldsymbol{F}_{ik}(\boldsymbol{v}_i\,\boldsymbol{E}_{kj}(\lambda_j + \lambda_k - 2\lambda_i) - \boldsymbol{v}_j\boldsymbol{E}_{kj}(\lambda_k - \lambda_i)) \\ &+ \mu(\boldsymbol{v}_j\boldsymbol{M}'_{ii} - \boldsymbol{v}_i\boldsymbol{M}'_{ij}) = 0\end{aligned}$$

We further define the following variables

$$
\begin{aligned}
r_{ij} &= \frac{\mu}{(\lambda_i - \lambda_j)^2}(\boldsymbol{v}_j \boldsymbol{M}'_{ii} - \boldsymbol{v}_i \boldsymbol{M}'_{ij}) \\
s^i_{jk} &= \frac{1}{(\lambda_i - \lambda_j)^2}\left(\boldsymbol{E}_{kj}(\lambda_j + \lambda_k - 2\lambda_i) - \frac{\boldsymbol{v}_j}{\boldsymbol{v}_i}\boldsymbol{E}_{ki}(\lambda_k - \lambda_i)\right) \\
t^i_{jk} &= \frac{1}{(\lambda_i - \lambda_j)^2}\left(\boldsymbol{G}_{kj} - \frac{\boldsymbol{v}_j}{\boldsymbol{v}_i}\boldsymbol{G}_{ki}\right) \\
w^i_{jk} &= \frac{\mu}{(\lambda_i - \lambda_j)^2}\left(\boldsymbol{M}'_{kj} - \frac{\boldsymbol{v}_j}{\boldsymbol{v}_i}\boldsymbol{M}'_{ki}\right),
\end{aligned}
$$

for $i \neq j$. And $s^j_{ik} = t^j_{ik} = w^i_{jk} = r_{ij} = 0$ for $i = j$. Then, we arrive at the following linear system

$$
\begin{aligned}
\boldsymbol{F}_{ij} + \textstyle\sum_k \boldsymbol{F}_{ik}(s^i_{jk} + t^i_{jk} + w^i_{jk} + \frac{r_{ij}}{n}) = 0, \quad i \neq j \qquad &(3\text{–}15) \\
\textstyle\sum_k \boldsymbol{F}_{ik}\boldsymbol{v}_k = \boldsymbol{v}_i, \qquad &(3\text{–}16)
\end{aligned}
$$

where the second set of equations come from the constraint $\boldsymbol{Q}\mathbf{1} = \mathbf{1}$. Equations (3–15) and (3–16) represent conditions that the optimal solution $\boldsymbol{Q}$ (or equivalently $\boldsymbol{F}$) needs to satisfy.

2. The Equivalence of $\boldsymbol{\Pi}^p$ and $\hat{\boldsymbol{\Pi}}$: Based on the conditions above, we move on to the second step. Recall that in this step our goal is to prove that $\boldsymbol{\Pi}^p$, which is a projection of the optimal fractional solution $\boldsymbol{\Pi}^f$, equals to $\hat{\boldsymbol{\Pi}}$. We formalize this notion in Lemma 3.6, the proof of which carries on the main idea of the second step.

Lemma 3.6. *Let $\boldsymbol{\Pi}^p$ be the solution computed by **Algorithm 2** and $\hat{\boldsymbol{\Pi}}$ be defined as in Theorem 3.5.1. Under the conditions stated in the theorem, $\boldsymbol{\Pi}^p = \hat{\boldsymbol{\Pi}}$.*

Proof. As the optimal fractional solution $\boldsymbol{\Pi}^f = \boldsymbol{Q}\hat{\boldsymbol{\Pi}}$, we first show that $\boldsymbol{Q}$ (or $\boldsymbol{F}$) is sufficiently close to the identity matrix $\boldsymbol{I}$, from which using the property of the projection process we obtain that $\boldsymbol{\Pi}^p$ is identical to $\hat{\boldsymbol{\Pi}}$. We achieve this by treating linear system consisting of Equations (3–15) and (3–16) as a perturbed version of

$$
\begin{aligned}
\boldsymbol{F}_{ij} = 0, \quad i \neq j \qquad &(3\text{–}17) \\
\textstyle\sum_k \boldsymbol{F}_{ik}\boldsymbol{v}_k = \boldsymbol{v}_i, \qquad &(3\text{–}18)
\end{aligned}
$$

the solution of which is clearly $\boldsymbol{I}$. Then using the results from stability of perturbed linear system [31] that is presented in Lemma 3.7 below and the conditions in Theorem 3.5.1, we can bound the difference between $\boldsymbol{F}$ and $\boldsymbol{I}$.

Lemma 3.7. *(Theorem 1 in [31]) Let $\|\cdot\|$ be any p-norm. For two linear systems $\boldsymbol{D}\boldsymbol{x} = \boldsymbol{b}$ and $\tilde{\boldsymbol{D}}\boldsymbol{x} = \tilde{\boldsymbol{b}}$, let $\boldsymbol{x}_0$ and $\boldsymbol{x}$ be their solutions, if $\|\boldsymbol{D} - \tilde{\boldsymbol{D}}\|\|\boldsymbol{D}^{-1}\| < 1$, then we have*

$$\frac{\|\boldsymbol{x} - \boldsymbol{x_0}\|}{\|\boldsymbol{x}_0\|} \leq \frac{\|\boldsymbol{D}\|\|\boldsymbol{D}^{-1}\|}{1 - \|\boldsymbol{D} - \tilde{\boldsymbol{D}}\|\|\boldsymbol{D}^{-1}\|} \left\{ \frac{\|\boldsymbol{D} - \tilde{\boldsymbol{D}}\|}{\|\boldsymbol{D}\|} + \frac{\|\boldsymbol{b} - \tilde{\boldsymbol{b}}\|}{\boldsymbol{b}} \right\}.$$

Denoting by $\boldsymbol{f} = (\boldsymbol{F}_{11}, \ldots, \boldsymbol{F}_{1n}, \ldots, \boldsymbol{F}_{n1}, \ldots, \boldsymbol{F}_{nn})^{\mathrm{T}}$ the row stack vector representation of $\boldsymbol{F}$, we can rewrite the perturbed system as $(\boldsymbol{D}+\boldsymbol{N})\boldsymbol{f} = \boldsymbol{b}$, and the original unperturbed system as $\boldsymbol{D}\boldsymbol{f} = \boldsymbol{b}$, with $\boldsymbol{D} = \mathrm{diag}\{\boldsymbol{D}_1, \ldots, \boldsymbol{D}_n\}$ being an $n^2 \times n^2$ block-diagonal matrix, where each $\boldsymbol{D}_i$ is an $n \times n$ block consisting of identity matrix with the ith row replaced by vector $\boldsymbol{v}^{\mathrm{T}}$. $\boldsymbol{N}$ is also an $n^2 \times n^2$ block-diagonal matrix with the $n \times n$ blocks $\boldsymbol{N}_i$ being a matrix with elements $(\boldsymbol{N}_i)_{jk} = s^i_{jk} + t^i_{jk} + w^i_{jk} + r_{ij}/n$. And $\boldsymbol{b}$ is an $n^2 \times 1$ vector with the $[(i-1)(n+1)+1]$-st element as v_i and other element as 0. Using Lemma 3.7 on the perturbed system and the unperturbed one with $\|\cdot\|$ taken as 2-norm (Euclidean norm), we obtain that

$$\|\boldsymbol{f} - \boldsymbol{f}_0\| \leq \|\boldsymbol{f}_0\| \frac{\|\boldsymbol{D}^{-1}\|\|\boldsymbol{N}\|}{1 - \|\boldsymbol{D}^{-1}\|\|\boldsymbol{N}\|}, \tag{3–19}$$

where $\boldsymbol{f}_0$ is the row stack vector representation of $\boldsymbol{I}$. Therefore, to derive the upper bound for the difference between $\boldsymbol{F}$ and $\boldsymbol{I}$, we need to further upper bound the RHS of Inequality (3–19). The technique we use here is harnessing the special structure of $\boldsymbol{D}$ and $\boldsymbol{N}$ so that we can derive bounds for $\|\boldsymbol{D}^{-1}\|$ and $\|\boldsymbol{N}\|$, which are represented in functions of variables $\{s\}, \{t\}, \{w\}$ and $\{r\}$. By further associating the variables with the spectral parameters $\delta, \epsilon_1, \epsilon_2$, etc. defined in the theorem, we yield an upper bound for the RHS of Inequality (3–19) that depends on those spectral parameters. For ease of illustration, we defer the detailed derivation of the upper bound to **Appendix A.3**.

Based on the upper bound, we have that if the conditions in the theorem are satis-

fied, then

$$\|\boldsymbol{F}-\boldsymbol{I}\|_{\mathrm{F}}=\|\boldsymbol{f}-\boldsymbol{f_0}\|\leq\frac{1}{2}.$$

Since $\|\mathbf{\Pi}^f-\hat{\mathbf{\Pi}}\|_{\mathrm{F}}=\|\boldsymbol{Q}\hat{\mathbf{\Pi}}-\hat{\mathbf{\Pi}}\|_{\mathrm{F}}=\|(\boldsymbol{Q}-\boldsymbol{I})\hat{\mathbf{\Pi}}\|_{\mathrm{F}}=\|\boldsymbol{Q}-\boldsymbol{I}\|_{\mathbf{F}}=\|\boldsymbol{F}-\boldsymbol{I}\|_{\mathbf{F}}\leq 1/2$, the entry-wise difference between $\mathbf{\Pi}^f$ and $\hat{\mathbf{\Pi}}$ is less than $1/2$. Thus, the projection process in **Algorithm 2** is bound to project $\mathbf{\Pi}_f$ as $\hat{\mathbf{\Pi}}$, which concludes the second step, i.e., the proof of Lemma 3.6. □

3. Optimality of $\hat{\mathbf{\Pi}}$: Now we proceed to the final step and prove that $\hat{\mathbf{\Pi}}=\mathbf{\Pi}^*$ by contradiction. If there exists some permutation matrix $\mathbf{\Pi}'\neq\hat{\mathbf{\Pi}}$ with $\|\mathbf{\Pi}'\tilde{\boldsymbol{A}}-\mathbf{\Pi}'\tilde{\boldsymbol{B}}\|_{\mathrm{F}}<\|\hat{\mathbf{\Pi}}\tilde{\boldsymbol{A}}-\hat{\mathbf{\Pi}}\tilde{\boldsymbol{B}}\|_{\mathrm{F}}$. Then, we consider $\tilde{\boldsymbol{B}}=\boldsymbol{B_0}+\boldsymbol{R'}$ with $\boldsymbol{B}_0=\mathbf{\Pi}'^{\mathrm{T}}\boldsymbol{A}\mathbf{\Pi}'$. Obviously, $\boldsymbol{R'}$ satisfies the conditions in Theorem 3.5.1. Hence, by Lemma 3.6, we should have that the the solution $\mathbf{\Pi}^p$ computed by **Algorithm 2** equals to $\mathbf{\Pi}'$. However, we also have $\mathbf{\Pi}^p=\hat{\mathbf{\Pi}}$, which leads to a contradiction. Thus, $\hat{\mathbf{\Pi}}$ is the optimal solution to $\boldsymbol{P3}$, which finishes the proof of the theorem. □

Time Complexity: In the first stage of **Algorithm 2**, we use the primal interior point algorithm proposed in [32] to solve the instance of $\boldsymbol{P3'}$, which has a time complexity of $O(N^3)=O(n^6)$ where $N=n^2$ is the number of variables in the instance. The projection process of the second stage can be implemented in $O(n^2)$ time. Thus, the total time complexity of **Algorithm 2** is $O(n^6)$. Note that the result only represents the running time of the algorithm in the worst case and the average time complexity of **Algorithm 2** is much lower [32].

Chapter 4 Unilateral De-anonymization

In this chapter, we investigate the de-anonymization problem with unilateral community information, i.e., when the adversary only possesses the community assignment function of the published network G_1. Following the path of the bilateral de-anonymization in Sections 3.1 and 3.2, we will give the corresponding results we obtain for the unilateral case. Through comparisons of these results and illustration in our later experiments, we demonstrate that de-anonymization with only unilateral community information is harder than that with bilateral community information, which shows the importance of community assignment as side information.

4.1 Analytical Aspect

Following the roadmap, we first present the results on the analytical aspect of the unilateral de-anonymization problem.

4.1.1 MAP-based Cost Function

We first derive our cost function in the unilateral case. Again, according to the definition of MAP estimation, given the published network G_1, auxiliary network G_2, parameters $\boldsymbol{\theta}$ and the community assignment function c of G_1, the MAP estimate $\hat{\pi}$ of the correct mapping π_0 is defined as:

$$\hat{\pi} = \arg\max_{\pi \in \Pi} Pr(\pi_0 = \pi \mid G_1, G_2, c, \boldsymbol{\theta}), \tag{4–1}$$

where Π denotes the set of all bijective mappings from V_1 to V_2. Note that in the unilateral case we have no prior knowledge of the community assignment of G_2. Consequently, we can not restrict Π to the set of mappings that observe the community

assignment constraints.

Due to the space limit, we omit the processing of the MAP estimator (4–1) and present the detailed steps in **Appendix A.4**. After a sequence of manipulations, we arrive at the following equation for calculation of the MAP estimate.

$$\begin{aligned}\hat{\pi} &= \arg\min_{\pi\in\Pi}\left\{\sum_{i<j}^{n} w_{ij}(\mathbb{1}\{(i,j)\notin E_1,(\pi(i),\pi(j)\in E_2)\})\right\}\\ &\triangleq \arg\min_{\pi\in\Pi}\Delta_{\pi},\end{aligned}$$

where $w_{ij} = \log\left(\frac{1-p_{c(i)c(j)}(s_1+s_2-s_1s_2)}{p_{c(i)c(j)}(1-s_1)(1-s_2)}\right)$. Note that different from the bilateral case, the cost function in the unilateral case is equivalent to a single-sided weighted edge disagreement induced by a mapping. This subtle difference has crucial implications to our analysis on the algorithmic aspect of unilateral de-anonymization.

4.1.2 Validity of the Cost Function

Following the same thread of thought, we proceed to justify the MAP estimation used in unilateral de-anonymization. Using similar proof technique, we derive the same result for the cost function in unilateral case as in bilateral one.

Theorem 4.1.1. *Let* $\alpha = \min_{ab} p_{ab}, \beta = \max_{ab} p_{ab}$, $\overline{w} = \max_{ij} w_{ij}$ *and* $\underline{w} = \min_{ij} w_{ij}$. *Assume that* $\alpha, \beta \to 0$, s_1, s_2 *do not go to 1 as* $n \to \infty$ *and* $\frac{\log\alpha}{\log\beta} \le \gamma$. *Furthermore, suppose that*

$$\frac{\alpha(1-\beta)^2 s_1^2 s_2^2 \log(1/\alpha)}{s_1+s_2} = \Omega\left(\frac{\gamma\log^2 n}{n}\right) + \omega\left(\frac{1}{n}\right),$$

then the MAP estimate $\hat{\pi}$ *in the unilateral case almost surely equals to the correct mapping* π_0 *as* $n \to \infty$.

Proof. The proof is basically identical to the proof of Theorem 3.1.1. The only difference here is that we redefine X_{ij} as a Bernoulli random variable with mean $p_{ij}s_1(1 - p_{\pi(i)\pi(j)}s_2)$ and Y_{ij} as a Bernoulli random variable with mean $p_{ij}s_1(1-s_2)$. Then, by using the same bounding technique for $Pr\{X_\pi - Y_\pi \le 0\}$, we conclude the same result for the cost function in unilateral case. □

Theorems 3.1.1 and 4.1.1 show that the cost function based on MAP estimation is equally effective in de-anonymization with bilateral and unilateral community information. However, as we will show in the sequel, the feasibility of the cost function in unilateral case is weaker than in bilateral case.

4.2 Algorithmic Aspect

In this section, we investigate the algorithmic aspect of de-anonymization with unilateral community information and propose corresponding algorithms as in the bilateral case.

4.2.1 The Unilateral MAP-ESTIMATE Problem

We first formally introduce the combinatorial optimization problem induced by minimizing the cost function in unilateral de-anonymization.

Definition 4.2.1. **(The UNI-MAP-ESTIMATE Problem)** Given two graphs $G_1(V, E_1, \boldsymbol{A})$ and $G_2(V, E_2, \boldsymbol{B})$, community assignment function c of G_1 and weights $\{w\}$, the goal is to compute a mapping $\hat{\pi} : V_1 \mapsto V_2$ that satisfies

$$\begin{aligned}\hat{\pi} &= \arg\min_{\pi\in\Pi} \left\{ \sum_{i<j}^{n} w_{ij}(\mathbb{1}\{(i,j) \notin E_1, (\pi(i),\pi(j)) \in E_2)\} \right\} \\ &\triangleq \arg\min_{\pi\in\Pi} \Delta_\pi,\end{aligned}$$

where $\Pi = \{\pi : V_1 \mapsto V_2\}$.

Similar to the bilateral de-anonymization, we require the weights $\{w\}$ to be induced by well-defined community affinity values $\{p\}$, s_1 and s_2, though the latter ones are not explicitly given. Due to the asymmetry of Δ_π in unilateral de-anonymization, intuitively, the UNI-MAP-ESTIMATE problem may bear higher approximation hardness than the BI-MAP-ESTIMATE problem in bilateral de-anonymization. The proposition we present below consolidates this intuition.

Proposition 4.3. *UNI-MAP-ESTIMATE problem is NP-hard. Moreover, there is no polynomial time (pseudo polynomial time) approximation algorithm for UNI-MAP-ESTIMATE with any multiplicative approximation guarantee unless* $P = NP$ *(*$NP \in DTIME(n^{\text{polylog}n})$*).*

Proof. The proof is done by reduction from k-CLIQUE problem. Given a graph $G(V, E)$, the k-CLIQUE problem asks whether there exists a clique of size no smaller than k in G. The main idea of the reduction is that: Given an instance of k-CLIQUE with $G(V, E)$ and k, we set G_1 as G and G_2 as a graph consisting of a clique of size k and $(|V| - k)$ additional nodes. Setting $w_{ij} = 1$ and $c(v) = 1$ for all v in G_1, we have an instance of UNI-MAP-ESTIMATE. Obviously, if the G contains a clique of size no less than k, the value $\Delta_{\hat{\pi}}$ of the optimal mapping $\hat{\pi}$ in UNI-MAP-ESTIMATE will be zero. Therefore, in this case, any algorithm with multiplicative approximation guarantee must find a mapping π with $\Delta_\pi = 0$. Furthermore, if G does not contain a clique of size no smaller than k, then any mapping π must satisfy $\Delta_\pi > 0$. Hence, a polynomial (pseudo-polynomial) time approximation algorithm for BI-MAP-ESTIMATE with multiplicative guarantee implies a polynomial (pseudo-polynomial) time algorithm for k-CLIQUE. Since k-CLIQUE problem is NP-Complete, we justify the approximation hardness of UNI-MAP-ESTIMATE as stated in the proposition. □

Note that the graph isomorphism problem is at least as hard as the problems in P, which implies that the approximation hardness result for UNI-MAP-ESTIMATE is stronger than that for BI-MAP-ESTIMATE.

4.2.2 Approximation Algorithms

4.2.2.1 Additive Approximation Algorithm

We design a similar approximation algorithm with an ϵ-additive approximation guarantee as in the bilateral case, by formulating the UNI-MAP-ESTIMATE problem

in quadratic assignment fashion as follows

$$\begin{aligned} \text{minimize } & \textstyle\sum_{i,j,k,l} q_{ijkl} x_{ik} x_{jl} && (4\text{–}2)\\ \textbf{s.t. } & \textstyle\sum_i x_{ij} = 1, \quad \forall i \in V_1 && (4\text{–}3)\\ & \textstyle\sum_j x_{ij} = 1, \quad \forall j \in V_2 && (4\text{–}4)\\ & x_{ij} \in \{0,1\} && (4\text{–}5) \end{aligned}$$

with the coefficients $\{q\}_{ijkl}$ of the formulation defined as:

$$q_{ijkl} = \begin{cases} w_{ij}, & \text{if } (i,j) \notin E_1, (k,l) \in E_2 \\ 0 & \text{otherwise.} \end{cases}$$

Note that due to the absence of community assignment constraints, we can directly formulate the problem as a minimization one and omit the penalty factor as in bilateral de-anonymization. By invoking the same QA-Rounding procedure on the formulated instance and convert the resulting solution $\{x\}$ to its equivalent mapping π. Using similar analysis technique as in Section 3.2.2.1, we have that the algorithm obtains solutions that have a gap of at most ϵn^2 to the optimal ones in time $O(n^{O(\log n/\epsilon^2)} + n^2)$. Although the QAP formulation of unilateral de-anonymization is less complicated in form, this does not imply that unilateral de-anonymization is easier than its bilateral counterpart, as the performance of the approximation algorithms proposed are the same. Actually, in the following, we conceptually show that the opposite, i.e., unilateral de-anonymization is harder than bilateral one, is true.

4.2.2.2 Convex Optimization Based Heuristic

We now proceed to present the heursitc based on convex optimization for the UNI-MAP-ESTIMATE problem, which relies on the following matrix formulation.

$$\begin{aligned} \text{mininize } & \|\boldsymbol{W} \circ (\boldsymbol{\Pi}\boldsymbol{A} - \boldsymbol{B}\boldsymbol{\Pi})\|_{\lfloor \mathrm{F} \rfloor}^2 \\ \textbf{s.t. } & \forall i \in V_1,\ \textstyle\sum_i \boldsymbol{\Pi}_{ij} = 1 && (4\text{–}6) \\ & \forall j \in V_2,\ \textstyle\sum_j \boldsymbol{\Pi}_{ij} = 1 && (4\text{–}7) \\ & \forall i, j,\ \boldsymbol{\Pi}_{ij} \in \{0, 1\}, && (4\text{–}8) \end{aligned}$$

where $\boldsymbol{W}$ and $\circ$ share the same definitions as those in $\boldsymbol{P3}$ and $\|\cdot\|_{\lfloor \mathrm{F} \rfloor}$ is defined to be a variant of Frobenius norm. Specifically, $\|\boldsymbol{M}\|_{\lfloor \mathrm{F} \rfloor} = \sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n}(\mathbb{1}\{\boldsymbol{M}_{ij} \leq 0\}\boldsymbol{M}_{ij}^2)}$ for a matrix $\boldsymbol{M}$, where only negative elements contribute to the value of the norm[1]. By relaxing the integral constraint (4–8), we again arrive at an optimization problem, which is shown to be convex in **Appendix A.5**. Our second algorithm for unilateral de-anonymization is to first solve the relaxed version of the matrix formulation of UNI-MAP-ESTIMATE and then project the fractional solution to an integral one. Unfortunately, due to the asymmetry of the operator $\|\cdot\|_{\lfloor \mathrm{F} \rfloor}$, it is difficult to derive closed form expression for the gradient of the Lagrangian function of UNI-MAP-ESTIMATE. Thus, we cannot prove conditional optimality of the algorithm as we did in bilateral case.

We provide a summary of the differences existing in bilateral and unilateral de-anonymizations from a higher level as follows.

- The extra knowledge on the community assignment function in bilateral de-anonymization enables us to restrict the feasible mappings to the ones that observe the community assignment, thus decreases the number of possible candidates and makes the problem intuitively easier than unilateral one.

- The community assignment as side information is the main reason behind the difference of the posterior distribution of the optimal mapping, which leads to different MAP estimates, and thus different cost functions in the two cases. Note

[1] It is easy to verify that operator $\|\cdot\|_{\lfloor \mathrm{F} \rfloor}$ satisfies the definition of norm.

that the cost function for bilateral de-anonymization cannot be calculated in unilateral case since we have no knowledge on the community assignment of G_2.

- Although under similar conditions, minimizing the cost function asymptotically almost surely recovers the correct mapping in both cases, the lack of community assignment in unilateral de-anonymization impose asymmetry in its cost function and render the cost function harder to (approximately) minimize, as justified by our stronger complexity-theoretic result.

- In terms of the proposed algorithms, the additive approximation algorithms for both bilateral and unilateral de-anonymization share the same guarantee. However, the convex optimization-based algorithm has been shown to yield conditionally yield optimal solutions only for bilateral de-anonymization.

- The empirical results demonstrate that in all the contexts, our algorithms successfully de-anonymize larger portion of users when provided with bilateral community information.

Chapter 5 Experiments

5.1 Experiments

In this section, we present our experimental validation of our theoretical results and the performances of the proposed algorithms. We first introduce our experimental settings and provide detailed results subsequently.

5.1.1 Experimental Settings

5.1.1.1 Experiment Datasets

Recall that the two key assumptions made in the modeling are that the underlying social network is generated by the stochastic block model and that the published and the auxiliary networks are sampled from the underlying network. To validate our theoretical findings and meanwhile evaluate the proposed algorithms in real contexts, we conduct experiments on three different types of data sets, with each one closer to the practical situations than the last one by gradually relaxing the assumptions.

(i) **Synthetic Dataset:** Following the stochastic block model, we generate three sets of networks with Poisson, power law and exponential expected degree distributions respectively by properly assigning the community affinity values $\{p\}$. The size of each community is determined by adding a slight variation to the average community size, which equals to the number of nodes divided by the number of communities. For each set of networks, we take the sampling probabilities of the published and the auxiliary networks as $s_1 = s_2$ ranging from 0.3 to 0.9. As this dataset strictly observes the assumptions of our models, it provides direct validations to our theoretical results.

(ii) **Sampled Social Networks:** The underlying social networks are extracted from LiveJournal online social network [33], with the communities following from the ground-truth communities in LiveJournal and the affinity values assigned to be

proportional to the ratio of the edges between the communities over the number nodes in the communities. The published and the auxiliary networks are sampled from the underlying networks, again, with the sampling probabilities $s_1 = s_2$ ranging from 0.3 to 0.9. This "semi-artificial" dataset lies in the middle of synthetic datasets and true cross-domain networks, which enables us to measure the robustness of our theoretical results against the restrictions imposed on the underlying social network.

(iii) **Co-authorship Networks:** We extract four co-authorship networks in different areas from Microsoft Academic Graph (MAG) [20]. From those, we construct a group of networks with equivalent sets of nodes (2053 nodes in each set) and set up the correspondence of nodes as ground-truth based on the unique identifiers of authors in MAG. The communities are assigned based on the institution information of the authors (the affinity values in this case are assigned as in Sampled Social Networks). The four networks are then combined into six pairs, in which one is set as the published network and the other as the auxiliary network. Without relying on any artificial assumptions on how the published and auxiliary networks are generated, these procedures enable us to construct most genuine scenarios of de-anonymization from cross-domain social networks. This key feature renders the dataset a touchstone for the applicability of our proposed algorithms.

(iv) **Xinzhe's Ego Networks:** We extract two small ego networks of 29 users from Xinzhe Fu's (The First Author) Wechat and Weibo data. The edges in both networks represent "friend" relation (two-way following in the case of Weibo). We partition the users into four communities based on prior knowledge such as high school classmates, college classmates, labmates, etc. The data were collected under the consent of the involved users and do not violate the users' privacy. The networks are encoded as undirected graphs. The Weibo network has 29 nodes and 42 edges while the Wechat network has 29 nodes and 107 edges.

Note that our empirical results in the first two datasets are respectively obtained by taking the average from 50 repetitive experiments. The statistics of the first three datasets are summarized in Table 5–1.

Dataset	Degree Distribution	Source	# of Nodes	# of Edges	# of Communities
Synthetic Networks	power law	synthetic	500-2000	≈500-100000	10-40
	Poisson	synthetic	500-2000	≈500-100000	10-40
	exponential	synthetic	500-2000	≈500-100000	10-40
Sampled Social Networks		SNAP[1]	500-2000	≈1000-40000	10-40
Co-authorship Networks		MAG[20]	≈ 2000	≈ 8000	≈ 60

Table 5–1: **Summary of datasets in experiments**

5.1.1.2 Algorithms Involved in Comparisons

For both bilateral and unilateral de-anonymization, we run genetic algorithm (**GA-BI,GA-UNI**) in hope of finding exact minimizer of our cost functions, i.e., the optimal solution of BI-MAP-ESTIMATE and UNI-MAP-ESTIMATE problems. In both de-anonymization cases, we also evaluate the performance of our two proposed algorithms: the additive approximation algorithm (**AA-BI,AA-UNI**) and the convex optimization-based algorithm (**CO-BI,CO-UNI**).

5.1.1.3 Performance Metrics

The two performance metrics we calculate in the experiments are the **accuracy** of the mappings yielded by the algorithms and the values of the cost function Δ_π of the mappings. The accuracy of a mapping π is defined as the portion of the nodes that π maps correctly (as the ground-truth correct mapping) over the total number of nodes. Since we are not interested in the absolute values of the cost function of the mapping, we calculate the **relative value** with respect to the cost function of the mappings produced by **GA**, i.e., for a mapping π and the mapping π_{GA} produced by **GA**, π's relative value is computed as $(\Delta_\pi - \Delta_{\pi_{GA}})/\Delta_{\pi_{GA}}$. Due to space limitations, we defer all the graphical representations of results on the mappings' cost function to **Appendix 5.2**.

5.1.2 Experiment Results

5.1.1.1 Synthetic Networks

We plot the performance of the aforementioned algorithms on synthetic networks with $\{500, 1000, 1500, 2000\}$ number of nodes in Figures 5–1 and 5–4, based on which

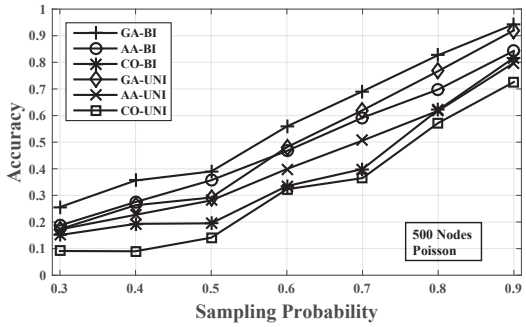
we have the following observations: (i) Both **GA-BI** and **GA-UNI** exhibit good performance, achieving a de-anonymization accuracy close to 1 when the sampling probability is large in networks with Poisson and power law degree distribution; (ii) The relative value of the correct mapping (**TRUE-BI,TRUE-UNI**) is fairly small. Hence, we conclude that, when the sampling probability is large, the cost function based on MAP estimation is an effective metric in both bilateral and unilateral de-anonymization, and is applicable to a wide range of degree distribution, which justify our theoretical results on the validity of the MAP estimate. However, when the sampling probability is small (e.g. $s = 0.3, 0.4$) or the expected degree distribution has large variation (exponential distribution), the accuracy of **GA** degrades substantially, only achieving a value of less than 0.4. This can be attributed to the fact that when the sampling probability becomes small, the published and the auxiliary networks have lower degree of structural similarity and the parameters deviate from the conditions in our theoretical results.

In terms of the two algorithms we propose, we can see that they obtain good performance with respect to both approximately minimizing the cost function and unraveling the correct mapping, with **AA** superior than **CO** especially in low-sampling-probability area. Note that although the relative value of the two algorithms is large in high-sampling-probability area, this does not imply the poor performance of the algorithms but is mainly due to the optimal Δ_π becoming considerably small as the similarity of G_1 and G_2 grows high.

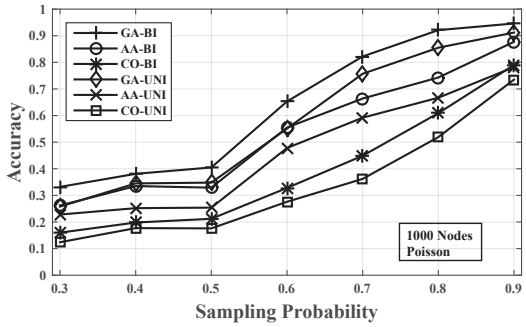
5.1.1.2 Sampled Social Networks

Figures 5–2 and 5–5 plot our empirical results on the second datasets where the published and auxiliary networks are sampled from real social networks with the number of nodes set as $\{500, 1000, 1500, 2000\}$.

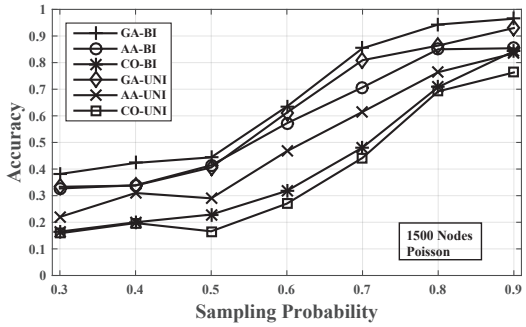
As demonstrated by Figures 5–2 and 5–5, although in this case the underlying social networks do not follow the stochastic block model, through minimizing the cost function we can still reveal a large proportion (up to 80%) of the correct mapping, which demonstrates the robustness of the cost function we proposed. Furthermore, the two algorithms **AA** and **CO** still achieve reasonable accuracy of up to 0.7, which is not surprising due to that the cost function they seek to minimize is still effective in


GA-BI
AA-BI
CO-BI
GA-UNI
AA-UNI
CO-UNI
Accuracy
Sampling Probability
500 Nodes
Poisson

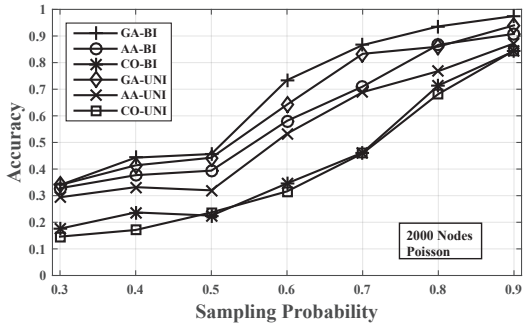
(a)


GA-BI
AA-BI
CO-BI
GA-UNI
AA-UNI
CO-UNI
Accuracy
Sampling Probability
1000 Nodes
Poisson

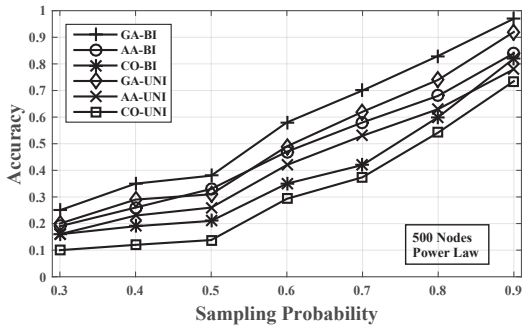
(b)


GA-BI
AA-BI
CO-BI
GA-UNI
AA-UNI
CO-UNI
Accuracy
Sampling Probability
1500 Nodes
Poisson

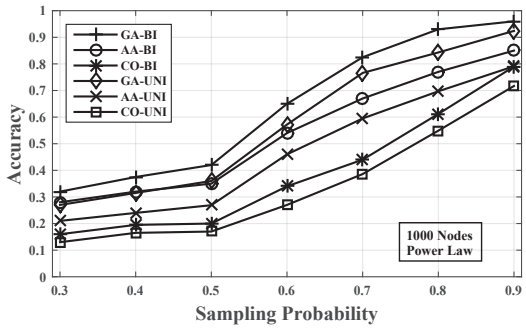
(c)


GA-BI
AA-BI
CO-BI
GA-UNI
AA-UNI
CO-UNI
Accuracy
Sampling Probability
2000 Nodes
Poisson

(d)


GA-BI
AA-BI
CO-BI
GA-UNI
AA-UNI
CO-UNI
Accuracy
Sampling Probability
500 Nodes
Power Law

(e)


GA-BI
AA-BI
CO-BI
GA-UNI
AA-UNI
CO-UNI
Accuracy
Sampling Probability
1000 Nodes
Power Law

(f)

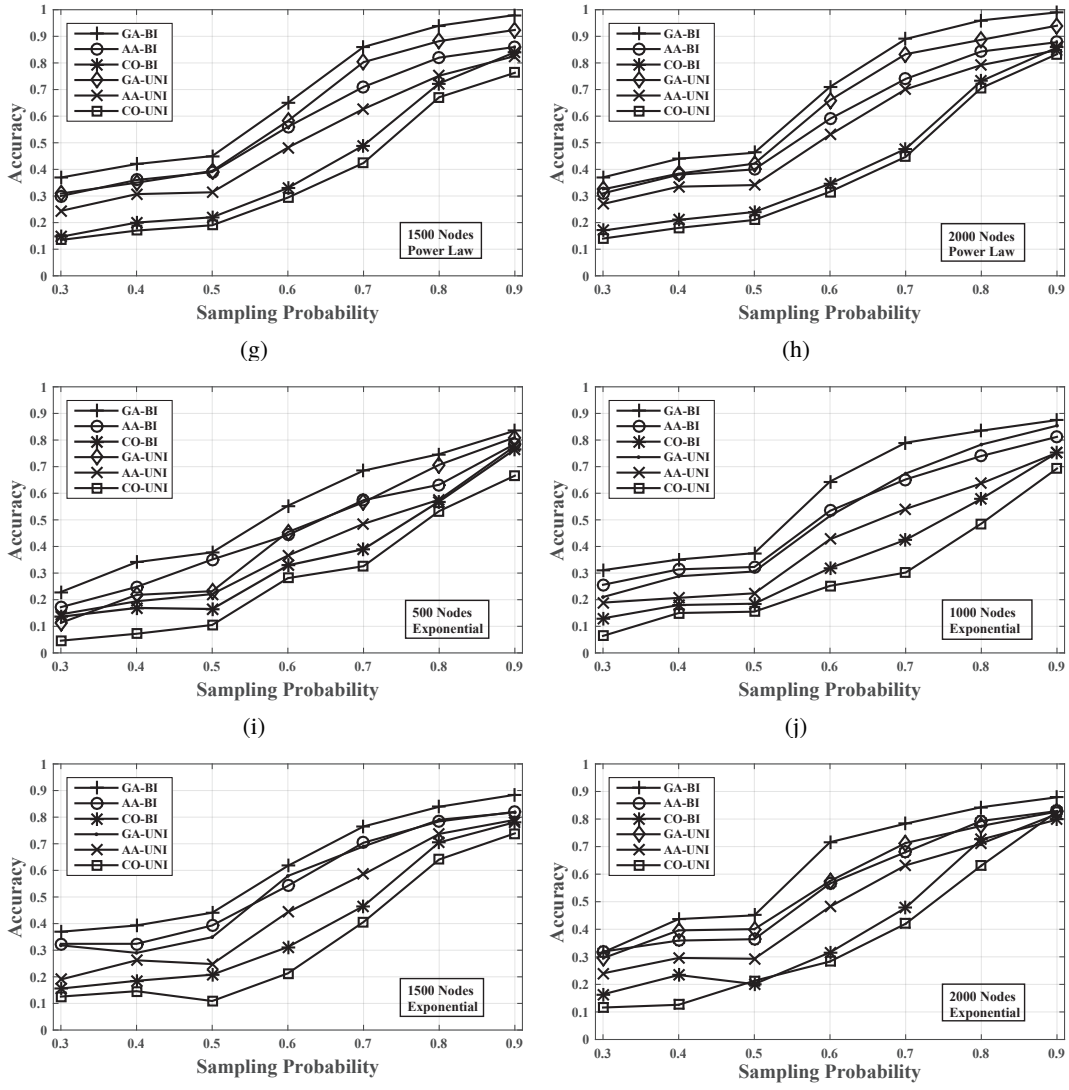


Figure 5–1: **The accuracy of the algorithms on synthetic datasets with different degree distributions.**

this case. However, a little defect is that the accuracy of **AA** can be higher than **GA** at some points. This reflects that the deviation of the real life social networks from the stochastic block model more or less influences the quality of the MAP estimate.

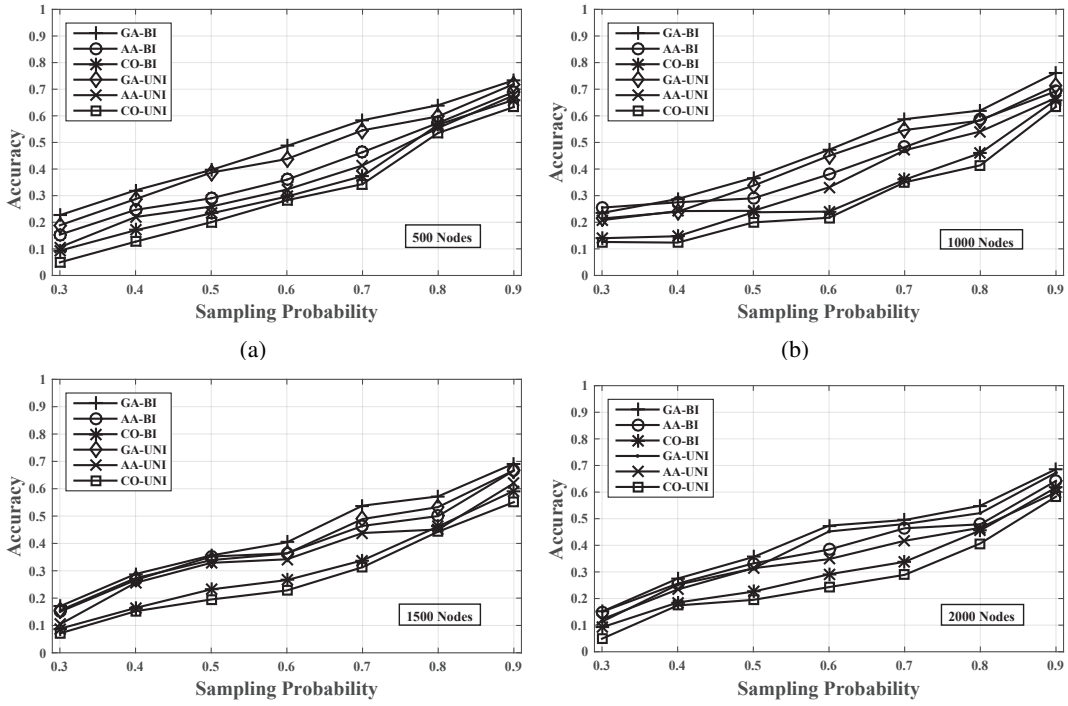


Figure 5–2: **The accuracy of the algorithms on Sampled Social Networks**

5.1.1.3 Cross-domain Co-authorship Networks

As stated in experimental setup, we extract four groups of cross-domain co-authorship networks named as Networks A, B, C, D and thus construct six scenarios for social network de-anonymization[1]. We evaluate the performance of the algorithms on the six scenarios and show the results in Figures 5–3 and 5–6. The figures present several observations and implications: (i) the proposed cost functions still serve as meaningful media for recovering the correct mapping even in realistic scenarios as the relative value of the correct mapping is close to zero and **GA** achieves an average accuracy of 67.3% in bilateral case and 59.0% in unilateral case; (ii) The two proposed algo-

[1]We do not distinguish the interchange of the published and auxiliary networks as different scenarios.

rithms still enjoy reasonable accuracy, with **AA** successfully de-anonymizing 60.8% of nodes in bilateral case and 51.5% of nodes in unilateral case, and **CO** successfully de-anonymizing 44.4% of nodes in bilateral case and 35.9% of nodes in unilateral case. Therefore, the two algorithms can be qualified as effective methods for seedless social network de-anonymization, which implies that the privacy of current anonymized networks still suffers from attacks of adversaries even when pre-mapped seeds are unavailable; (iii) The performance of **CO** is most susceptible to the structure of networks among all three algorithms as the standard deviation of its accuracy on the six scenarios are above 3.5% (3.51% for **CO-BI**, 3.81% for **CO-UNI**) while the counterparts of the other two algorithms are below 3.0%.

5.1.1.4 Xinzhe's Ego Networks

According to our experiment results, it turns out that on this set of practical but small datasets, the proposed de-anonymization algorithms has non-trivial mapping accuracy. The accuracies of **GA, AA** and **CO** are 27.6%, 20.6%, 13.7% respectively, which are much higher than random guessing. However, the accuracies are much lower than previous ones, which is mainly due to the peculiarity and sparsity of Xinzhe's ego network. An important implication is that we can actually use the proposed algorithm to construct correspondence between a user's Wechat account and Weibo account, raising privacy issues and also interesting side-effects.

5.1.1.5 Significance of Community Information

A notable phenomenon from all the experiments is that the accuracy of the algorithms in bilateral de-anonymization is higher than that in unilateral de-anonymization, especially for **AA** and **CO**. According to the experimental results, the gap is at least 3.5% in each setting and can reach up to 15% in the worst case. This, from an empirical point of view, demonstrates the importance of the community information on social network de-anonymization.

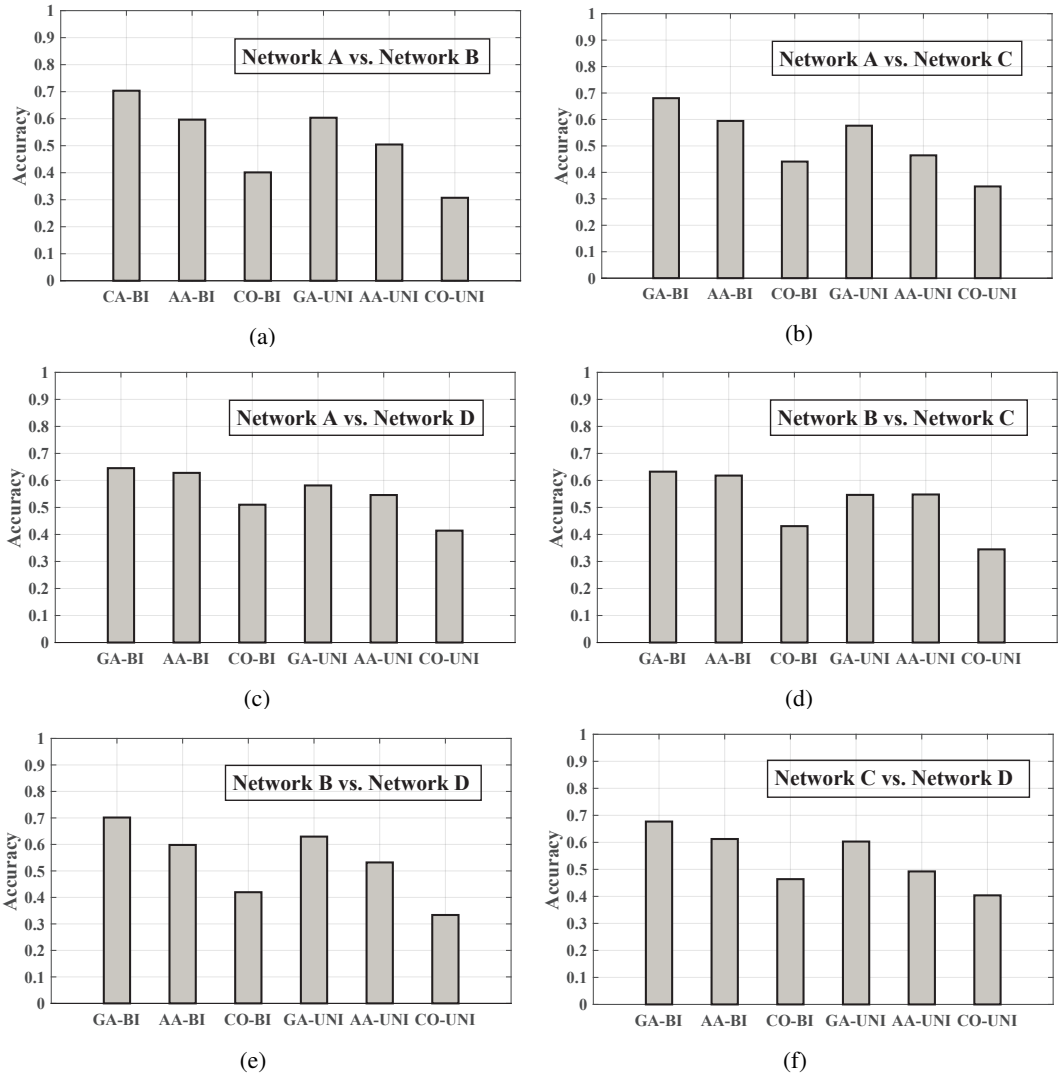
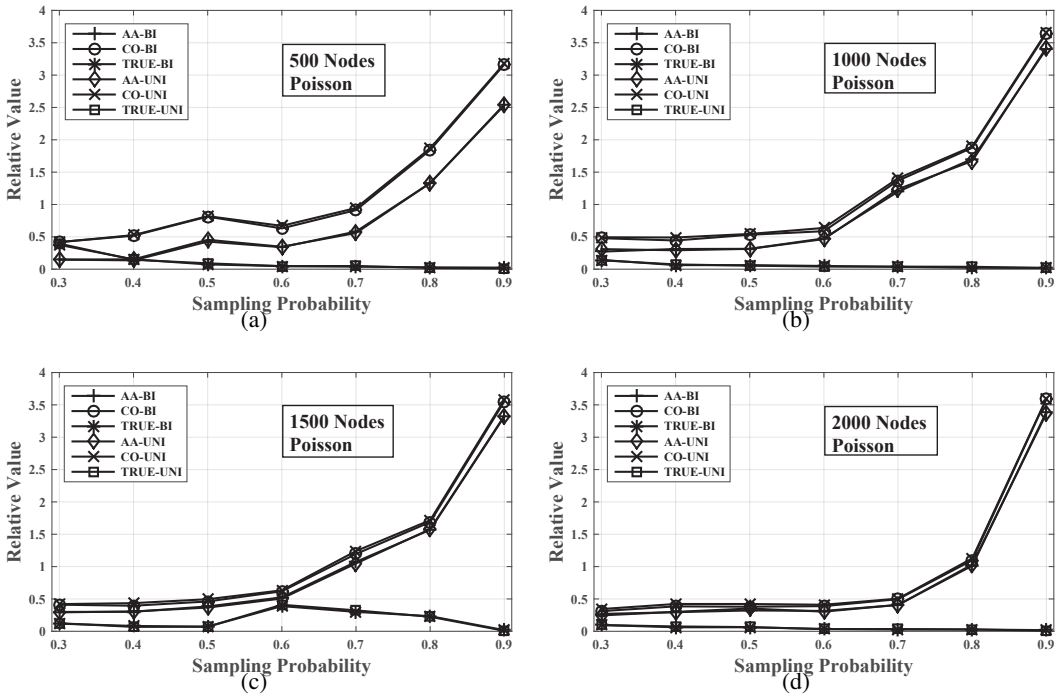


Figure 5–3: **The accuracy of the algorithms on Cross-domain Co-authorship Networks**

5.2 Supplementary Experiment Results

In this section we present graphical results on the relative value of the cost function of the mappings produced by the algorithms. Recall that for a mapping π and the mapping π_{GA} produced by **GA** algorithm, the relative value of the cost function of π equals to $(\Delta_\pi - \Delta_{\pi_{GA}})/\Delta_{\pi_{GA}}$.

Figures 5–4, 5–5 and 5–6 demonstrate the results on the relative value of cost function produced by mappings in the synthetic datasets, sampled social networks and cross-domain co-authorship networks respectively.



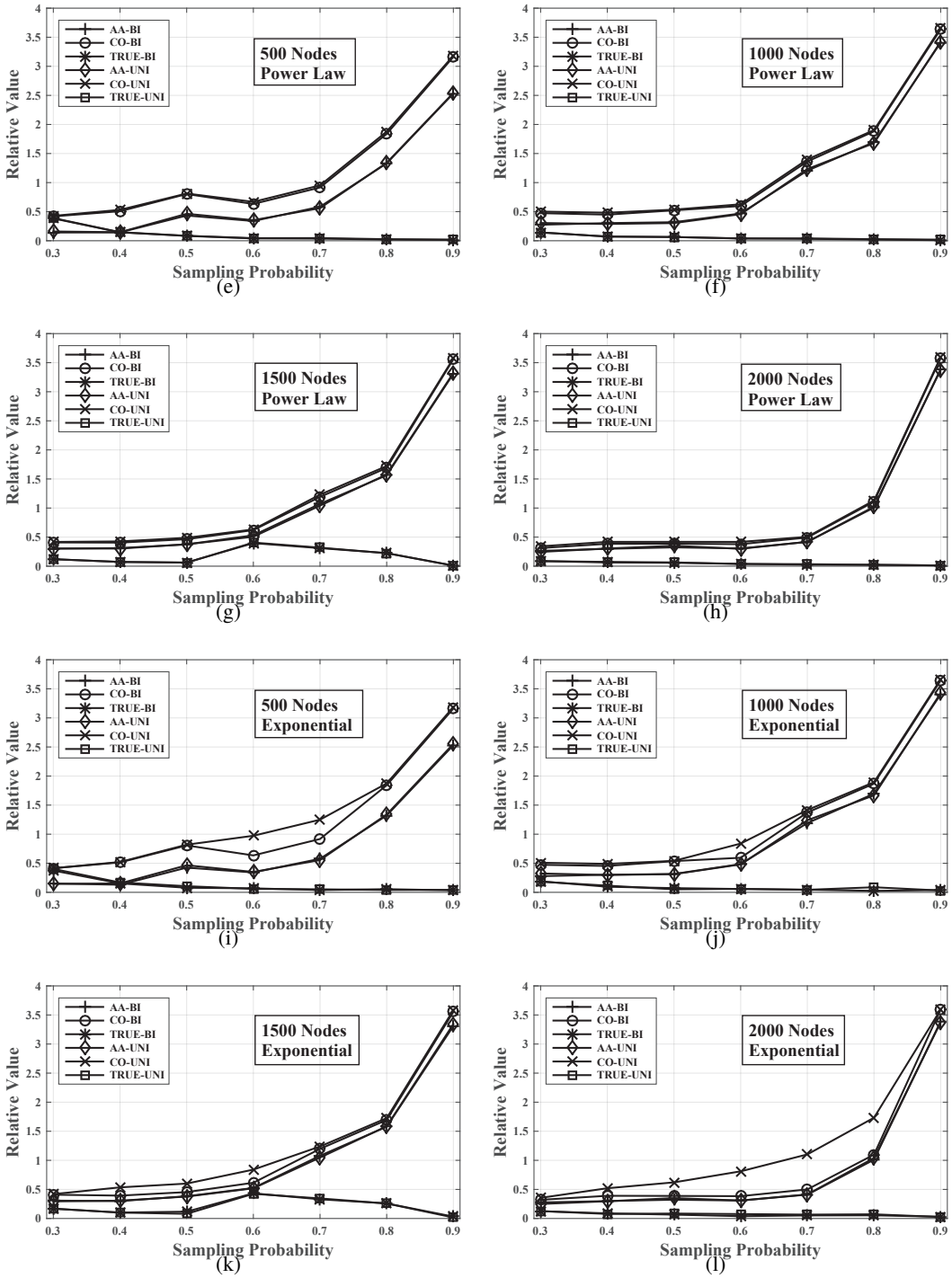


Figure 5–4: **The relative value of the cost function of the mappings produced by the algorithms on synthetic datasets with different degree distributions.**

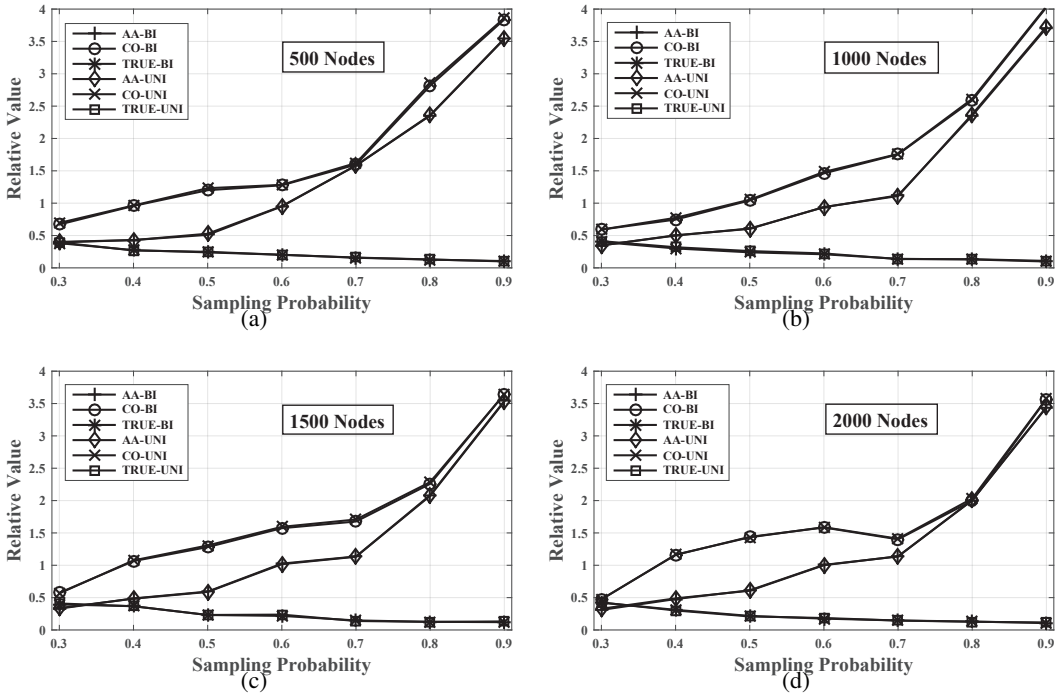
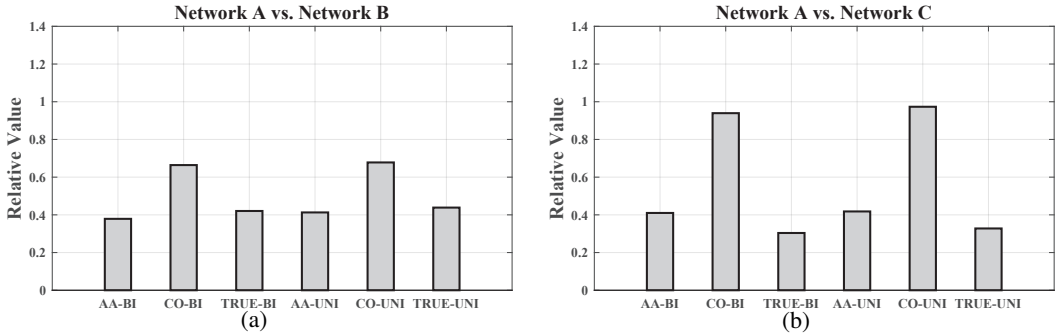


Figure 5–5: **The relative value of the cost function of the mappings produced by the algorithms on Sampled Social Networks**



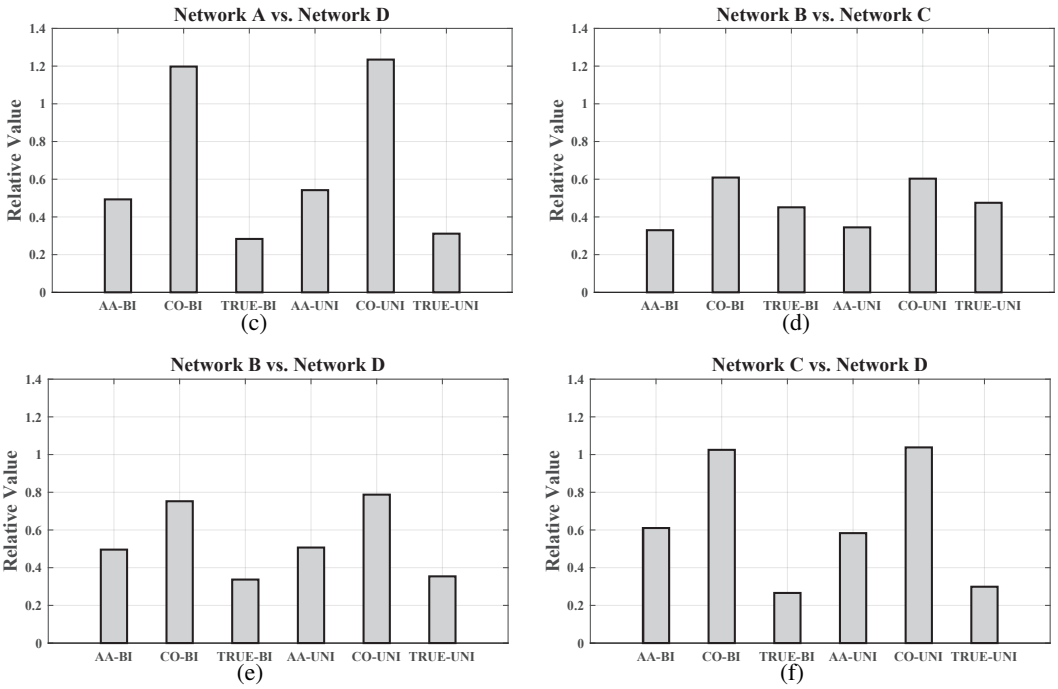


Figure 5–6: **The relative value of the cost function of the mappings produced by the algorithms on Cross-domain Co-authorship Networks**

Chapter 6 Conclusion

In this paper, we have presented a comprehensive study of the community-structured social network de-anonymization problem. Integrating the clustering effect of underlying social network in our models, we have derived a well-justified cost function based on MAP estimation. To further consolidate the validity of such cost function, we have shown that under certain mild conditions, the minimizer of the cost function indeed coincides with the correct mapping. Subsequently, we have investigated the feasibility of the cost function algorithmically by first proving the approximation hardness of the optimization problem induced by the cost function and then proposing two algorithms with their respective performance guarantee by resolving the interweaving of cost function, network topology and candidate mappings through relaxation techniques. All our theoretical findings have been empirically validated through both synthetic and real datasets, with a notable dataset being a set of rare true cross-domain networks that reconstruct a genuine context of social network de-anonymization.

Appendix A Supplementary Technical Materials

A.1 Proof of Theorem 4.1

The method we use here is similar to that in [8]. Recall that for a mapping π, we define $\Delta_\pi = \sum_{i\le j}^{n} w_{ij}|\mathbb{1}\{(i,j) \in E_1\} - \mathbb{1}\{\pi(i),\pi(j) \in E_2\}|$. Then the proof can be briefly divided into two major steps. The first one is to derive an upper bound for the expectation of the number of (incorrect) mappings π's with $\Delta_\pi \le \Delta_{\pi_0}$. The second one is to show that the derived upper bound converges to 0 under the conditions stated in the theorem, as $n \to \infty$. Based on that, the proof can be concluded as the number of π's with $\Delta_\pi \le \Delta_{\pi_0}$ goes to 0, i.e., the correct mapping π_0 is th unique minimizer for Δ_π as $n \to \infty$. Now we turn to the first step as follows:

1. **Derivation of the Upper Bound:** We define Π_k as the set of all the mappings in Π that map k nodes incorrectly. Obviously, $\Pi_0 = \{\pi_0\}$. Now we have $|\Pi_k| \le \binom{n}{k}\left(\frac{k!}{2}\right) \le n^k$. We subsequently define S_k as a random variable representing the number of incorrect mappings in Π_k whose value of cost function is no larger than Δ_{π_0}. Formally, S_k is given by $S_k = \sum_{\pi\in\Pi_k} \mathbb{1}\{\Delta_\pi \le \Delta_{\pi_0}\}$. Summing over all k, we denote $S = \sum_{k=2}^{n} S_k$ as the total number of incorrect mappings that induce no larger cost function than the correct mapping π_0. The mean of S can be calculated as:

$$\begin{aligned}\mathbb{E}[S] &= \sum_{k=2}^{n} \mathbb{E}[S_k] = \sum_{k=2}^{n}\sum_{\pi\in\Pi_k} \mathbb{E}[\mathbb{1}\{\Delta_\pi \le \Delta_{\pi_0}\}] \\ &= \sum_{k=2}^{n}\sum_{\pi\in\Pi_k} Pr\{\Delta_\pi - \Delta_{\pi_0} \le 0\} \\ &\le \sum_{k=2}^{n} n^k \max_{\pi\in\Pi_k} Pr\{\Delta_\pi - \Delta_{\pi_0} \le 0\}. \end{aligned} \tag{A–1}$$

For a mapping π, let V_π be the set of vertices that it maps incorrectly. Then, we define $E_\pi = V_\pi \times V$, i.e., the set of node pairs with one or two vertices mapped

incorrectly under π. For a $\pi \in \Pi_k$, we have $|E_\pi| = nk - \frac{k^2}{2} - \frac{k}{2}$. As every node pair in $V \times V - E_\pi$ is mapped identically in π and π_0, they contribute equally to Δ_{π_0} and Δ_π respectively. Next, we define two random variables for π as

$$X_\pi = \sum_{(i,j)\in E_\pi} w_{ij} |\mathbb{1}\{(i,j) \in E_1\} - \mathbb{1}\{(\pi(i), \pi(j) \in E_2\}|,$$
$$Y_\pi = \sum_{(i,j)\in E_\pi} w_{ij} |\mathbb{1}\{(i,j) \in E_1\} - \mathbb{1}\{(i,j) \in E_2\}|.$$

It is easy to verify that $\Delta_\pi - \Delta_{\pi_0} = X_\pi - Y_\pi$ for all π, where Y_π is the value of cost function contributed by node pairs in E_π under the correct permutation. For a node pair (i,j), the probability that it contributes to Y_π equals to $p_{c(i)c(j)}(s_1 + s_2 - 2s_1s_2)$. Therefore, Y_π is the weighted sum of independent Bernoulli random variables.

For X_π, assume that π has $\phi \geq 0$ transpositions[1], then each transposition induces one invariant node pair in E_π. The remaining node pairs are not invariant under π, i.e., they are mapped incorrectly under π. Each node pair (i,j) contributes w_{ij} to X_π if $(i,j) \in E_1$ and $(\pi(i), \pi(j)) \notin E_2$ or vice versa. This happens with probability $p_{c(i)c(j)}(s_1 + s_2 - 2p_{c(i)c(j)}s_1s_2)$. Note that the random variable for each node pair is not independent. As in [8], we conservatively ignore the positive correlation and get a lower bound of X_π, which is the weighted sum of independent random Bernoulli variables. Also, since transpositions in π can only occur in nodes in V_π, we have that $\phi \leq k/2$. Now, denote X_{ij} as a Bernoulli random variable with mean $p_{c(i)c(j)}(s_1+s_2-2p_{c(i)c(j)}s_1s_2)$ and Y_{ij} as a Bernoulli random variable with mean $p_{c(i)c(j)}(s_1+s_2-2s_1s_2)$ as Y_{ij}. Based on the above manipulations, we can get a lower bound of X_π and an upper bound of Y_π as follows:

$$X_\pi \overset{\text{(stoch.)}^2}{\geq} \sum_{(i,j)\in E_\pi \setminus \phi} w_{ij} X_{ij} \triangleq X'_\pi$$
$$Y_\pi \overset{\text{(stoch.)}}{\leq} \sum_{(i,j)\in E_\pi} w_{ij} Y_{ij} \triangleq Y'_\pi.$$

[1]If a mapping π has a transposition on i, j, it means that $\pi(i) = j$ and $\pi(j) = i$.

Therefore, we can use the probability of event $\{X_{\pi'} - Y_{\pi'}\} \leq 0$ to upper bound the probability of event $\{X_\pi - Y_\pi\} \leq 0$. Denoting λ_X as the expectation of X'_π and λ_Y as the expectation of Y'_π, the bound we use for $Pr\{X_\pi - Y_\pi \leq 0\}$ is summarized in the following lemma.

Lemma A.2. *For all mapping π, random variables X_π and Y_π satisfy that*

$$Pr\{X_\pi - Y_\pi \leq 0\} \leq 2\exp\left(\frac{-(\lambda_X - \lambda_Y)^2}{12(\lambda_X + \lambda_Y)}\right) \tag{A–2}$$

Proof. First, we have that for all π

$$\begin{aligned} Pr\{X_\pi - Y_\pi \leq 0\} &\leq Pr\{X'_\pi - Y'_\pi \leq 0\} \\ &\leq Pr\left\{Y'_\pi \geq \frac{\lambda_X + \lambda_Y}{2}\right\} + Pr\left\{X'_\pi \leq \frac{\lambda_X + \lambda_Y}{2}\right\} \end{aligned}$$

Then we invoke Lemma A.3 (Theorems 1 and 2 in [36]), which presents Chernoff-type bounds for weighted sum of independent Bernoulli variables.

Lemma A.3. *(Theorems 1 and 2 in [36]) Let $a_1, a_2, \ldots, a_r$ be positive real numbers and let $X_1, \ldots, X_n$ be independent Bernoulli trials with $\mathbb{E}[X_j] = p_j$. Defining random variable $\Psi = \sum_{j=1}^r a_j X_j$ with $\mathbb{E}[\Psi] = \sum_{j=1}^r a_j p_j = m$, we have*

$$\begin{aligned} Pr\{\Psi \geq (1+\delta)m\} &\leq \exp\left(-m\delta^2/3\right), \\ Pr\{\Psi \leq (1-\delta)m\} &\leq \exp\left(-m\delta^2/2\right). \end{aligned}$$

Using Lemma A.3 by treating X'_π and Y'_π as the weighted (w_{ij}) sum of random variables X_{ij} (Y_{ij}), we obtain that

$$\begin{aligned} Pr\left\{Y'_\pi \geq \frac{\lambda_X + \lambda_Y}{2}\right\} &\leq \exp\left(-(\lambda_X - \lambda_Y)^2/12(\lambda_X + \lambda_Y)\right), \\ Pr\left\{X'_\pi \leq \frac{\lambda_X + \lambda_Y}{2}\right\} &\leq \exp\left(-(\lambda_X - \lambda_Y)^2/8(\lambda_X + \lambda_Y)\right). \end{aligned}$$

[2] $\overset{(stoch.)}{\geq}$ denotes stochastic domination

Hence, we have

$$Pr\{X_\pi - Y_\pi \le 0\} \le 2\exp\left(\frac{-(\lambda_X-\lambda_Y)^2}{12(\lambda_X+\lambda_Y)}\right). \quad \square$$

$\square$

We now proceed to derive lower bound for the numerator and upper bound for the denominator in the exponent of the RHS of Inequality (A–2) to obtain the upper bound of the RHS. By standard calculation, we have

$$\begin{aligned}
&(\lambda_X-\lambda_Y)^2\\
\ge&\left(2\sum_{(i,j)\in E_\pi\setminus\phi} w_{ij}p_{c(i)c(j)}(1-p_{c(i)c(j)})s_1s_2 - \frac{k\overline{w}\beta(s_1+s_2-2s_1s_2)}{2}\right)^2\\
\ge&\frac{k^2}{4}\left[4\left(n-\frac{k}{2}-1\right)\underline{w}\alpha(1-\beta)s_1s_2 - \overline{w}\beta(s_1+s_2-2s_1s_2)\right]^2,
\end{aligned}$$

and

$$\begin{aligned}
&\lambda_X+\lambda_Y\\
\le&\sum_{(i,j)\in E_\pi}[w_{ij}p_{c(i)c(j)}(s_1+s_2-2s_1s_2)\\
&\quad + w_{ij}p_{c(i)c(j)}(s_1+s_2-2p_{c(i)c(j)}s_1s_2)]\\
\le&2\sum_{(i,j)\in E_\pi} w_{ij}p_{c(i)c(j)}(s_1+s_2)\\
\le&2\left(nk-\frac{k^2}{2}-k\right)\overline{w}\alpha(s_1+s_2).
\end{aligned}$$

Therefore, by Lemma A.2, $Pr\{X_\pi - Y_\pi \le 0\}$ can be upper bounded by

$$
\begin{aligned}
&Pr\{X_\pi - Y_\pi \le 0\} \le 2\exp\left[-(\lambda_X-\lambda_Y)^2/12(\lambda_X+\lambda_Y)\right] \\
\le& 2\exp\left\{-\frac{k^2\left[4(\frac{2n-k+2}{2})\underline{w}\alpha(1-\beta)s_1s_2 - \overline{w}\beta(s_1+s_2-2s_1s_2)\right]^2}{96(nk-\frac{k^2}{2}-k)\overline{w}\alpha(s_1+s_2)}\right\} \qquad \text{(A–3)} \\
\le& \exp\left\{-\frac{k^2\left[(n-\frac{k}{2}-1)\underline{w}\alpha(1-\beta)s_1s_2\right]^2}{6(nk-\frac{k^2}{2}-k)\overline{w}\alpha(s_1+s_2)}\right\}, \qquad \text{(A–4)}
\end{aligned}
$$

where Inequality (A–4) follows from the conditions stated in the theorem.

2. **Convergence of the Upper Bound:** Now, we further show that the derived upper bound converges to 0 as $n \to \infty$. Due to the monotonicity of w_{ij} with respect to $p_{c(i)c(j)}$, we easily obtain that $\overline{w} = \log\left(\frac{1-\alpha(s_1+s_2-2s_1s_2)}{\alpha(1-s_1)(1-s_2)}\right)$ and $\underline{w} = \log\left(\frac{1-\beta(s_1+s_2-2s_1s_2)}{\beta(1-s_1)(1-s_2)}\right)$. Hence, $\overline{w}$ and $\underline{w}$ can be determined by α, β, s_1, s_2.

Plugging Inequality (A–4) into Inequality (A–1), we have

$$
\begin{aligned}
\mathbb{E}[S] &\le 2\sum_{k=2}^{n} n^k \cdot \exp\left(-\frac{k^2\left[(n-\frac{k}{2}-1)\underline{w}\alpha(1-\beta)s_1s_2\right]^2}{6(nk-\frac{k^2}{2}-k)\overline{w}\alpha(s_1+s_2)}\right) \\
&\le \sum_{k=2}^{\infty}\exp\left\{k\left(-\frac{\left[(n-\frac{k}{2}-1)\underline{w}\alpha(1-\beta)s_1s_2\right]^2}{6(n-\frac{k}{2}-1)\overline{w}\alpha(s_1+s_2)} + \log n\right)\right\} \\
&\le \sum_{k=2}^{\infty}\exp\left\{k\left(-\frac{\left[(n-\frac{k}{2}-1)\underline{w}^2\alpha^2(1-\beta)^2s_1^2s_2^2\right]}{6\overline{w}\alpha(s_1+s_2)} + \log n\right)\right\}
\end{aligned}
$$

Since $\alpha, \beta \to 0$, $\frac{\log\alpha}{\log\beta} \le \gamma$, we also have $\frac{\overline{w}}{\underline{w}} \le \gamma' = \Theta(\gamma)$ and $\overline{w} = \Theta(\log\frac{1}{\alpha})$ where γ' may be a function of γ. Hence, we have for some constant C,

$$
\mathbb{E}[S] \le \sum_{k=2}^{\infty}\exp\left\{k\left(-\frac{\left[Cn\alpha^2(1-\beta)^2s_1^2s_2^2\log\frac{1}{\alpha}\right]}{\gamma'^2\alpha(s_1+s_2)} + \log n\right)\right\}.
$$

Therefore, if $\frac{\alpha(1-\beta)^2s_1^2s_2^2\log(1/\alpha)}{s_1+s_2} = \Omega(\frac{\gamma\log^2 n}{n}) + \omega(\frac{1}{n})$, the sum of the above geometric series goes to zero as n goes to infinity. Therefore, $\mathbb{E}[S] \to 0$. Hence, with the

above conditions in Theorem 3.1.1 satisfied, the MAP estimate $\hat{\pi}$ coincides with the correct mapping π_0 with probability goes to 1 as n goes to infinity.

A.2 Superiority of Our Cost Function

In this section, we compare our cost functions over previous ones proposed in the literature. Specifically, we demonstrate the superiority of our cost function in bilateral case over the most similar previous cost function proposed by Pedarsani et al. [8]. Recall that the cost function derived in [8], which we denoted as Δ'_π, is

$$\Delta'_\pi = \sum_{i \le j}^{n} \left| \mathbb{1}\{(i,j) \in E_1\} - \mathbb{1}\{(\pi(i),\pi(j)) \in E_2\} \right|.$$

The advantages of our cost function is two-fold. First, Δ'_π, as an unweighted version of our proposed Δ_π, corresponds to the MAP estimator in bilateral de-anonymization when the underlying social network is an Erdős-Rényi graph. Therefore, our cost function in a sense, subsumes the cost function in [8] as a special case in bilateral de-anonymization, and has more generality when the underlying network is non-uniform or the adversary only possesses unilateral community information. Second, we show that in certain cases, the correct mapping π_0 is the unique minimizer of Δ_π, while it is not the unique minimizer of Δ'_π. Indeed, when the underlying social network is as shown in Figure A–1, and the sampling probabilities $s_1 = s_2 \le \frac{\gamma'}{2}$, with γ' defined as in the proof of Theorem 3.1.1, we have that the unique minimizer of Δ_π asymptotically almost surely coincides with π_0 by Theorem 3.1.1. However, as Δ'_π does not count the weight of node pairs, in each realization of G_1 and G_2, there exists a mapping π' that permutes $\pi_0 = \arg\min_{\pi \in \Pi} \Delta_\pi$ on some nodes in C_3 with $\Delta'_{\pi'} \le \Delta_{\pi_0}$. Therefore, in this case, the minimizer of Δ'_π does not equals to π_0, which demonstrates that Δ_π has wider application.

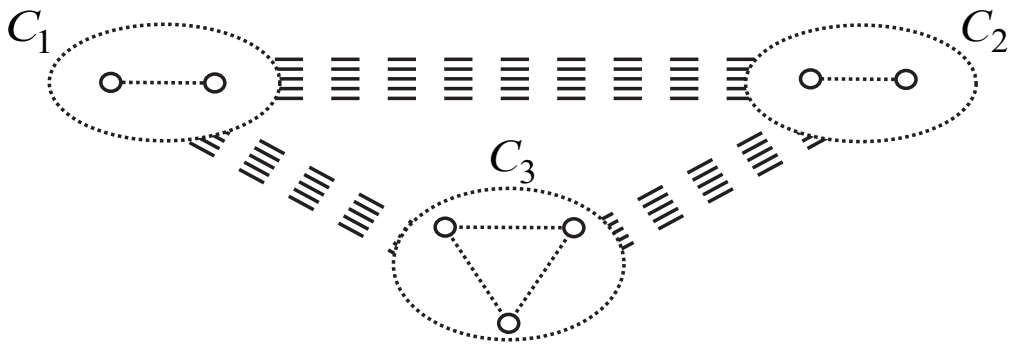


Figure A–1: **An example demonstrating the superiority of our cost function: the sizes of the communities $|C_1|, |C_2|$ equal to some constant C and $|C_3| = n - 2C$, the affinity values $p_{11} = p_{22} = p_{33} = p_{12} = p_{23} = 5 \log n/n$, $p_{13} = \log n/\sqrt{n}$, the sampling probabilities $s_1 = s_2 = 2/3$**

A.3 Upper Bound of Inequality (19)

To present the upper bound of Inequality (3–19), we begin with bounding $\|\mathbf{D}^{-1}\|$ and $\|\mathbf{N}\|$. First, by the special block-diagonal structure of $\mathbf{D}$, we readily have that $\mathbf{D}^{-1}$ is also block diagonal with each $n \times n$ diagonal block as $\mathbf{D}_i^{-1}$, which is the identity matrix with the ith row replaced by $\frac{1}{\mathbf{v}_i}(-\mathbf{v}_1, \ldots, -\mathbf{v}_{i-1}, 1, -\mathbf{v}_{i+1}, \ldots, -\mathbf{v}_n)$. We have

$$\|\mathbf{D}_i^{-1}\| \leq 1 + \frac{\sqrt{n}\epsilon_1}{\epsilon_2}, \quad \text{for all } i.$$

Hence we have,

$$\|\mathbf{D}^{-1}\| \leq \max_{i=1\ldots n} \|\mathbf{D}_i^{-1}\| \leq 1 + \frac{\sqrt{n}\epsilon_1}{\epsilon_2}. \tag{A–5}$$

Similarly, we obtain

$$\begin{aligned}\|\mathbf{N}\|^2 &\leq \max_{i,j=1\ldots n} \|\mathbf{N}_i\|_{\mathrm{F}}^2 = \max_{i=1\ldots n} \sum_{jk} (s_{jk}^i + t_{jk}^i + w_{jk}^i + \frac{r_{ij}}{n})^2 \\ &\leq 4 \left(\max_{i=1\ldots n} \sum_k \left(s_{jk}^i\right)^2 + \max_{i,j=1\ldots n} \sum_{jk} \left(t_{jk}^i\right)^2 \right. \\ &\quad \left. + \max_{i,j=1\ldots n} \sum_k \left(w_{jk}^i\right)^2 + \max_{i,j=1\ldots n} \sum_k \left(\frac{r_{ij}}{n}\right)^2 \right)^2 .\end{aligned}$$

Next, we bound these the sum of the square of terms s_{jk}^i, t_{jk}^i, w_{jk}^i and r_{ij} one by one using the following inequalities.

$$\begin{aligned}&\max_{i=1\ldots n} \sum_{jk} \left(s_{jk}^i\right)^2 \\ =& \max_{i=1\ldots n} \sum_k \frac{1}{(\lambda_i - \lambda_j)^4} \\ &\qquad \cdot \left(\mathbf{E}_{kj}(\lambda_j + \lambda_k - 2\lambda_i) - \frac{v_j}{v_i} \mathbf{E}_{ki}(\lambda_k - \lambda_i) \right)^2 \\ \leq& \max_{i=1\ldots n} \frac{1}{\delta^4} \left(4\sigma \sum_{jk} |\mathbf{E}_{kj}| + 2\sigma \frac{\epsilon_1}{\epsilon_2} \sum_{kj} |\mathbf{E}_{kj}| \right)^2 \\ \leq& \frac{4\sigma^2}{\delta^4} \left(1 + 2\frac{\epsilon_1}{\epsilon_2}\right)^2 \xi^2\end{aligned}$$

$$
\begin{aligned}
&\max_{i=1\ldots n}\sum_{jk}\left(t_{jk}^{i}\right)^{2}\\
=&\max_{i=1\ldots n}\sum_{jk}\frac{1}{(\lambda_i-\lambda_j)^4}\left(\mathbf{G}_{kj}-\frac{v_j}{v_i}\mathbf{G}_{ki}\right)^{2}\\
\leq&\sum_{jk}\frac{1}{\delta^4}\left(\mathbf{G}_{kj}+2\frac{\epsilon_1}{\epsilon_2}\mathbf{G}_{ki}\right)^{2}\\
\leq&\frac{1}{\delta^4}\left(1+2\frac{\epsilon_1}{\epsilon_2}\right)^{2}\|\mathbf{G}\|_{\mathrm{F}}^{2}\\
\leq&\frac{1}{\delta^4}\left(1+2\frac{\epsilon_1}{\epsilon_2}\right)^{2}\xi^{4}.
\end{aligned}
$$

$$
\begin{aligned}
&\max_{i=1\ldots n}\sum_{jk}\left(w_{jk}^{i}\right)^{2}\\
=&\max_{i=1\ldots n}\sum_{jk}\frac{\mu^2}{(\lambda_i-\lambda_j)^4}\left(\mathbf{M}'_{kj}-\frac{\mathbf{v}_j}{\mathbf{v}_i}\mathbf{M}'_{ki}\right)^{2}\\
\leq&\frac{\mu^2}{\delta^4}\max_{i=1\ldots n}\sum_{jk}\left(\sum_{k}\mathbf{M}'_{kj}+2\frac{\epsilon_1}{\epsilon_2}\sum_{k}\mathbf{M}'_{ki}\right)^{2}\\
\leq&\frac{\mu^2}{\delta^4}\left(1+2\frac{\epsilon_1}{\epsilon_2}\right)^{2}\|\mathbf{M}'\|_{\mathrm{F}}^{2}\\
\leq&\frac{\mu^2}{\delta^4}\left(1+2\frac{\epsilon_1}{\epsilon_2}\right)M^{2}.\quad\text{(by the orthonomality of }\mathbf{U}\text{)}
\end{aligned}
$$

$$
\begin{aligned}
&\max_{i,j=1\ldots n}\sum_{k}\left(\frac{r_{ij}}{n}\right)^{2}\\
=&\max_{i,j=1\ldots n}\frac{\mu^2}{n(\lambda_i-\lambda_j)^4}\left(\mathbf{v}_j\mathbf{M}'_{ii}-\mathbf{v}_i\mathbf{M}'_{ij}\right)^{2}\\
\leq&\frac{4\epsilon_1^2\mu^2}{n\delta^4}\|\mathbf{M}'\|_{\mathrm{F}}^{2}\\
\leq&\frac{4\epsilon_1^2\mu^2}{n\delta^4}M^{2}.
\end{aligned}
$$

From the above manipulations, we have

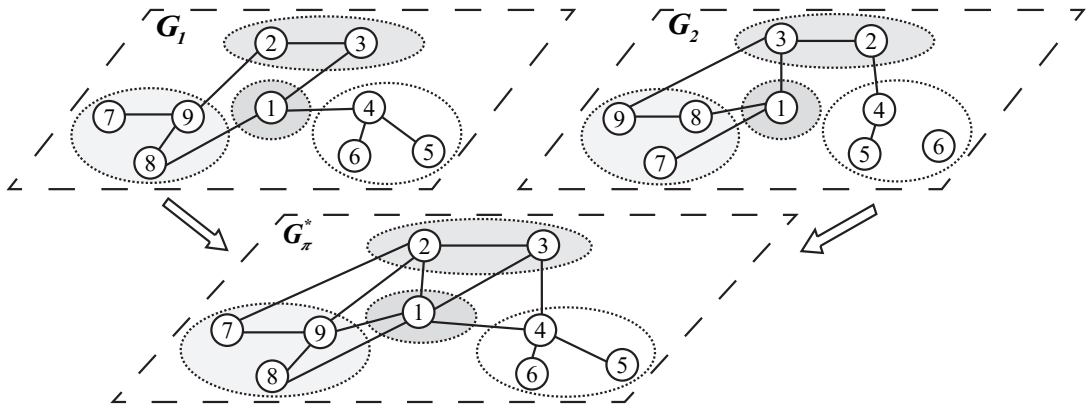


Figure A–2: **An example of G_π^* that has the minimum number of edges in $\mathcal{G}_\pi$, which is the set of all realizations of G that are consistent with G_1, G_2, π. In this case $\pi = \pi_0$.**

$$\begin{aligned}\|\mathbf{N}\|^2 &\le 4\left[\left(1+2\frac{\epsilon_1}{\epsilon_2}\right)^2\left(\frac{\sigma^2}{\delta^4}\xi^2+\frac{1}{\delta^4}\xi^4+\frac{\mu^2}{\delta^4}M^2\right)+\frac{4\epsilon_1^2\mu^2M^2}{n\delta^4}\right]\\ &\le 5\left[\left(1+2\frac{\epsilon_1}{\epsilon_2}\right)^2\left(\frac{\sigma^2}{\delta^4}\xi^2+\frac{1}{\delta^4}\xi^4+\frac{\mu^2}{\delta^4}M^2\right)\right], \qquad \text{(A–6)}\end{aligned}$$

for sufficiently large n. Substituting Inequalities (A–5) and A–6 into (3–19), it follows that

$$\|\mathbf{F}-\mathbf{I}\|_{\mathrm{F}} = \|\mathbf{f}-\mathbf{f}_0\| \le \sqrt{n}\frac{1-\left(1+\frac{\sqrt{n}\epsilon_1}{\epsilon_2}\right)\sqrt{\frac{5}{\delta^4}\left[\left(1+2\frac{\epsilon_1}{\epsilon_2}\right)^2(\sigma^2\xi^2+\xi^4+\mu^2M^2)\right]}}{\left(1+\frac{\sqrt{n}\epsilon_1}{\epsilon_2}\right)\sqrt{\frac{5}{\delta^4}\left[\left(1+2\frac{\epsilon_1}{\epsilon_2}\right)^2(\sigma^2\xi^2+\xi^4+\mu^2M^2)\right]}}.$$

A.4 MAP estimation of Unilateral De-anonymization

In this section, we derive the MAP estimator for unilateral de-anonymization. Recall that given G_1, G_2, c, $\boldsymbol{\theta}$, the MAP estimate $\hat{\pi}$ of the correct mapping π_0 is defined as follows

$$\hat{\pi} = \arg\max_{\pi \in \Pi} Pr(\pi_0 = \pi \mid G_1, G_2, c, \boldsymbol{\theta}), \tag{A–7}$$

The MAP estimator can be further written as:

$$\hat{\pi} = \arg\max_{\pi \in \Pi} \sum_{G \in \mathcal{G}_\pi} p(G, \pi \mid G_1, G_2, c, \boldsymbol{\theta}), \tag{A–8}$$

where $\mathcal{G}_\pi$ is the set of all realizations of the underlying social network that are consistent with G_1, G_2 and π. By Bayesian rule, we have

$$\begin{aligned}
&\arg\max_{\pi \in \Pi} \sum_{G \in \mathcal{G}_\pi} p(G, \pi \mid G_1, G_2, c, \boldsymbol{\theta}) \\
=&\arg\max_{\pi \in \Pi} \sum_{G \in \mathcal{G}_\pi} \frac{p(G_1, G_2 \mid G, \pi) p(G, \pi)}{p(G_1, G_2)} \\
=&\arg\max_{\pi \in \Pi} \sum_{G \in \mathcal{G}_\pi} p(G_1, G_2 \mid G, \pi) p(G) p(\pi) \\
=&\arg\max_{\pi \in \Pi} \sum_{G \in \mathcal{G}_\pi} p(G_1 \mid G) p(G_2 \mid G, \pi) p(G).
\end{aligned}$$

Note that we drop parameters c and $\boldsymbol{\theta}$ for brevity since their values are fixed. From the

definitions of the models, we have:

$$
\begin{aligned}
&\arg\max_{\pi\in\Pi}\sum_{G\in\mathcal{G}_\pi} p(G_1 \mid G=g)p(G_2 \mid G,\pi)p(G)\\
=&\arg\max_{\pi\in\Pi}\sum_{G\in\mathcal{G}_\pi}\prod_{i<j}^{n}(1-s_1)^{|E^{ij}|-|E_1^{ij}|}s_1^{|E_1^{ij}|}\\
&\cdot\prod_{i<j}^{n}(1-s_2)^{|E^{ij}|-|E_2^{\pi(i)\pi(j)}|}s_2^{|E_2^{\pi(i)\pi(j)}|}\cdot\prod_{i<j}^{n}p_{c(i)c(j)}^{|E^{ij}|}(1-p_{c(i)c(j)})^{1-|E^{ij}|}\\
=&\arg\max_{\pi\in\Pi}\left(\prod_{i<j}^{n}\left(\frac{s_1}{1-s_1}\right)^{|E_1^{ij}|}\left(\frac{s_2}{1-s_2}\right)^{|E_2^{\pi(i)\pi(j)}|}\right)\\
&\cdot\left(\sum_{g\in\mathcal{G}_\pi}\prod_{i<j}^{k}\left(\frac{p_{c(i)c(j)}(1-s_1)(1-s_2)}{1-p_{c(i)c(j)}}\right)^{|E^{ij}|}\right)\\
=&\arg\max_{\pi\in\Pi}\prod_{i<j}^{n}\left(\frac{s_2}{1-s_2}\right)^{|E_2^{\pi(i)\pi(j)}|}\\
&\cdot\sum_{g\in\mathcal{G}_\pi}\prod_{i<j}^{k}\left(\frac{p_{c(i)c(j)}(1-s_1)(1-s_2)}{1-p_{c(i)c(j)}}\right)^{|E^{ij}|}\\
=&\sum_{g\in\mathcal{G}_\pi}\prod_{i<j}^{k}\left(\frac{p_{c(i)c(j)}(1-s_1)(1-s_2)}{1-p_{c(i)c(j)}}\right)^{|E^{ij}|},
\end{aligned}
$$

where $|E^{ij}|, |E_1|^{ij}, |E_2^{ij}|$ take value 0 or 1 indicating whether there exists an edge between nodes i and j in G, G_1, G_2 respectively. Note that in the above manipulations, we frequently eliminate the terms that do not depend on π. Particularly, in the last step, although the term $\left(\frac{s_2}{1-s_2}\right)^{|E_2^{\pi(i)\pi(j)}|}$ depends on π, the value of the whole product $\prod_{i<j}^{n}\left(\frac{s_2}{1-s_2}\right)^{|E_2^{\pi(i)\pi(j)}|}$ is independent of π itself since it is a bijective mapping.

Now, let G_π^* be the graph having the smallest number of edges in $\mathcal{G}_\pi$, which is equivalent to that $G_\pi^* = (V, E_1 \cup \pi(E_1))$. An illustration of G_π^* is provided in Figure A–2. Denote the set of edges in G_{π^*} as E_{π^*}, with $|E_{\pi^*}^{ij}|$ indicating the number of edges between i and j. By the definition we have that in $\mathcal{G}_\pi$, all the graphs have edge sets that

are supersets of G^*_π. By summing over all the graphs in $\mathcal{G}_\pi$, we have that

$$\hat{\pi} = \arg\max_{\pi\in\Pi} \prod_{i<j}^{n} \left(\frac{p_{c(i)c(j)}(1-s_1)(1-s_2)}{1-p_{c(i)c(j)}}\right)^{|E^{ij}_{\pi^*}|} \cdot \prod_{i<j}^{n} \left(1+\left(\frac{p_{c(i)c(j)}(1-s_1)(1-s_2)}{1-p_{c(i)c(j)}}\right)\right)^{1-|E^{ij}_{\pi^*}|},$$

where the above equality follows from that

$$\begin{aligned}
&\sum_{g\in\mathcal{G}_\pi} \prod_{i<j}^{n} \left(\frac{p_{c(i)c(j)}(1-s_1)(1-s_2)}{1-p_{c(i)c(j)}}\right)^{|E^{ij}|-|E^{ij}_{\pi^*}|} \\
=&\sum_{0\le k_{ij}\le 1-|E^{ij}_{\pi^*}|} \prod_{i<j}^{n} \left(\frac{p_{c(i)c(j)}(1-s_1)(1-s_2)}{1-p_{c(i)c(j)}}\right)^{k_{ij}} \\
=&\prod_{i<j}^{n} \left(1+\left(\frac{p_{c(i)c(j)}(1-s_1)(1-s_2)}{1-p_{c(i)c(j)}}\right)\right)^{1-|E^{ij}_{\pi^*}|}.
\end{aligned}$$

Then, from the above equation we can further write the MAP estimator as:

$$\begin{aligned}
&\arg\max_{\pi\in\Pi} \prod_{i<j}^{n} \left(\frac{p_{c(i)c(j)}(1-s_1)(1-s_2)}{1-p_{c(i)c(j)}(s_1+s_2-s_1s_2)}\right)^{|E^{ij}_{\pi^*}|} \\
=&\arg\min_{\pi\in\Pi} \prod_{i<j}^{n} \left(\frac{1-p_{c(i)c(j)}(s_1+s_2-s_1s_2)}{p_{c(i)c(j)}(1-s_1)(1-s_2)}\right)^{|E^{ij}_{\pi^*}|} \\
=&\arg\min_{\pi\in\Pi} \left[|E^{ij}_{\pi^*}| \log\left(\frac{1-p_{c(i)c(j)}(s_1+s_2-s_1s_2)}{p_{c(i)c(j)}(1-s_1)(1-s_2)}\right)\right].
\end{aligned}$$

Next, by the definition of g_{π^*}, we notice that

$$|E^{ij}_{\pi^*}| = \lceil \frac{(|E^{ij}_1| + |E^{\pi(i)\pi(j)}_2|)}{2} \rceil.$$

Hence, by setting $w_{ij} = \log\left(\frac{1-p_{c(i)c(j)}(s_1+s_2-s_1s_2)}{p_{c(i)c(j)}(1-s_1)(1-s_2)}\right)$ we have

$$\hat{\pi} = \arg\min_{\pi \in \Pi} \left(\sum_{i<j}^{n} w_{ij} (\mathbb{1}\{(i,j) \notin E_1, (\pi(i), \pi(j)) \in E_2\} \right)$$

Note that the MAP estimator is not symmetric with regard to G_1 and G_2. This stems from the fact that the adversary in this case only has knowledge on the community assignment function of G_1.

A.5 Convexity of the Relaxed UNI-MAP-ESTIMATE

In this section, we prove that the relaxed matrix formulation of the optimization problem UNI-MAP-ESTIMATE is a convex optimization problem. The relaxed formulation is presented as follows:

$$\begin{aligned} \text{mininize } & \|\mathbf{W} \circ (\ \mathbf{A} - \mathbf{B}\ )\|_{\lfloor \mathrm{F} \rfloor}^2 \\ \textbf{s.t. } & \forall i, \sum_{i} {}_{ij} = 1 && \text{(A–9)} \\ & \forall j, \sum_{j} {}_{ij} = 1 && \text{(A–10)} \end{aligned}$$

Obviously, the set of feasible solutions defined by Constraints (A–9) and (A–10) is a convex set. Then, for the objective function $\|\mathbf{W} \circ (\ \mathbf{A} - \mathbf{B}\ )\|_{\lfloor \mathrm{F} \rfloor}^2$, according to the definition of operator $\|\cdot\|_{\lfloor \mathrm{F} \rfloor}$ it can be interpreted as weighted summation of truncated quadratic functions of each element of Π with the weights being positive real numbers. Each truncated function is equivalent to the square of a linear function of an element of Π with the part where the elements take positive values truncated. Therefore, each truncated function is convex. It follows that the whole objective function, being a weighted combination of convex functions, is convex. Thus, we conclude that the relaxed UNI-MAP-ESTIMATE is a convex optimization problem, the global optima of which can be found in $O(n^6)$ time using the same algorithm as in the bilateral case.

References

[1] J. Leskovec and A. Krevl, "SNAP Datasets: Stanford Large Network Dataset Collection", http://snap.stanford.edu/data, 2014.

[2] E. Bakshy, D. Eckles, R. Yan and I. Rosenn, "Social influence in social advertising: evidence from field experiments", in *Proc. ACM EC*, pp. 146-161, 2012.

[3] M. Yuan, L. Chen, S. Y. Philip and T. Yu, "Protecting sensitive labels in social network data anonymization", in *IEEE Trans. on Knowledge and Data Engineering*, Vol. 25, No. 3, pp. 633-647, 2013.

[4] X. Wu, X. Zhu, G. Q. Wu and W. Ding, "Data mining with big data", in *IEEE Trans. on Knowledge and Data Engineering*, Vol. 26, No.1, pp. 97-107, 2014.

[5] W. Wang, L. Ying and J. Zhang, "The value of privacy: strategic data subjects, incentive mechanisms and fundamental limits", in *Proc. ACM SIGMETRICS*, pp. 249-260, 2016.

[6] R. Baden, A. Bender, N. Spring, B. Bhattacharjee and D. Starin, "Persona: an online social network with user-defined privacy", in *ACM SIGCOMM Computer Communication Review*, Vol. 39, No. 4, pp. 135-146, 2009.

[7] A. Narayanan and V. Shmatikov, "De-anonymizing social networks", in *IEEE Symposium on Security and Privacy*, pp. 173-187, 2009.

[8] P. Pedarsani and M. Grossglauser, "On the privacy of anonymized networks" in *Proc. ACM SIGKDD*, pp. 1235-1243, 2011.

[9] E. Kazemi, L. Yartseva and M. Grossglauser, "When can two unlabeled networks be aligned under partial overlap?", in *IEEE 53rd Annual Allerton Conference on Communication, Control, and Computing*, pp. 33-42, 2015.

[10] D. Cullina and N. Kiyavash, "Improved achievability and converse bounds for Erdős-Rényi graph matching", in *Proc. ACM SIGMETRICS*, pp. 63-72, 2016.

[11] P. Erdős and A. Rényi, "On random graphs", in *Publicationes Mathematicae*, pp. 290-297, 1959.

[12] F. Chung and L. Lu, "The average distance in a random graph with given expected degrees", in *Internet Mathematics*, Vol. 1, No. 1, pp. 91-113, 2003.

[13] S. Ji, W. Li, M. Srivatsa and R. Beyah, "Structural data de-anonymization: Quantification, practice, and implications", in *Proc. ACM CCS*, pp. 1040-1053, 2014.

[14] S. Ji, W. Li, M. Srivatsa, J.S. He and R. Beyah, "General graph data de-anonymization: From mobility traces to social networks", in *ACM Trans. on Information and System Security*, Vol. 18, No. 4, pp. 12, 2012.

[15] E. Onaran, G. Siddharth and E. Erkip, "Optimal de-anonymization in random graphs with community structure", arXiv preprint arXiv:1602.01409, 2016.

[16] S. Ji, W. Li, N. Z. Gong, P. Mittal and R. Beyah, "On your social network de-anonymizablity: Quantification and large scale evaluation with seed knowledge" in *NDSS* 2015.

[17] S. Nilizadeh, A. Kapadia and Y-Y. Ahn, "Community-enhanced de-anonymization of online social networks", in *Proc. of ACM CCS*, 2014.

[18] A. Decelle, F. Krzakala, C. Moore and L. Zdeborová, "Asymptotic analysis of the stochastic block model for modular networks and its algorithmic applications" in *Physical Review E*, No. 84, Vol. 6, pp. 066106, 2011.

[19] M. Newman, "Networks: an introduction", Oxford university press, 2010.

[20] Microsoft Academic Graph https://www.microsoft.com/en-us/research/project/microsoft-academic-graph/

[21] L. Yartseva and M. Grossglauser, "On the performance of percolation graph matching", in *Proc. ACM COSN*, pp. 119-130, 2013.

[22] E. Kazemi, S. H. Hassani and M. Grossglauser, "Growing a graph matching from a handful of seeds", in *Proc. the VLDB Endowment*, pp. 1010-1021, 2015.

[23] C. F. Chiasserini, M. Garetto and E. Leonardi, "Social network de-anonymization under scale-free user relations", in *IEEE/ACM Trans. on Networking*, Vol. 24, No. 6, pp. 3756-3769, 2016.

[24] N. Korula and S. Lattanzi, "An efficient reconciliation algorithm for social networks", in *Proc. the VLDB Endowment*, pp. 377-388, 2014.

[25] C. F. Chiasserini, M. Garetto and E. Leonardi, "Impact of clustering on the performance of network de-anonymization", in *Proc. ACM COSN*, pp. 83-94, 2015.

[26] M. Girvan and M. Newman, "Community structure in social and biological networks", in *Proc. the National Academy of Sciences*, Vol. 99, No. 12, pp. 7821-7826, 2002.

[27] G. Fanti, P. Kairouz, S. Oh, K. Ramchandran and P. Viswanath, "Rumor Source Obfuscation on Irregular Trees", in *Proc. ACM SIGMETRICS*, pp. 153-164, 2016.

[28] J. Mcauley and J. Leskovec, "Discovering social circles in ego networks" in *ACM Trans. on Knowledge Discovery from Data*, Vol. 8, No. 1, 2014.

[29] S. Arora, A. Frieze and H. Kaplan, "A new rounding procedure for the assignment problem with applications to dense graph arrangement problems", in *Mathematical programming*, Vol. 92, No. 1, pp. 1-36, 2012.

[30] Y. Aflalo, B. Alexander and R. Kimmel, "On convex relaxation of graph isomorphism", in *Proc. the National Academy of Sciences*, Vol. 112, No. 10, pp. 2942-2947, 2015.

[31] J. R. Bunch, "The weak and strong stability of algorithms in numerical linear algebra", in *Linear Algebra and Its Applications* Nol. 88, pp. 49-66, 1987.

[32] D. Goldfarb and S. Liu, "An $O(n^3L)$ primal interior point algorithm for convex quadratic programming", in *Mathematical Programming*, No. 49, Vol. 1, pp. 325-340, 1990.

[33] J. Yang and J. Leskovec, "Defining and evaluating network communities based on ground-truth", in *Knowledge and Information Systems*, No. 42, Vol. 1, pp. 181-213, 2015.

[34] V. Lyzinski, D. E. Fishkind, M. Fiori, J. T. Vogelstein, C. E. Priebe and G. Sapiro, "Graph matching: Relax at your own risk" in *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. 38, No. 1, pp. 60-73, 2016.

[35] C. McDiarmid,"On the method of bounded differences", in *Surveys in combinatorics* No. 141, Vol. 1, pp. 148-188, 1989.

[36] P. Raghavan, "Probabilistic construction of deterministic algorithms: Approximating packing integer programs", in *Journal of Computer and System Sciences*, No. 37, Vol. 2, pp. 130-143, 1988.

Acknowledgements

First, I would like to express my sincerest gratitude to Prof. Xinbing Wang and Dr. Luoyi Fu. Since I joined the IIoT Research Center in my sophomore year, Prof. Wang and Dr. Fu have offered me invaluable support and guidance. I have benefited a lot from the research platform that Prof. Wang created for undergraduate students at SJTU and the hands-on training brought by Dr. Fu.

Second, I would like to thank my fellow groupmates, especially the ones that I have collaborated with, including Zhiying Xu, Zhongzhao Hu, Qianyang Peng, Jie You and Hongyu Gong. They have made tremendous contribution to the projects we have conducted during my undergraduate years. Working with them is an absolutely delightful and fruitful experience.

Third, I deeply appreciate the devotion of the instructors and TAs at SJTU. It is their efforts that make the classes enjoyable and lay a solid foundation for my future career.

Finally, I am wholeheartedly grateful to my family and friends. They have been providing me with enormous support in every aspects. Particularly, I owe a great deal to my parents and grandparents. They made me who I am today, and they are the ones that keep me going.

攻读学位期间发表的学术论文目录
Publications During Undergraduate Years

[1] **Xinzhe Fu**, Zhiying Xu, Qianyang Peng, Jie You, Luoyi Fu, Xinbing Wang and Songwu Lu, "ConMap: A Novel Framework for Optimizing Multicast Energy in Delay-constrained Mobile Wireless Networks", in *Proc. of ACM MobiHoc*, 2017.

[2] Jiaqi Liu, Yuhang Yao, **Xinzhe Fu**, Luoyi Fu, Xiaoyang Liu and Xinbing Wang, "Evolving K-Graph: Modeling Hybrid Interactions in Networks", in *Proc. of ACM MobiHoc*, 2017. (**Poster**)

[3] Luoyi Fu, **Xinzhe Fu**, Zhongzhao Hu, Zhiying Xu and Xinbing Wang, "De-anonymization of Social Networks with Communities: When Quantifications Meet Algorithms", in arXiv:1703.09028, 2017.

[4] **Xinzhe Fu**, Zhiying Xu, Qianyang Peng, Luoyi Fu and Xinbing Wang, "Complexity vs. Optimality: Unraveling Source-Destination Connection in Uncertain Graphs", in *Proc. of IEEE INFOCOM* 2017. (**Winner of the Best-in-Session Presentation Award**)

[5] Hongyu Gong, Luoyi Fu, **Xinzhe Fu**, Lutian Zhao, Kainan Wang and Xinbing Wang, "Distributed Multicast Tree Construction in Wireless Sensor Networks", in *IEEE Trans. on Information Theory*, 2016.

[6] Fan Wu, **Xinzhe Fu**, Shengzhong Liu and Ye Hu, "Principles of Wireless Sensor Networks (Translated Version in Chinese)", China Machine Press. (**To appear in 2017**)

[7] Luoyi Fu, **Xinzhe Fu**, Zhiying Xu, Qianyang Peng, Xinbing Wang and Songwu Lu, "Determining Source-Destination Connectivity in Uncertain Networks: Mod-

eling and Solutions", in *IEEE/ACM Trans. on Networking*, 2017. (**Under major revision**)

[8] Luoyi Fu, **Xinzhe Fu**, Zhiying Xu, Qianyang Peng, Xinbing Wang and Songwu Lu, "Joint Optimization of Multicast Energy in Delay-constrained Mobile Wireless Networks" in *IEEE/ACM Trans. on Networking*, 2017. (**Submitted**)

[9] Jiaqi Liu, Luoyi Fu, Yuhang Yao, **Xinzhe Fu**, Xiaoyang Liu and Xinbing Wang, "Modeling, Analysis and Validation of Evolving Networks with Hybrid Interactions", in *IEEE/ACM Trans. on Networking*, 2017. (**Submitted**)

[10] Luoyi Fu, Zhiying Xu, **Xinzhe Fu**, Jun Zhao and Xinbing Wang, "Unraveling Impact of Critical Sensing Range on Mobile Heterogeneous Camera Sensor Networks" in *IEEE Trans. on Mobile Computing*, 2017. (**Submitted**)