

基于 DeepLink 的社交网络去匿名方法

王培, 贾焰, 李爱平, 蒋千越

(国防科技大学计算机学院, 湖南 长沙 410073)

摘要: 现有的社交网络去匿名方法主要是基于网络结构, 对网络结构进行学习并表示是去匿名的关键。用户身份链接 (user identity linkage) 的目的是检测来自不同社交网络平台的同一个用户。基于深度学习的跨社交网络用户对齐技术, 很好地学习了不同社交网络的结构特征, 实现了跨社交网络的用户对齐。将该技术用于同一社交网络匿名用户识别, 实验结果优于传统去匿名方法。

关键词: 匿名; 去匿名; 隐私; 社交网络; 图数据

中图分类号: TP183

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020045

De-anonymization method for networks based on DeepLink

WANG Pei, JIA Yan, LI Aiping, JIANG Qian Yue

College of Computer, National University of Defense Technology, Changsha 410073, China

Abstract: Existing de-anonymization technologies are mainly based on the network structure. To learn and express network structure is the key step of de-anonymization. The purpose of the user identity linkage is to detect the same user from different social networking platforms. DeepLink is a cross-social network user alignment technology. It learns the structural of the social networks and align anchor nodes through deep neural networks. DeepLink was used to identify de-anonymization social networks, and the results outperforms the traditional methods.

Key words: anonymization, de-anonymization, privacy, social network, graph data

收稿日期: 2019-07-16; 修回日期: 2019-09-17

通信作者: 李爱平, liaiping@nudt.edu.cn

基金项目: 国家重点研究发展计划基金 (2017YFB0802204, 2016YFB0800303, 2017YFB0803301, 2016QY03D0603, 2016QY03D0601, 2016QY01W0101); 国家自然科学基金 (61732004, 61732022, 61502517, 61472433, 61672020, U1803263); 东莞创新研究团队计划 (2018607201008)

Foundation Items: The National Key R&D Program of China (2017YFB0802204, 2016YFB0800303, 2017YFB0803301, 2016QY03D0603, 2016QY03D0601, 2016QY01W0101), The National Natural Science Foundation of China (61732004, 61732022, 61502517, 61472433, 61672020, U1803263), DongGuan Innovative Research Team Program (2018607201008)

论文引用格式: 王培, 贾焰, 李爱平, 等. 基于 DeepLink 的社交网络去匿名方法[J]. 网络与信息安全学报, 2020, 6(4): 104-108.

WANG P, JIA Y, LI A P, et al. De-anonymization method for networks based on DeepLink[J]. Chinese Journal of Network and Information Security, 2020, 6(4): 104-108.

1 引言

随着互联网技术的发展, 基于社交网络大数据的应用, 在为各行各业带来巨大收益的同时, 推动着大数据分析在各行业中的应用和进步。用户隐私是大数据行业的一个关键问题, 社交网络从一开始出现就与这个问题息息相关, 在未来挖掘和研究社交数据的道路上, 只有注重对用户隐私的保护^[1], 才能形成可持续的研究与发展。

社交网络可以用图结构来表示, 用节点来表示用户, 边来表示用户关系。许多网络的研究可以抽象成基于图结构网络的研究, 如 Wi-Fi 轨迹、蓝牙轨迹、即时消息、社交网络等。

在对基于图结构网络的研究过程中, 为了保护用户的隐私, 会对网络进行匿名处理。通过对匿名社交网络进行去匿名, 可以测试匿名技术的效果, 从而促进匿名技术的发展, 更好地保护用户的隐私。

Zhou 等^[2]提出的 DeepLink 是基于深度学习的跨社交网络用户对齐技术, 充分地学习了不同社交网络的结构特征, 实现了跨社交网络的用户对齐。本文将 DeepLink 技术用于同一社交网络匿名用户识别, 取得了不错的结果。

2 相关工作

2.1 用户身份链接技术

用户身份链接的目的是检测来自不同社交网络平台的同一个用户。解决这一问题的方法众多, 主要有基于用户特征的方法、基于用户产生内容的方法、基于用户行为的方法。此外, 包括从有监督、无监督到基于子空间的学习方法。上述方法通常需要提取用户相关特征(如用户 ID、昵称、坐标、签名、标签、行为习惯等)来对不同社交网络中的用户进行建模。但这些特征主要基于先验知识, 而且会随平台和应用的变化而变化。

基于近年来自动提取特征方面的成功经验, Zhou 等^[2]提出了基于深度神经网络的用户身份链接算法——DeepLink。它是一种半监督的学习方式, 主要基于网络结构, 不涉及任何用户特征提取与建模, 在与 IONE^[3]、ONE^[3]、MAH^[4]、MAG^[4]、CRW^[5]等方法的对比实验中效果突出。

2.2 图数据去匿名技术

图数据去匿名技术通过对比同一网络的不同匿名图, 识别来自本网络的用户。现有的去匿名技术主要包括基于种子节点的去匿名技术和无种子节点的去匿名技术。

基于种子节点的去匿名技术首先将某些用户识别为种子节点。Backstrom 等^[6]提出基于种子节点进行主动攻击和被动攻击, 这种方法不可扩展, 且容易防御。针对 Backstrom 的不足, Narayanan 和 Shmatikov^[7]对其作出了改进, 提出了可扩展的两阶段攻击方法。Nilizadeh^[8]等提出基于社区的去匿名方法, 该方法也增强了其他基于种子节点的攻击, 如 Srivatsa^[9]和 Ji^[10]的方法。

无种子节点的去匿名关键在于对网络结构的表示与学习^[11], 现有的完全无种子节点去匿名技术相对较少。Pedarsani^[12]主要依赖到其他节点的距离和度数来进行去匿名。Ji^[10]提出的是一种基于冷启动的优化算法。

3 基于 DeepLink 的去匿名方法设计

DeepLink 具有良好的网络学习与表示能力, 本文将该方法用于社交网络的去匿名。匿名社交网络及其辅助网络属于同一社交网络的不同匿名图。

3.1 社交网络匿名方法

采用 Hay^[13]提出来的方法对 Twitter 网络进行匿名处理生成匿名网络和辅助网络。该方法是基于边的匿名方法。首先随机删除一定数量的边, 其次随机添加同样数量的边, 该方法应用较为普遍。

3.2 网络结构采样

为了将用户嵌入一个潜在的空间, 通过随机游走为每个用户生成多个序列, 每个序列都是对用户社会关系的编码, 所有的序列合起来形成语料库, 并将其用来学习用户的嵌入向量。

采样过程如下: 从一个随机用户 v 开始, 每一步沿着随机选择的边进行, 直到达到长度 L 。这样不仅可以提取隐藏的网络结构, 而且可以捕捉其所代表的社会信息, 如网络中的好友关系和社区属性。

3.3 用户向量嵌入

通过随机游走获取用户语料库之后, 采用

Skip-Gram 模型来更新每个用户的结构表示。

Skip-Gram 是一种无监督学习技术,可以预测给定用户的相邻用户。Skip-Gram 可以表示为由输入层、映射层(隐藏层)和输出层组成的神经网络。输入层中每个用户由 One-hot 编码方式表示,即所有用户均表示成一个 N 维向量,其中, N 为用户表中用户的总数。在向量中,每个用户都将与之对应的维度置为 1,其余维度的值均为 0。输出层向量的值可以通过映射层向量 (K 维),以及连接映射层和输出层之间的 $K \times N$ 维权重矩阵计算得到。输出层也是一个 N 维向量,每维与用户表中的一个用户相对应。最后对输出层向量应用 softmax 激活函数,可以计算每一个用户的生成概率。训练神经网络的权重,使语料库中所有用户的整体生成概率最大,使网络尽可能地预测所有用户的社会信息。Skip-Gram 最终的学习目的是通过训练好神经网络,获得映射矩阵,将每个用户映射到相应的特征向量。为了提高效率,采用负采样的方法进行优化。

3.4 多层神经网络

在获取用户向量空间之后,基于一定数量的种子节点,通过多层感知机来学习从匿名图到辅助图的映射。假设种子节点对为 (U_a, U_x) ,其对应的向量对为 (V_a, V_x) ,其中 U_a 来自匿名网络 G_a , U_x 来自辅助网络 G_x 。从匿名图到辅助图的映射为 φ ,可以通过如式(1)所示的最小化损失函数

$$\text{loss} = \min(1 - \cos(\varphi(V_a), V_x)) \quad (1)$$

优化神经网络,学习映射函数 φ 。这里 $\cos()$ 代表余弦相似性,损失函数 loss 介于 0 和 2 之间,0 代表两个向量完全相同,2 代表两个向量完全相反。

假设有 n 对种子节点对,它们的向量矩阵可以分别表示为 $A \in R^{d \times n}$, $B \in R^{d \times n}$, d 表示用户嵌入向量的维度。网络的损失函数如式(2)所示。

$$l(A, B) = \argmin_{W, b} (1 - \cos(\varphi(A), B; W, b)) \quad (2)$$

其中, W 为权重矩阵, b 为偏置向量,通过 R 轮迭代直到收敛。将训练好的神经网络进行测试,即可评估本文方法的可行性。

4 实验

实验使用 Nilizadeh^[8]提供的 Twitter 数据集,该数据集包括 9 745 个用户和 50 164 种用户关系。通过 Hay 等^[13]提出的匿名算法,从网络中随机删除、增加 15% 的边,分别产生匿名网络与辅助网络。本实验为了充分获取结构信息,对网络进行了 10 轮的随机游走,游走长度为 40。

实验选取 5% 的锚节点作为训练集,95% 的节点用来测试。测试的指标选取 Precision@ k (P@ k)。P@ k 可以用来衡量用户识别的准确率,如式(3)所示。

$$P@k = \sum_i^n \frac{l_i \{\text{success}@k\}}{n} \quad (3)$$

其中, $l_i \{\text{success}@k\}$ 表示最相似的 k 个用户中是否存在正确匹配用户,如果存在为 1,否则为 0。

(1) 维度对结果的影响

本文研究了用户嵌入向量的维度对准确率的影响,结果如表 1 所示。本实验中,当维度为 100 时,效果最好。实验结果表明:不是维度越高,准确率越高。

表 1 维度与准确率的关系
Table 1 The relationship between dimensions and accuracy

维度	准确率					
	P@1	P@5	P@10	P@15	P@30	P@100
400	66%	80%	83%	83%	84%	84%
200	67%	81%	83%	84%	85%	85%
100	78%	88%	90%	91%	91%	91%
50	67%	81%	84%	85%	85%	85%

(2) 迭代轮数对结果的影响

本文研究了迭代次数对准确率的影响,实验结果如图 1 所示。该实验中,用户嵌入向量的维度为 50。实验结果表明:随着训练轮数的上升,各个准确度指标都有所提高,在接近 10 000 轮训练的时候,准确度趋于稳定。

(3) 与 DeepLink 实验对比

本文对比了 DeepLink 在不同的两个场景下的表现,两个场景分别是本文中提出的同质网络和文献[2]中使用的非同质网络。对比结果如表 2 所示。对比结果表示 DeepLink 在同质

表2 本文方法与 DeepLink 对比
Table 2 The comparison of our method and DeepLink

方法	准确率					
	P@1	P@5	P@10	P@15	P@30	P@100
本文方法	78%	88%	90%	91%	91%	91%
DeepLink	33%	57.4%	64.9%	67.2%	69.4%	69.8%

网络中取得了更好的结果。原因在于本文中的匿名网络和辅助网络属于同一个社交网络, 结构比较相似, DeepLink 能够充分地利用网络结构信息。

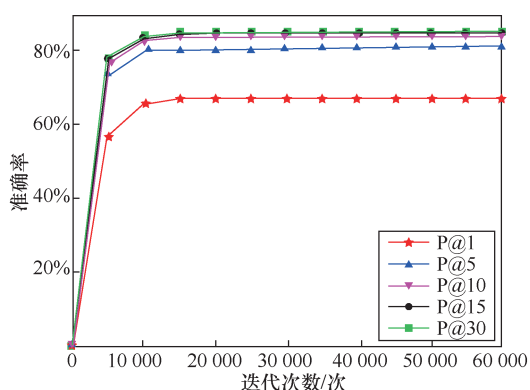


图1 迭代次数与准确率关系

Figure 1 The relationship between iterations and accuracy

(4) 与 Ji^[8]、Nilizadeh^[9]实验对比

本节将本文方法与 Ji、Nilizadeh 的方法进行对比, 结果如表 3 所示。实验中数据集相同, 匿名图与辅助图也相同。实验结果表明, 本文的方法与 Nilizadeh 的实验结果一样, 比 Ji 的方法准确率高。

表3 本文方法与 Ji、Nilizadeh 对比
Table 3 The comparison of our method, Ji and Nilizadeh

方法	准确率
本文方法	78%
Ji ^[7]	40%
Nilizadeh ^[8]	78%

5 结束语

本文将 Deeplink 技术用于同一社交网络匿名使用户识别, 实验结果表明, DeepLink 方法在社交网络去匿名应用中处于领域领先水平。该方法能够充分学习网络的结构信息, 虽然种子节点只有 5%, 但实验结果仍然较好。

该方法还有值得进一步讨论与改进的地方。一是可以增加改动的边数来提高网络的匿名水平。二是可以采用不同的匿名方法对社交网络进行匿名处理, 研究该方法对不同匿名技术的还原能力。三是可以采用 LINE^[14]、GraRep^[15]等其他方法生成用户节点的语料库, 探索节点表示的其他可能性。四是可以增加种子节点的比例来探究网络的去匿名能力。

参考文献:

- [1] 姚瑞欣, 李晖, 曹进. 社交网络中的隐私保护研究综述[J]. 网络与信息安全学报, 2016, 2(4): 33-43.
YAO R X, LI H, CAO J. Overview of privacy preserving in social network[J]. Chinese Journal of Network and Information Security, 2016, 2(4): 33-43.
- [2] ZHOU F, LIU L. DeepLink: a deep learning approach for user identity linkage[C]//IEEE International Conference on Computer Communications. 2018: 1313-1321.
- [3] LIU L, CHEUNG W K, LI X, et al. Aligning users across social networks using network embedding[C]//International Joint Conference on Artificial Intelligence. 2016: 1774-1780.
- [4] TAN S, GUAN Z, CAI D, et al. Mapping users across networks by manifold alignment on hypergraph[C]//AAAI Conference on Artificial Intelligence. 2014: 159-165.
- [5] ZHANG J, YU P S. Integrated anchor and social link predictions across social networks[C]//International Joint Conference on Artificial Intelligence. 2015: 2125-2132.
- [6] BACKSTROM L, DWORK C, KLEINBERG J. Wherefore art thou r3579x? anonymized social networks, hidden patterns, and structural steganography[C]//International World Wide Web Conference. 2007: 181-190.
- [7] NARAYANAN A, SHMATIKOV V. De-anonymizing social networks[C]//IEEE Symposium on Security and Privacy. 2009: 173-187.
- [8] NILIZADEH S, KAPADIA A, AHN Y Y. Community-enhanced de-anonymization of online social networks[C]//ACM Conference on Computer and Communications Security. 2014: 537-548.
- [9] SRIVATSA M, HICKS M. De-anonymizing mobility traces: using social networks as a side-channel[C]//ACM Conference on Computer and Communications Security. 2012: 628-637.
- [10] JI S, LI W, SRIVATSA M, et al. Structure based data de-anonymization of social networks and mobility traces[C]//Information Security Conference. 2014: 237-254.
- [11] 尹赢, 吉立新, 黄瑞阳, 等. 网络表示学习的研究与发展[J]. 网络与信息安全学报, 2019, 5(2): 77-87.

YIN Y, JI L X, HUANG R Y, et al. Research and development of network representation learning[J]. Chinese Journal of Network and Information Security, 2019, 5(2): 77-87.

- [12] PEDARSANI P, FIGUEIREDO D R, GROSSGLAUSER M. A bayesian method for matching two similar graphs without seeds[C]//The 51st Annual Allerton Conference on Communication, Control & Computing. 2013: 1598-1607.
- [13] HAY M, MIKLAU G, JENSEN D, et al. Anonymizing social networks[C]// Computer Science Department Faculty Publication Series. 2007: 180-196.
- [14] TANG J, QU M, WANG M, et al. Line: large- scale information network embedding[C]//International World Wide Web Conference. 2015: 1067-1077.
- [15] CAO S, LU W, XU Q. Grarep: learning graph representations with global structural information[C]//ACM International on Conference on Information & Knowledge Management. 2015: 891-900.



贾焰（1960—），女，四川成都人，博士，国防科技大学教授、博士生导师，主要研究方向为网络空间安全。



李爱平（1974—），男，山东诸城人，博士，国防科技大学研究员、博士生导师，主要研究方向为网络空间安全。

[作者简介]



王培（1991—），男，山西运城人，国防科技大学硕士生，主要研究方向为网络空间安全。



蒋千越（1990—）男，黑龙江齐齐哈尔人，国防科技大学硕士生，主要研究方向为网络空间安全。