Research Proposal #2

小组成员：

- PB20111704 张宇昂
- PB20111647 鲍润晖
- PB20000103 王炳勋
- PB20111651 何泽昊

Abstract

随着社交媒体应用的广泛普及，社交媒体用户匿名化已成为攻击者窃取信息和不法者发布不当言论的手段之一，这引起了广泛关注。本次调研旨在探索一种反匿名化的方法，以解决日益严重的匿名化危害。我们的调研涵盖了Seed Method和Seedless Method两种方法，它们之间的区别在于是否需要掌握社交网络拓扑建模中种子节点的信息。由于这两种方法均存在一定的缺陷，我们计划通过对它们进行调研、复现、改进或结合，并在数据集上进行测试，以找到一种行之有效的反匿名化方法。

Motivation

社交网络是如今互联网中最广泛使用的应用之一。在社交网络上，我们可以和亲友，同事交流，分享生活中的趣事，发布以及获取信息等。但是与此同时隐私安全问题也成为社交网络中需要考虑的一个重要问题，用户匿名性问题就是其中之一。

匿名化通常是社交网络中用户用来保证隐私安全的一种方法。然而，在某些情况下，攻击者会试图利用反匿名化来获取用户真实信息，进行诈骗等不良行为；除此之外，某些用户利用匿名性发布一些不应出现在社交网络上的言论或信息，但借助匿名性的保护无法收到追查或制裁。因此，调研社交网络用户的反匿名化问题是非常有意义的。

目前，在反匿名化社交媒体中的用户方面，已有两种常用的方法：

1. Seed method: 需要预知一些种子节点的身份信息。这些种子节点可以是已知的、已验证的、或者是其他途径获取的信息，例如用户的公开信息、社交网络中的著名人物、或者其他已知身份的节点。通过种子节点的身份信息，可以推断出其他节点的身份信息。
2. Seedless method: 不需要预先知道任何种子节点的身份信息。它可以通过分析社交网络中节点之间的链接关系、用户行为和文本内容等信息，来推断每个节点的身份信息。

可以看出，这两种方法的区别主要是**是否具有一些关于种子结点的身份信息**，它们各自的局限性也因此各有不同：

1. Seed method: 需要的计算开销较大，如果**种子节点**信息不准确、较少或存在恶意信息时，将导致预测不准确
2. Seedless method: 由于没有预先知道的信息，准确度可能不如 Seeded 方法。同时，也可能会受到社交网络数据不完整或缺失的影响

Related Works

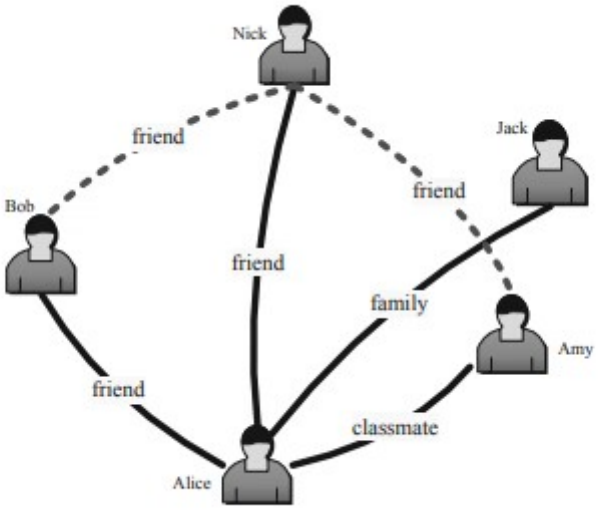
Seed Method

De-anonymizing social networks

作为社交网络反匿名化相关领域的开山之作，本文提出了一种通用的匿名社交网络重识别算法。该算法仅使用网络结构，不对多个网络之间的成员重叠做出任何先验假设，最终实现匿名社交网络的反匿名化。[1]

算法为以下几步：

- 数据预处理
  了解社交网络中少量用户的详细信息，通过这些信息，用爬虫方法得到网络中大量的用户和关系。
- 社交网络建模
  - 考虑一个特定时间t的社交网络**G（V，E）**，其中V和E是节点和连接的集合，图中的实线代表现有连接，虚线代表未来要生成的或者要删除的连接。通过社交网络的图形化建模，得到含有用户与用户间关系的信息的图。



  - 匿名目标图是一个有向图，其中每个用户都表示为一个节点，并且如果两个用户之间存在社交关系，则这两个节点之间存在一条有向边。该图是由社交网络中的用户数据构建而成的。
    攻击者辅助图是一个包含外部辅助信息的无向图，可以帮助攻击者推断出匿名目标图中用户的身份。它可以是任何类型的外部信息，例如用户的年龄、性别、地理位置等。攻击者可以收集这些信息并将它们与匿名目标图相结合，从而更好地推断出用户的身份。
- 节点识别
  - 识别出少量同时存在于匿名目标图和攻击者辅助图中的*种子*节点，并将它们相互映射。假设攻击者辅助图由k个节点组成，这些节点同时存在于辅助图和目标图中。那么只要知道这些节点中每个节点的度和每对节点的共同邻居的数量就足够了。
  - 运用**种子查找算法**将匿名目标图中的节点映射到攻击者辅助图相应的节点。
- 社交网络重构
  利用上一步得到的映射关系，不断找出新的映射关系，并加入到原有的关系中。

作者通过在Twitter和flicker上进行的实验，结果表明，30.8%的映射被正确重新识别，12.1%被错误识别，57%未被识别。

An efficient reconciliation algorithm for social networks

这篇论文提出了一种高效的算法，用于在多个在线社交网络中识别同一个用户，它基于一个简单的原理：同一个用户在不同社交网络中的账户会有相似的特征。

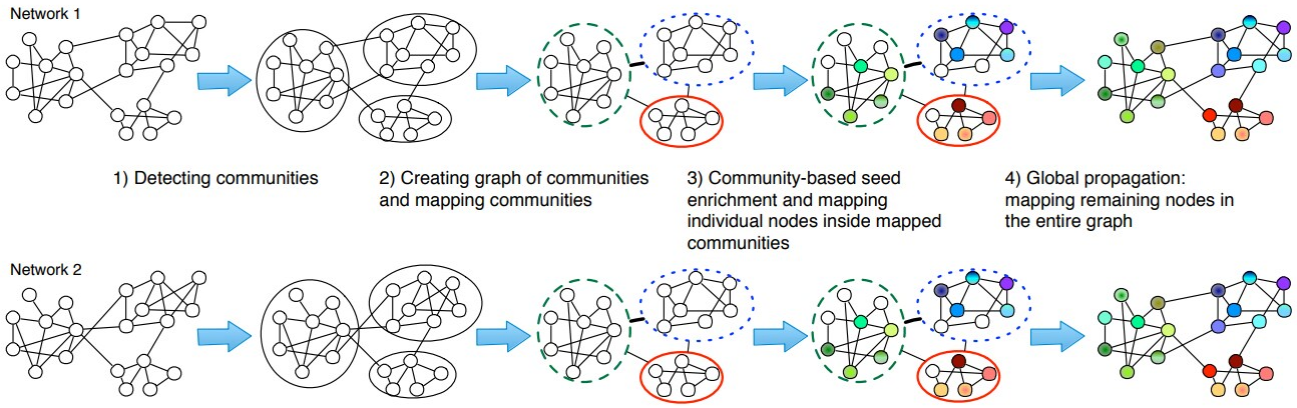
算法为以下几步：

- 对每个社交网络中的用户生成一个特征向量
  - 包含邻居信息：比如邻居的数量、邻居的邻居的数量、邻居之间的连接数等
  - 包含结构特征：比如聚类系数、平均路径长度、介数中心性等
  - 对每个用户，将其邻居信息和结构特征拼接成一个特征向量，并进行归一化处理
- 对每个社交网络中的特征向量进行*局部敏感哈希*，将相似的向量映射到相同的哈希桶中
  - *局部敏感哈希*是对每个特征向量，计算它与一些随机超平面的符号（正或负），并将这些符号拼接成一个二进制串作为哈希值
- 对每个社交网络中的用户，从其他社交网络中的相同哈希桶中找出*最近邻*的一些候选匹配，并根据*相似度阈值*和*一致性规则*确定最终的匹配
  - 其中*最近邻*的距离度量采用余弦相似度
  - *相似度阈值*是可以自定义的参数，用来过滤掉不够相似的候选匹配
  - *一致性规则*是指如果一个用户在多个社交网络中都有相同的候选匹配，那么这个候选匹配就更有可能是真正的匹配

这篇论文的作者在Twitter，Flickr和YouTube数据集上进行了实验，并且在实践中，作者引入了一些**种子节点**（已知在不同网络中对应的节点）来初始化去匿名化的过程和评估匹配的准确性，最终效果不错。

Community-Enhanced De-anonymization of Online Social Networks

这篇论文提出了“**社区**”这一结构，它是多个有关联的用户组成的社交网络的子图，介于宏观与微观之间。本文使用社区结构提高了去匿名化的效果与鲁棒性。



算法为以下几步：

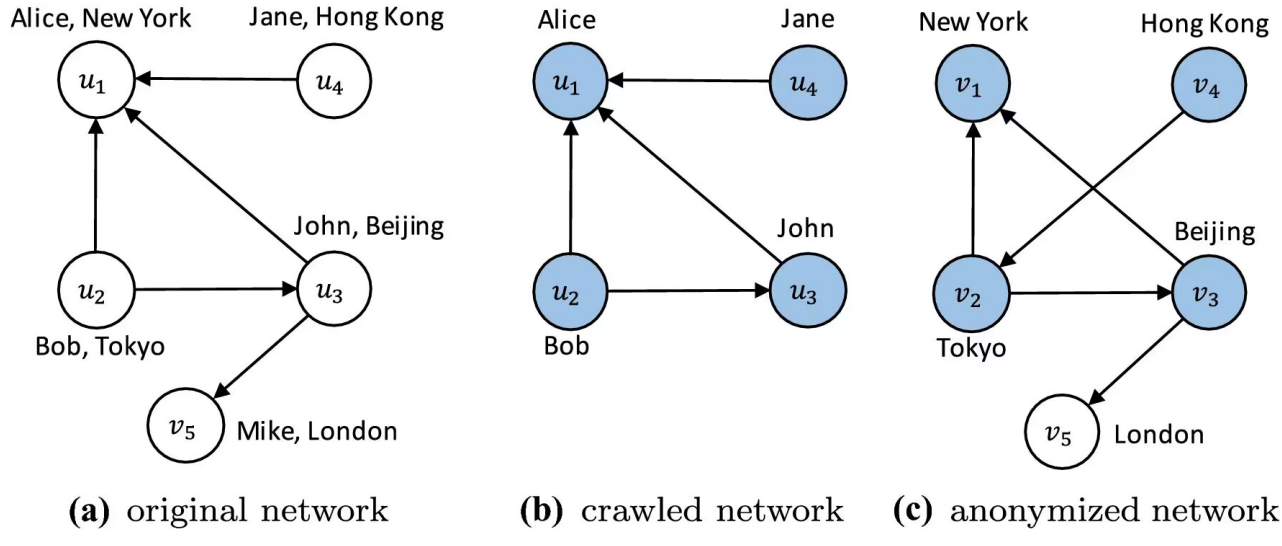
- 在每个社交网络中，使用*社区检测算法*来划分用户所属的社区，并为每个社区分配一个唯一的*标签*
  - *社区检测算法*可以是*Louvain算法*，根据网络的模块度（即连接紧密性）来划分；可以是*标签传播算法*，根据节点的邻居来更新节点的标签，直到标签达到稳定；也可以是*基于属性的算法*，根据节点的属性（如年龄、性别、地理位置等）的相似性来划分社区
- 在每个社交网络中，为每个用户计算一个特征向量
  - 包括他们的度数、邻居的度数、社区标签和社区内外的边数等
- 在两个社交网络之间，使用*贪心算法*来匹配相似的特征向量，并将匹配的用户对应起来
- 在匹配的过程中，使用一些*启发式规则*来优化匹配结果
  - *启发式规则*比如优先匹配度数高的用户、避免匹配同一社区内的用户等

同样，作者也引入了一些**种子节点**来初始化去匿名化的过程和评估匹配的准确性，他们在Flickr，LiveJournal，Orkut和YouTube数据集上进行了实验，并发现该方法还能够处理不同网络之间的结构异构性，即不同网络的社区划分可能不一致或不完全重合的情况。

Seedless Method

Fast De-anonymization of Social Networks with Structural Information

本文介绍了一种快速无种子去匿名化算法RoleMatch，它仅根据结构信息对网络进行去匿名化处理，得益于新的相似性度量 RoleSim++，可以高精度地计算节点相似性。此外在节点匹配阶段，除了节点相似度外，RoleMatch还利用邻域信息来改善映射结果。

- 优势
  - 提出了一种高效且无种子的方法RoleMatch，用于去匿名化。
  - 提出了一种新的节点相似性度量RoleSim++，它充分利用了结构信息，提高了去匿名化性能。
  - 开发了一种高效的迭代算法来计算RoleSim++，并利用节点相似性和邻域结构信息引入了一种快速节点匹配算法。两种算法有效降低了角色匹配的计算成本。
  - 研究了全局和本地去匿名化，并进行了全面的实验，以证明RoleMatch算法在真实数据集上的有效性和效率
- 去匿名化问题
  给定两个有向网络G1=(V1,E1)和G2=(V2,E2)
  G1是从原始网络爬网的网络，G2是一个匿名网络，并假设存在子网Gc⊂G1和G′c⊂G2，这样Gc.V=G′c.V，Gc表示爬网和匿名网络之间的重叠，称为重叠网络。去匿名化D(G1,G2)是匹配Gc和G′c之间节点尽可能多的过程。
- 噪音
  为了衡量去匿名化的难度，需要定义匿名网络的噪音。
  在D(G1,G2)问题中，噪声是网络中不属于重叠网络的节点集合Gc，即V1∪V2\Vc.
  为了量化噪声，引入重叠率λ=|Vc||V1∪V2|，那么，噪声比为1−λ.
- 全局去匿名化和局部去匿名化
  对于提高去匿名化的精度的需求，需要从原始网络中获取一个与匿名网络一样大的爬网网络。在这种情况下，噪声相对较低，并且对去匿名化几乎没有负面影响，去匿名化变得容易。这种去匿名化称为全局去匿名化，即|G1|≈|G2|
  对于只对网络中部分节点的信息感兴趣的很多情况，只对包含感兴趣节点的子网进行去匿名化。在这种情况下，只抓取目标附近的节点，并构建一个子网作为去匿名化的爬网网络。这种去匿名化称为本地去匿名化，即|G1|≪|G2|
- 

(a) original network **(b)** crawled network **(c)** anonymized network

- Rolematch

  RoleMatch 是一种快速的去匿名化算法，仅根据已爬网网络和匿名网络的结构信息对节点映射进行去匿名化处理。

  角色匹配主要采用两个网络G1和G2，初始化相似度矩阵得分后，根据结构信息迭代计算所有节点相似度对。相似性分数越高，表示成为正确节点映射的概率就越高。

  根据上一阶段计算的相似度得分，RoleMatch调用函数findNodeMatch生成最终节点映射。在这个函数中应用了一种称为NeighborMatch的匹配算法，该算法综合地结合了节点相似性和邻域反馈。

  Rolematch接受seeded，因为RoleMatch纯粹根据结构信息计算相似性，对于RoleMatch，seeded和seedless的唯一区别是，在计算节点相似性期间，如果提供了种子映射，则所有种子对的相似性得分在整个迭代过程中保持为不变，并且在节点匹配阶段，种子对在其他节点之前匹配。

- NeighborMatch

  匹配算法NeighborMatch基于两个观察结果：首先，正确的映射往往具有更高的相似性分数，其次，如果一对节点的邻居是正确的映射，则它们更有可能成为正确的映射。更具体地说，NeighborMatch 为每对节点分配优先级，并遵循优先级生成匹配。

  通过使用Kazemi等人提出的渗流网络匹配方法的思想，可以自动在线分配优先级。渗透网络匹配（PGM）基于种子生成结果。种子对在开头标记为匹配。然后，重复匹配匹配邻居数高于阈值 r 的节点对，直到不再有至少匹配 r 个邻居的不匹配对。NeighborMatch在开始时使用得分最高的对作为种子，在接下来的迭代中，当有多个候选项时，它总是选择得分最高的对。

  由于NeighborMatch是使用不同种子进行渗透网络匹配的变体，因此理论结果仍然有效并保证了NeighborMatch的性能。例如，假设一开始匹配了相似度得分最高的m对节点，并且m达到临界值，那么有很高概率，至少o（n）个节点可以成功去匿名化，其中n=|V1∩V2|

  此外，与原始的渗流网络匹配相比，NeighborMatch具有几个优点。网络渗透要求所有候选对之前至少匹配r个邻居，因此当没有有效的候选者时，匹配过程会卡住。该算法避免了卡住，因为相似性分数提供了自然而合理的候选对选择，即在所有不匹配的对中挑选出得分最高的一个。因此，该匹配算法能够匹配更多的节点对，即使是那些度数小于阈值r的节点对。

Problems & Expected Goals

在本次调研中，我们希望探究的问题和目标是：

1. 是否可以对已有的方法进行改进，来提高预测的准确率，得到更加行之有效的反匿名化方法
2. 结合前面对现有工作的分析，可以得到一个合理的猜想：如果能够结合Seedless method和存在种子节点信息的Seed method是否可以得到一个更好的方法
3. 对已有的工作进行复现和研究，得到这两种方法的具体理解，能够详细总结出两种方法在细节上的优/缺点

Execution Plan & Methodology

1. 明确需要反匿名化的社交网络数据的类型和范围，具体来说是否包括用户的个人信息，社交网络，用户行为，浏览记录，其他应用/社交网络的信息以及其他可能获取到的信息等。
2. 寻找/爬取质量较高的具备/不具备种子节点信息的数据集供Seed Method和Seedless Method测试使用，在收集数据时需要确保数据合法以及对数据集中的用户进行了隐私保护，遵循相关的法律法规和隐私政策。
3. 详细了解已调查/其他反匿名化的方法，确定要采用的方法，是Seed Method or Seedless Method or Mixture，提出已有方案的改进策略或者是新的方案
4. 对选定的方法和一些调研得到的方法在数据集上进行测试，观测其效果：
   - 对数据进行预处理，包括数据清洗、去重、标准化等操作

- 根据反匿名化方法，对数据进行分析和推断，揭示用户的身份信息
- 对揭示出来的用户身份信息进行验证和确认，确保准确性和可信度
- 针对反匿名化过程中可能涉及的隐私问题，采取相应的隐私保护措施，确保数据安全和隐私保护

5. 对反匿名化结果进行分析和报告，包括反匿名化准确度、效率、隐私保护措施等方面的评估和总结。同时需要对反匿名化结果进行解释和说明，确保结果的可理解性和可操作性。

References

- 数据匿名化，能保护你的隐私安全吗
- 利用Sage对Abstract和Motivation进行润色，修改了一些表达
- Fast De-anonymization of Social Networks with Structural Information
- An efficient reconciliation algorithm for social networks
- Community-Enhanced De-anonymization of Online Social Networks
- De-anonymizing social networks
- Link prediction in social networks: the state-of-the-art