# TrustGeo: 一种用于可信赖 IP 地理位置定位的不确定性感知动态图学习

**摘要**

在线网络社交等多种网络服务需要获取准确的用户位置信息，但是现存的多种定位 IP 地址的技术大都依赖于 GPS、手机信号塔、和 WiFi 获取用户位置数据，这些技术在获取用户位置时必须要获得用户的授权才能进行，因此当基于位置的访问受到限制时，这种方式就不再适用。而一些已有的基于深度学习和机器学习的 IP 地址定位技术由于准确性和可靠性低，并没有大范围推广使用。为了改进这种技术，文章提出了 TrustGeo，通过结合不确定性感知和动态图学习，以提高地理定位的准确性和可靠性，此外 TrustGeo 还会生成置信度分数（又名认知不确定性），为开发人员提供额外的信号来监控系统的性能。

**关键词：** GNN；置信度；IP 地址定位；

## 1 引言

大多数应用在为用户提供服务时需要获取用户的精确地理定位，如在一些导航软件中，用户地址定位的准确程度极大程度上影响用户体验度，但是现存的 IP 定位技术一般利用网络延迟和地理距离之间的正相关性，通过地标服务器到目标 IP 的跟踪路由将网络延迟与拓扑测量相结合以进行位置估计，但是这种测量技术过于依赖网络传输，影响了模型的泛化能力；有的 IP 定位技术通过用户数据如用户网页内容、社交信息图表、用户注册记录、邮政信息等实现达到的精准程度却并不能达到要求，但是这种基于网络挖掘的方法通常受到不可靠和不完整的信息的限制，因为被动的网络数据收集很容易导致地理定位不准确；另外，随着深度学习和神经网络的大规模兴起，深度学习工具在应用类机器学习中获得了极大的关注，有些模型尝试将机器学习中的方法应用于 IP 定位，但是用于回归和分类的工具并不能捕获模型的不确定性，模型无法估计自身的置信度。因此本文在先前提出的基于 GNN 的 IP 地址定位模型 GraphGeo 上进行改进，在使用 GNN 的基础上，通过对 NN 的数据不确定性和预测不确定性进行建模，预测不确定性解释了模型参数的不确定性，从而可以用来描述模型学习内容的置信度。在之前，已经有人使用贝叶斯神经网络预测模型的不准确性，但是使用贝叶斯模型的计算成本高昂并且需要训练大量模型实例，因此我们在此基础上做出改进，使用基于证据深度学习代替贝叶斯神经网络在单个模型中进行不确定性估计，并通过参数化分布上的分布来进行前向传递，从而大大节省了训练的时间成本。总结来说，TrustGeo 在两个方面进行了创新：

1. 在计算地表主机到目标 IP 地址之间的网络延迟时，不仅仅依靠它们之间的属性相似性对 IP 地址聚类测量网络距离，还通过公共路由器对距离进行限制，缩小 IP 聚类的范围，防止相对距离计算不准确。

2. 使用基于证据的深度学习计算模型的数据不确定性和预测不确定性，考虑网络测量不确定性和 IP 图的动态变化，使其在现实世界的 IP 地理定位服务中更值得信赖。

并且使用纽约、洛杉矶、上海三个大都市的 IP 地址信息数据集进行了模型训练和广泛的实验结果评估，得出的评估结果证明 TrustGeo 在各方面都具有较好的性能。

## 2 相关工作

在此介绍之前 IP 地址定位使用的技术方法，特点以及不足，本文在此基础上做出的改进。以及本文提到的方法主要技术介绍，包括动态图学习（GNN）和基于证据的深度学习网络。

### 2.1 传统 IP 地址定位方法分析

传统 IP 地址定位方法主要分为三种

1. 挖掘网络 cookie 进行 IP 定位。在现存的 IP 地址定位技术中 Checkin-Geo [7] 利用用户愿意在位置共享服务中共享的位置数据以及用户从 PC 登录的日志来进行地理定位。GeoCAM [12] 定期监控托管实时网络摄像头的网站以提取位置信息。这些方法的缺点在前文已经描述，不仅定位有局限性，而且会在一定程度上侵犯用户的隐私。

2. 利用网络延迟计算地理距离，网络延迟与地理距离之间成正比，基于这个原理的 IP 地址定位占现有技术的大多数，早期的工作 GeoPing [10] 将 ICMP 数据包从地理上分布的探测主机发送到目标 IP，该目标 IP 通过最近的地标服务器的位置进行本地化。CBG [5] 在地球表面围绕每个地标服务器创建圆圈，并使用多边定位来推断目标 IP 的位置。作为网络延迟的补充，TBG [3] 使用从地标服务器到目标 IP 的跟踪路由将网络延迟与拓扑测量相结合以进行位置估计。Spotter [6] 是一种概率密度模型，它导出了常见的延迟距离模型，并利用最高概率密度来定位目标主机。

3. 利用机器学习和深度学习。如 NN-Geo [4] 从多个观察者收集 RTT（往返时间）作为特征，并使用 RBF（径向基函数）神经网络来精确定位 IP。GNN-Geo [2] 将 IP 地理定位重新表述为属性图节点回归问题，并设计一个基于 GNN 的框架来利用来自目标 IP 主机的周围知识。GraphGeo [13] 从拓扑和语义角度建立 IP 主机之间的邻域关系以形成加权图，并通过不确定性感知的 GNN 聚合其邻居的知识以进行 IP 地理定位。

### 2.2 动态图学习

图神经网络（Graph Neural Network，GNN）是一种专门用于处理图结构数据的神经网络模型如图1。[9] 与传统神经网络不同，GNN 能够捕捉图中节点之间的复杂关系，并通过迭代更新节点表示来学习图的整体结构特征。GNN 的核心是一种通过节点之间的信息传递捕捉

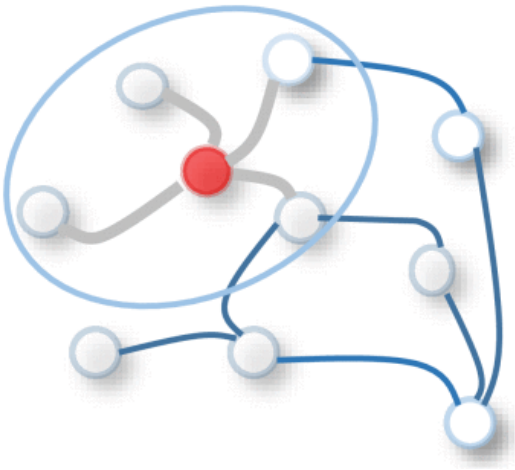


图 1. 动态图学习示意图 [14]

图形依赖关系的神经模型。[16] 基于 CNN 和图嵌入，图神经网络（GNNs）的变体被提出，用于从图结构中集体聚合信息。因此，它们可以对由元素及其依赖关系组成的输入和输出进行建模。GNN 的核心思想是通过迭代的方式聚合邻居节点的表示来更新当前节点的表示。这一过程通常包括以下几个关键步骤：[15]

1. 初始化节点表示：为每个节点分配一个初始的特征向量。
2. 邻居聚合：根据节点的邻居信息，通过聚合函数（如求和、平均、最大池化等）更新节点表示。
3. 节点更新：结合节点自身的特征和聚合后的邻居信息，通过更新函数（如非线性激活函数）更新节点表示。
4. 输出表示：根据任务需求，从更新后的节点表示中提取输出信息。

### 2.3 基于证据的深度学习网络

这是一种训练非贝叶斯神经网络，以估计连续目标及其相关证据，从而学习随机性和认知不确定性的方法。方法通过在原始高斯似然函数上放置证据先验，并训练神经网络推断证据分布的超参数来实现这一点。此外，模型在训练过程中施加先验，使得当模型预测的证据与正确输出不一致时，模型得到正则化。方法在推理过程中不依赖于采样，也不依赖于训练中的分布外（OOD）示例，从而实现了高效和可扩展的不确定性学习 [1]

证据深度学习模型框架如图2，模型将学习过程定义为证据获取过程。每个训练示例都为学习到的更高阶的证据分布提供支持。从这个分布中采样产生低阶似然函数的实例，绘制这些来自数据的实例，与贝叶斯神经网络中将先验放在网络权重上的做法不同，证据方法直接将先验放在似然函数上。通过训练神经网络输出高阶证据分布的超参数，可以在不进行采样的情况下学习到关于认知和随机不确定性的基于证据的表示。方法执行的步骤可以概括为以下几步：

1. 通过正态逆伽马（Normal Inverse-Gamma, NIG）分布作为高阶证据分布，用于建模均值和方差的不确定如图3

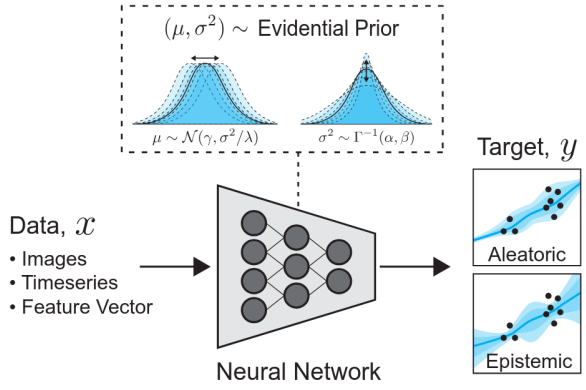



图 2. 基于证据的深度学习网络框架：给定一个输入，网络被训练来预测证据分布的参数，该分布模拟了单个似然参数的高阶概率分布。[1]

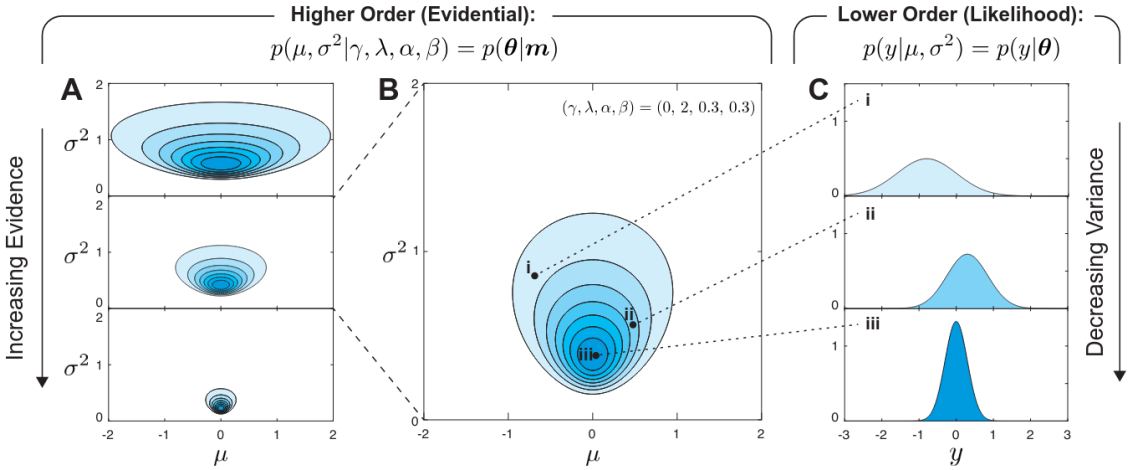



图 3. 正态逆伽马分布 [1]

2. 建立证据先验：在高斯似然函数上放置证据先验，这些先验直接作用于数据的均值和方差参数。

3. 训练神经网络：训练一个神经网络来预测输入数据对应的 NIG 分布的超参数，即 （均值的先验均值）、（均值的“虚拟观测”数量）、（方差的“虚拟观测”数量）和 （方差的缩放参数）。

4. 证据正则化：实施一个证据正则化器，当模型预测错误时，通过增加不确定性来惩罚模型。

5. 构建损失函数并利用损失函数进行模型优化：构建包含最大化模型拟合和最小化错误证据的损失函数，并将这两个部分通过一个正则化系数 结合起来，使用梯度下降或其他优化算法来最小化损失函数，从而学习神经网络的参数和 NIG 分布的超参数。

6. 不确定性估计：利用学习到的 NIG 分布超参数来估计每个预测的不确定性，包括预测的均值、方差、以及由此派生的不确定性度量。

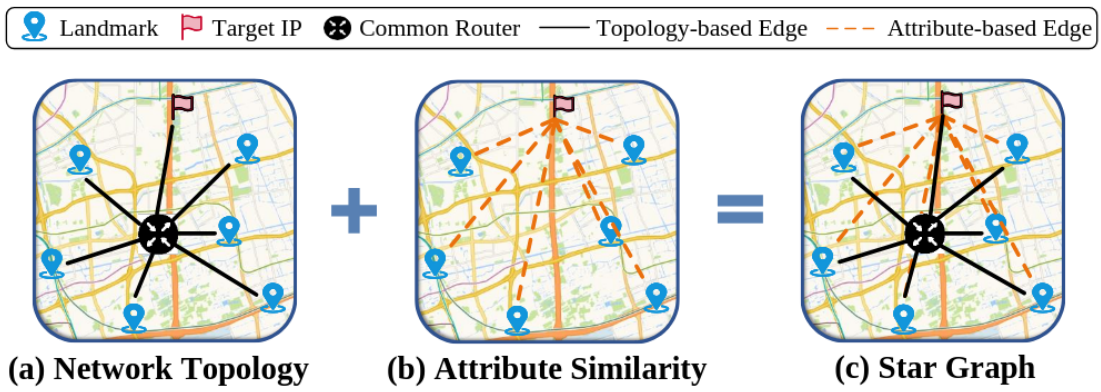



图 4. 构建 star-graph。我们将普通路由器视为星型节点，将目标 IP 和地标视为卫星节点。所提出的星图采用“多管齐下”的方法，其中考虑已知属性，同时寻找 IP 网络中可利用的结构。[13]

## 3 本文方法

### 3.1 本文方法概述

本文对于 IP 地址定位的方法主要分为两步：首先根据 GNN 构建出 Star-graph，在之前的研究中使用地标和目标主机构建图，直接使用地标 IP 和目标 IP 到路由器的延迟差作为地标和目标 IP 主机之间延迟的近似。这种方法中的延迟计算不准确导致 IP 预测效果不佳。因此本文提出使用 Star GNN 构建星形图，星形图由一个星形节点和多个卫星节点组成，其中星形节点与所有卫星节点相连，可以向它们传递消息。构建 star graph 以更自然的方式融合 IP 主机和邻居关系的特征信息。

然后将基于图的 IP 地理位置视为多视图决策融合任务，定义了用于地理位置的信息来自两个方面：目标 IP 本身的信息和其邻居的协作信息。使用基于证据的深度学习网络计算每个视图（自信息视图和邻居视图）的不确定性，并使用这些不确定性作为标准来适应性地融合不同视图的信息。

最后在纽约、上海、洛杉矶三个大都市的 IP 地址信息数据集上进行了广泛的实验，以验证 TrustGeo 在提高街道级 IP 地理位置准确性和可靠性方面的有效性。

### 3.2 构建 star-graph

定义公共路由器为星型节点，目标 IP 和地标主机为卫星节点构建 star-graph 如图4。首先基于目标 IP，地标 IP 和他们之间的公共路由器构建网络拓扑图。通过使用 “tranceroute“工具探测位于不同城市的主机并查找距离目标 IP 延迟最小的最后一跳路由器，通过地标主机的位置和到公共路由器的往返时间（RTT）构建拓扑连接（设置边的权重与 RTT 成反比）。

接着构建不同卫星节点之间的直接连接，由于地理位置相似的节点通常具有相似的属性，因此可以通过它们特征向量的点积来计算它们的相似性。将相似性作为连接卫星节点的边的权重。

将两种图结合构成 star-graph，对于已经建立的 star-graph，由于图中只有卫星节点具有属性信息，因此使用卫星节点的平均池化作为星型节点的信息。然后使用目标 IP 的邻域信息

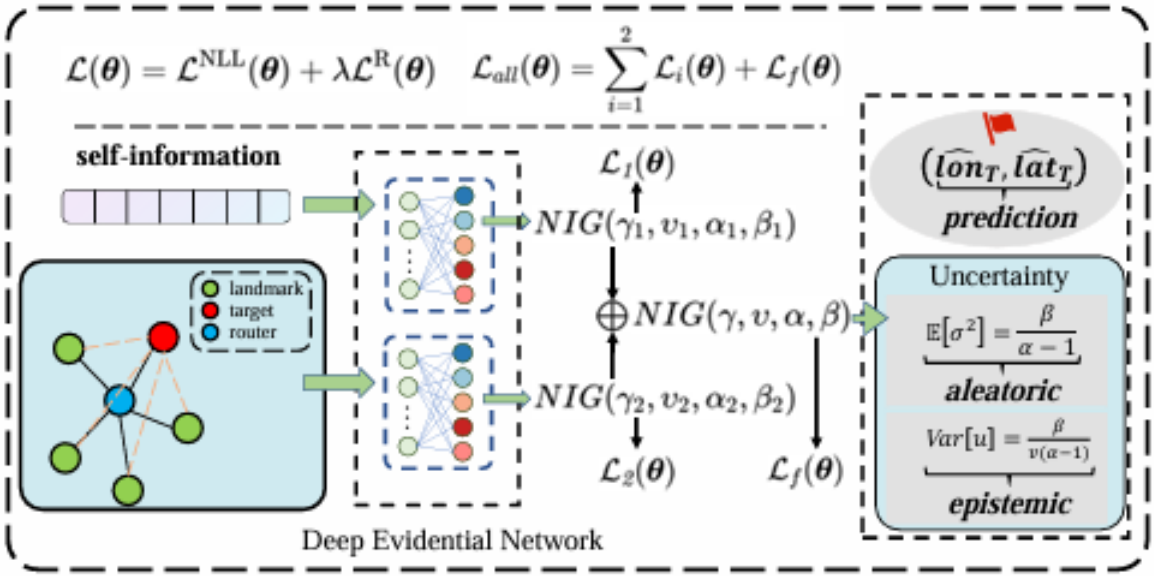



图 5. TrustGeo 模型图示 [11]

对目标 IP 地址的卫星节点进行迭代更新，迭代更新两次后获取到目标 IP 的预测信息。

### 3.3 量化不确定性用于模型训练

方法在进行估计时没有明确地模拟任何潜在的噪声或不确定性，但是在现实场景中，IP 地址的属性信息有可能不准确或者过时，当网络出现拥塞或波动时，ping 和 tranceroute 测量到的数据可能不可靠；此外构建 GNN 模型时，也会因为邻居节点的稀疏影响预测的准确度，因此对模型进行网络不确定性测量和动态图不确定性测量，检测预测结果的不确定性，并及时提醒用户。

1. 基于证据的深度学习网络框架进行网络不确定性测量：首先在未知方差上放置一个高斯先验分布，在未知均值上放置一个逆伽玛先验分布，使用贝叶斯定理，结合先验分布和似然函数，推导出后验分布，使用正态逆伽马分布作为后验分布的近似。

2. 动态图不确定性测量：使用一种新的信息融合算法，通过捕获不同视图的不确定性作为标准自适应地融合不同视图的信息如图5。分别将分别将证据不确定性学习（2.3 节）应用于自信息视图和图学习视图获得两个 NIG 分布，将两个 NIG 分布基于图的不准确性进行融合 [8]。损失函数计算：损失函数定义为负对数似然率与正则化项的和。将模型总的损失函数表示为两个视图的损失函数与融合分布的损失函数之和。将多任务学习损失反向传播以进行模型优化。

   模型训练主要分为两个阶段：

   (a) 增加模型证据，通过最大化模型证据来优化模型参数。

   (b) 当预测不正确时，减少证据（增加不确定性）这通过引入一个正则化项来实现，该正则化项在预测错误时增加损失函数的值对模型施加惩罚。

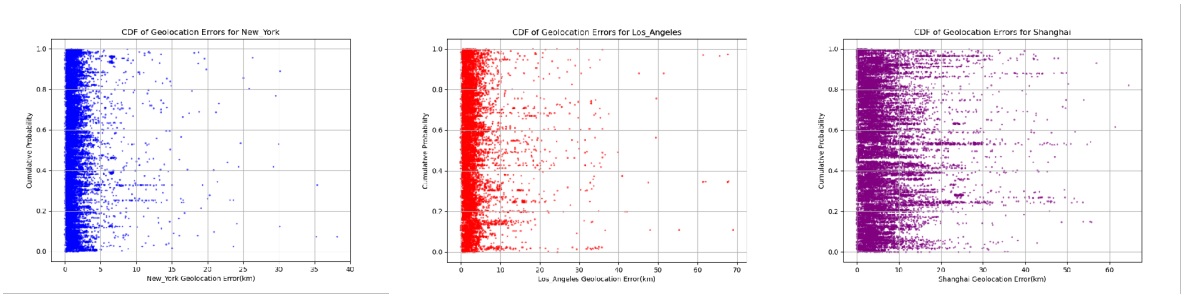
# 4 复现细节

## 4.1 数据集处理

使用作者提供的数据集进行训练，文章提供了纽约、洛杉矶和上海三个大都市的 IP 地址数据集，分别包含 91,808、92,804 和 126,258 个 IP 地址，对数据集进行划分，选择 80% 的 80% IP 进行训练，其余 20% 进行测试。在训练过程中，将 70% 的 IP 作为地标，30% 作为目标 IP。测试过程中，将训练集视为地标，将其他集视为目标 IP 来报告结果。利用五倍交叉验证程序来减轻随机数据选择造成的偏差。

## 4.2 与已有开源代码对比

与已有开源代码相比，本文使用 matplotlib 画出了不同城市的 IP 地址分布的累积分布图如8a8b8c图所示。




(a) 纽约累积分布图　(b) 洛杉矶累积分布图　(c) 上海累积分布图

图 6. 三个数据集中 IP 地址预测误差累积分布图

## 4.3 实验环境搭建

复现使用 Intel(R) Core(TM) i9-14900K CPU 的系统上进行的，该 CPU 的最大运行频率为 6 GHz，每个插槽拥有 32 个核心和 24 个线程。该系统由两块 NVIDIA GeForce RTX 4090 GPU 提供动力，每块 GPU 配备 24GB 的 GDDR6 内存，驱动版本为 565.57.01，支持 CUDA 12.7。操作系统是 Ubuntu 22.04.5 LTS (Jammy Jellyfish) 的设备

## 4.4 界面分析与使用说明

如图8a8b8c所示，绘制出三个数据集训练结果的累积分布函数图，横轴表示地理位置定位误差，纵轴表示累积概率。它显示了定位误差小于或等于横轴上某个特定值的样本所占的百分比，每个点代表一个定位误差值及其对应的累积概率，通过观察图可以得到定位误差的分布特征，由图可以观察到误差分布：纽约 < 洛杉矶 < 上海，这与作者在论文中得到的结论（如图7）相同。表中的 RMSE 均方根误差对大误差更加敏感，MAE 表示平均绝对误差，提供一个平均误差的度量，Median 中位数误差，提供预测误差分布中心趋势的信息。通过不同模型在三个数据集上运行得到的参数对比可以得出当前模型的预测误差更小，各方面性能更优的结论。

| Type | Method | Time | New York | | | Los Angeles | | | Shanghai | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | RMSE | MAE | Median | RMSE | MAE | Median | RMSE | MAE | Median |
| Delay Measurement Methods | GeoPing | 2001 | 14.25 | 11.66 | 10.24 | 18.19 | 13.40 | 9.450 | 29.23 | 24.84 | 22.23 |
| | CBG | 2006 | 18.74 | 14.89 | 11.97 | 21.05 | 17.77 | 13.93 | 34.60 | 28.77 | 24.28 |
| | TBG | 2006 | 16.20 | 13.15 | 10.57 | 17.98 | 15.60 | 12.32 | 27.24 | 22.53 | 19.97 |
| | NCRGeo | 2018 | 3.252 | 2.518 | 2.110 | 7.006 | 5.684 | 5.012 | 9.839 | 6.746 | 5.240 |
| | XLBoost-Geo | 2020 | 3.005 | 2.179 | 1.572 | 6.820 | 4.577 | 4.129 | 9.990 | 6.850 | 5.242 |
| Attribute Learning Methods | NN-Geo | 2016 | 7.740 | 6.369 | 5.654 | 11.19 | 9.322 | 8.672 | 10.25 | 7.178 | 5.148 |
| | LightGBM | 2017 | 3.356 | 2.963 | 2.827 | 6.968 | 5.878 | 5.119 | 9.924 | 6.431 | 4.898 |
| | MLP-Geo | 2020 | 7.127 | 5.858 | 5.077 | 10.54 | 8.651 | 7.567 | 10.03 | 7.017 | 5.107 |
| | TabNet | 2021 | 3.985 | 3.272 | 3.198 | 7.252 | 6.262 | 5.189 | 9.986 | 6.722 | 5.012 |
| Graph Learning Methods | GNN-Geo | 2021 | 3.014 | 2.135 | 1.618 | 6.807 | 4.655 | 4.039 | 9.645 | 6.026 | 4.482 |
| | GraphGeo | 2022 | 2.681 | 1.614 | 1.118 | 6.621 | 3.778 | 2.269 | 9.051 | 5.981 | 3.982 |
| **Ours** | **TrustGeo** | - | **2.283** | **1.316** | **0.888** | **5.025** | **2.793** | **1.786** | **8.389** | **5.457** | **3.619** |

图 7. 论文测试结果 [11]

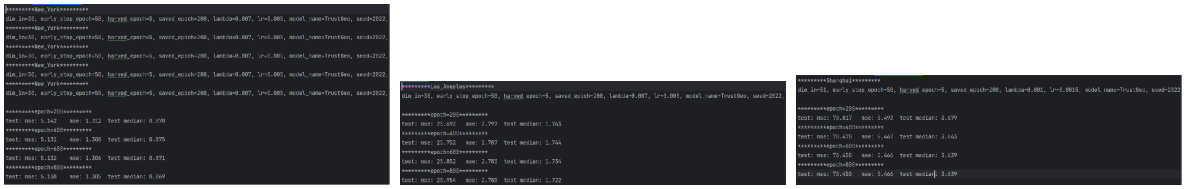
### 4.5 创新点

使用可视化方式显示预测出的 IP 地址的累积分布函数，通过累积分布函数（CDF）图像的引入，不仅展示了定位误差的总体趋势，还为模型性能的局部特性提供了更直观的对比依据，使得实验评估不再局限于单一数值，增强了对结果的多维解读能力。提供了模型在不同误差区间的表现分布（例如 90% 样本误差小于 30 千米），更易与其他模型进行性能对比。可以帮助识别特定区域模型性能不足的情况，为数据集扩充或模型微调提供依据。

## 5 实验结果分析

对于纽约、洛杉矶和上海数据集，最佳学习率分别设置为 0.005、0.003、0.0015。系数 lamda 分别设置为 0.007、0.007、0.001。

参数表示：epoch 表示遍历次数，MSE 均方根误差，MAE 表示平均绝对误差，Median 中位数误差，提供预测误差分布中心趋势的信息，如果 MSE 和 MAE 在连续多个 epoch 后保持稳定，这通常意味着模型已经收敛，即模型的参数已经优化到在当前数据集上的最佳状态。观察图中参数变化即可得出模型已经收敛的结论。



(a) 纽约数据集测试结果　(b) 洛杉矶数据集测试结果　(c) 上海数据集测试结果

图 8. 实验结果展示图

## 6 总结与展望

本文通过动态图学习和基于证据的深度学习模型，有效解决了传统 IP 地址定位中准确性和可靠性不足的问题。TrustGeo 实现了对预测不确定性的量化，显著提升了模型的泛化能力和实践价值。实验结果表明，本文方法在大规模数据集上的表现优于现有技术，尤其是在街道级别的精确定位任务中。引入对抗性训练机制以进一步提升模型对异常数据的鲁棒性，或者结合因果推理技术，消除潜在的偏置因素，构建更加稳定的预测框架。此外，还可以考虑在本文使用的方法上进行应用扩展，例如拓展至恶意 IP 检测和网络安全领域，形成多任务处理能力，在智能交通、物流路径优化等场景下测试其实际应用效果。

## 参考文献


[1] Alexander Amini, Wilko Schwarting, Ava Soleimany, and Daniela Rus. Deep evidential regression. *Advances in neural information processing systems*, 33:14927–14937, 2020.

[2] Shichang Ding, Xiangyang Luo, Jinwei Wang, and Xiaoming Fu. Gnn-geo: A graph neural network-based fine-grained ip geolocation framework. *IEEE Transactions on Network Science and Engineering*, 10(6):3543–3560, 2023.

[3] Bamba Gueye, Artur Ziviani, Mark Crovella, and Serge Fdida. Constraint-based geolocation of internet hosts. In *Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement*, IMC '04, page 288–293, New York, NY, USA, 2004. Association for Computing Machinery.

[4] Hao Jiang, Yaoqing Liu, and Jeanna N. Matthews. Ip geolocation estimation using neural networks with stable landmarks. In *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 170–175, 2016.

[5] Ethan Katz-Bassett, John P. John, Arvind Krishnamurthy, David Wetherall, Thomas Anderson, and Yatin Chawathe. Towards ip geolocation using delay and topology measurements. In *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, IMC '06, page 71–84, New York, NY, USA, 2006. Association for Computing Machinery.

[6] Sándor Laki, Péter Mátray, Péter Hága, Tamás Sebők, István Csabai, and Gábor Vattay. Spotter: A model based active geolocation service. In *2011 Proceedings IEEE INFOCOM*, pages 3173–3181. IEEE, 2011.

[7] Hao Liu, Yaoxue Zhang, Yuezhi Zhou, Di Zhang, Xiaoming Fu, and K.K. Ramakrishnan. Mining checkins from location-sharing services for client-independent ip geolocation. In *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pages 619–627, 2014.

[8] Hang Qian. Big data bayesian linear regression and variable selection by normal-inverse-gamma summation. *Bayesian Anal*, 2018.

[9] Benjamin Sanchez-Lengeling, Emily Reif, Adam Pearce, and Alexander B. Wiltschko. A gentle introduction to graph neural networks. *Distill*, 2021. https://distill.pub/2021/gnn-intro.

[10] Wenxin Tai, Bin Chen, Fan Zhou, Ting Zhong, Goce Trajcevski, Yong Wang, and Kai Chen. Trustgeo: Uncertainty-aware dynamic graph learning for trustworthy ip geolocation. In *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, pages 4862–4871, 2023.

[11] Wenxin Tai, Bin Chen, Fan Zhou, Ting Zhong, Goce Trajcevski, Yong Wang, and Kai Chen. Trustgeo: Uncertainty-aware dynamic graph learning for trustworthy ip geolocation. In *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, KDD '23, page 4862–4871, New York, NY, USA, 2023. Association for Computing Machinery.

[12] Zhihao Wang, Qiang Li, Jinke Song, Haining Wang, and Limin Sun. Towards ip-based geolocation via fine-grained and stable webcam landmarks. In *Proceedings of The Web Conference 2020*, WWW '20, page 1422–1432, New York, NY, USA, 2020. Association for Computing Machinery.

[13] Zhiyuan Wang, Fan Zhou, Wenxuan Zeng, Goce Trajcevski, Chunjing Xiao, Yong Wang, and Kai Chen. Connecting the hosts: Street-level ip geolocation with graph neural networks. In *Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, KDD '22, page 4121–4131, New York, NY, USA, 2022. Association for Computing Machinery.

[14] Zonghan Wu, Shirui Pan, Fengwen Chen, Guodong Long, Chengqi Zhang, and S Yu Philip. A comprehensive survey on graph neural networks. *IEEE transactions on neural networks and learning systems*, 32(1):4–24, 2020.

[15] Keyulu Xu, Weihua Hu, Jure Leskovec, and Stefanie Jegelka. How powerful are graph neural networks? *arXiv preprint arXiv:1810.00826*, 2018.

[16] Jie Zhou, Ganqu Cui, Shengding Hu, Zhengyan Zhang, Cheng Yang, Zhiyuan Liu, Lifeng Wang, Changcheng Li, and Maosong Sun. Graph neural networks: A review of methods and applications. *AI open*, 1:57–81, 2020.