

Beijing Forest Studio
北京理工大学信息系统及安全对抗实验中心



网络拓扑混淆技术

硕士研究生 刘栋涵

2025年4月26日

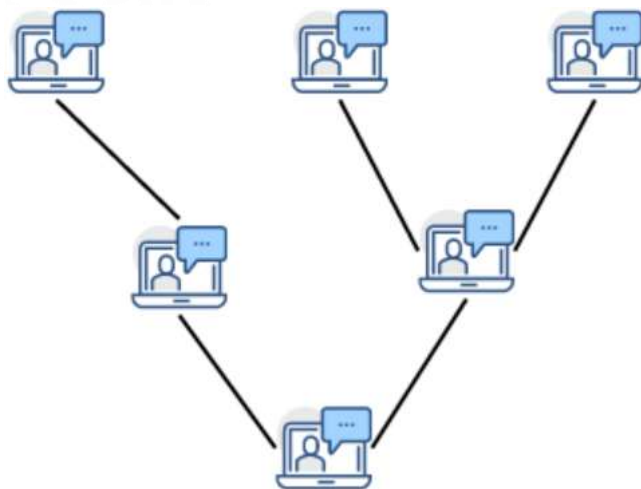
- 总结反思
 - 内容无关配图过多
 - 字体格式未统一
- 相关内容
 - 暂无

- 预期收获
- 题目内涵解析
- 研究背景与意义
- 研究历史与现状
- 知识基础
- 算法原理
 - AntiTomo
 - EigenObfu
- 特点总结与工作展望
- 参考文献

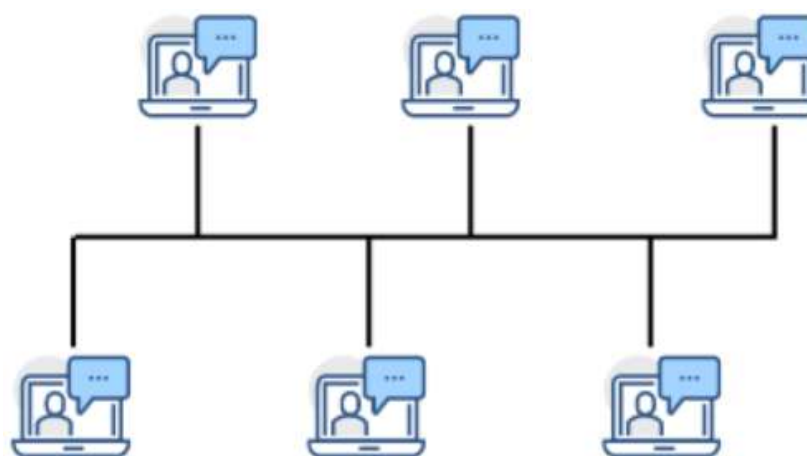


- 预期收获
 - 1.了解网络拓扑混淆技术的基本概念和研究方向
 - 2.理解网络拓扑混淆技术的核心目标
 - 3.掌握混淆网络拓扑生成方法与策略

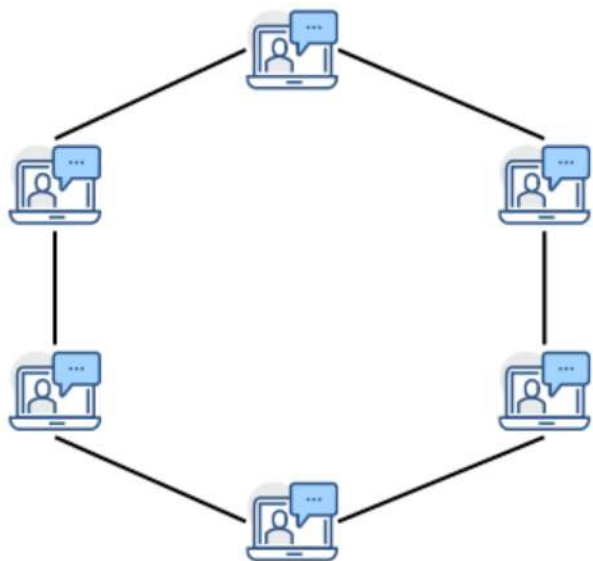
网络拓扑类别



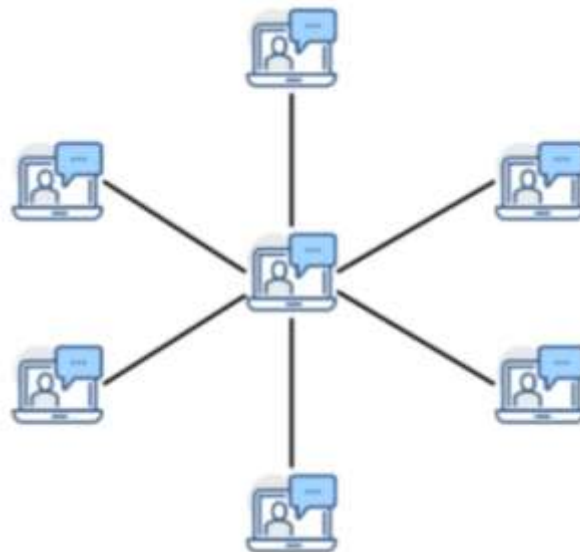
树型网络拓扑



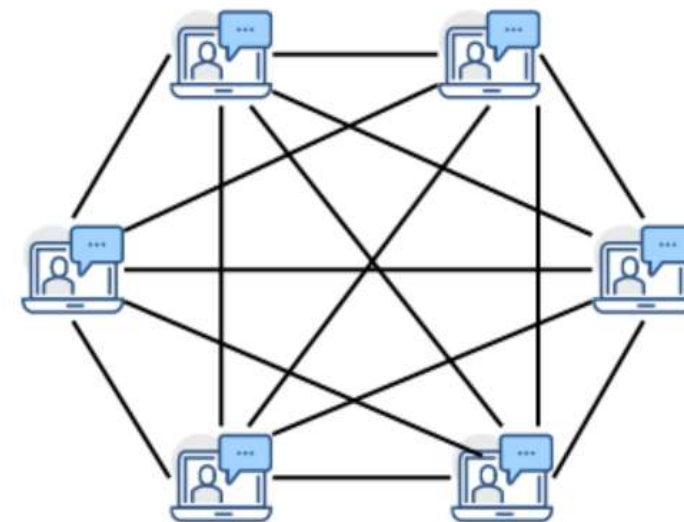
总线型网络拓扑



环型网络拓扑



星型网络拓扑



网型网络拓扑

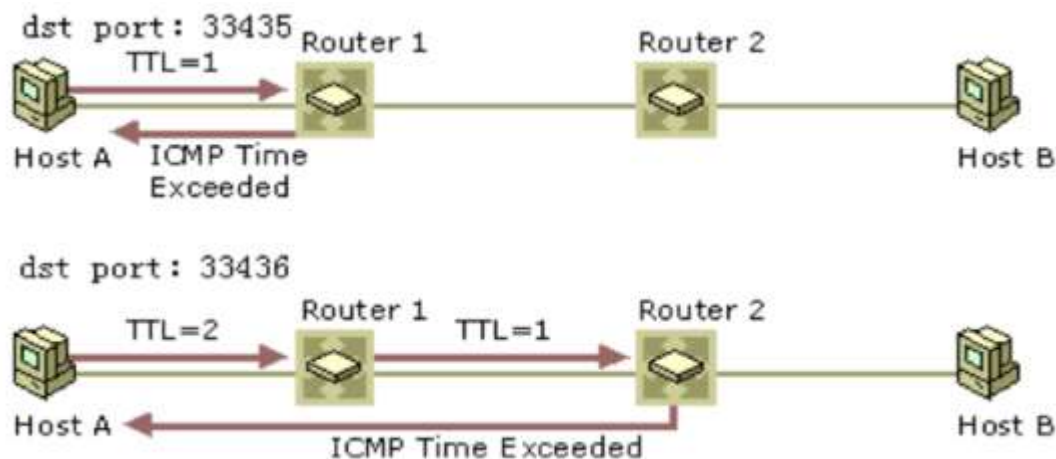
- 研究背景

- 网络拓扑具有脆弱性，攻击者若瘫痪某些关键节点或链路，将导致网络通信受到极大干扰
- 攻击者的网络侦察与精准攻击
 - 攻击者通常通过各种手段来推测**目标网络的结构**,包括节点、链路及它们之间的连接关系
 - 现有的网络安全防御方法往往侧重**防守反击**策略,如检测到攻击时进行流量重定向、负载均衡等

- 研究意义

- 通过**主动隐藏**网络的真实结构，**增加**攻击者获取有效信息的难度

- 网络拓扑推理：通过分析网络节点之间的连接关系和数据交互信息，推断出网络拓扑结构的过程
 - Traceroute
 - 指用于确定数据包从源主机到目标主机所经过的网络路径的网络诊断工具
 - 网络层析成像
 - 通过端到端的测量技术获得端到端性能参数
 - 根据端到端的性能参数计算出节点间的相关性
 - 根据节点间的相关性重构节点的连接情况从而推断网络的拓扑结构



- 研究目标
 - 生成**虚假**且具有**欺骗性**的拓扑视图来干扰攻击者对目标网络感知的**防御方法**
- 内涵解析
 - 结构隐蔽
 - 生成与真实拓扑在**功能等价性**约束下的混淆拓扑，消除可辨识的节点连接模式特征
 - 关键要素保护
 - 建立针对**核心节点**和**骨干链路**的混淆策略，隐藏核心设备（如防火墙、数据库服务器）的位置和连接关系
 - 推理抗性证明
 - 确保混淆机制满足信息论层面的**不可逆性**，即攻击者无法通过多项式时间算法从观测数据中**还原**真实拓扑

Hou等人提出了ProTO系统。
ProTO通过检测探测行为并**延迟探测包**，使攻击者只能推断出一个与真实拓扑无关的虚假网络拓扑，从而有效防止网络拓扑信息泄露

Liu等人提出了NetObfu系统
NetObfu通过构建一个安全的虚拟拓扑，将真实的**网络瓶颈链路隐藏**，并引入**蜜罐链路**来吸引攻击者的注意力，从而有效防止网络拓扑信息泄露

Liu等人提出了AntiTomo机制，设计了一个基于多目标优化模型的方法，通过调整相关延迟生成具有高欺骗性、高安全性、**低延迟增长**和**高效率**的混淆网络拓扑，有效保护网络关键信息不被恶意利用

2020

2021

2022

2018

2021

2022

2024

Zhang设计的MASK-NET方案先对网络的静态度量（如节点度、介数）与实时队列长度进行联合建模，快速检测瓶颈资源

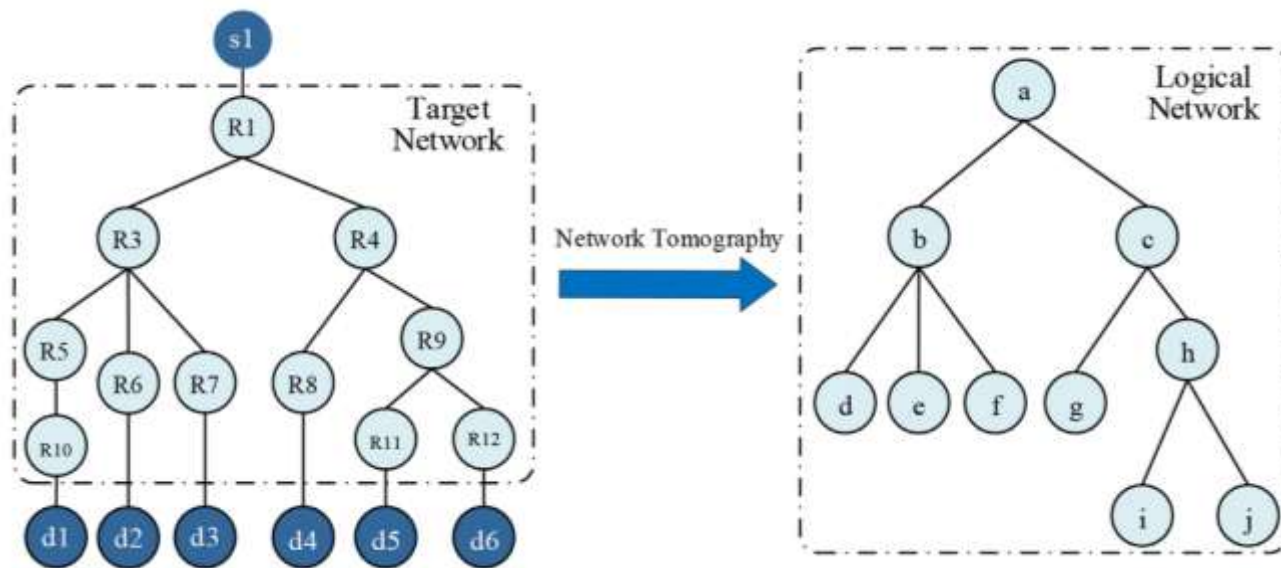
Kim等人提出了BOTTLENET系统。通过分析网络的静态和动态指标，识别**网络瓶颈节点和链路**，并利用SDN技术生成复杂的虚拟拓扑，使攻击者无法轻易推断出真实的网络结构

Kim等人提出了EqualNet机制，设计了一种基于长期网络拓扑混淆的主动防御方法，通过**均衡追踪流量**在网络节点和链路上的分布，从而有效保护网络中的**关键节点和链路**免受链路洪水攻击（LFAs）的恶意利用

Zhu等人提出了EigenObfu机制，设计了一种基于**特征向量中心性**的网络拓扑混淆方法，通过**识别和隐藏关键节点**并生成具有高相似度、低部署成本的混淆网络拓扑，有效迷惑攻击者，使其无法准确推断出网络结构

- 网络拓扑混淆方法

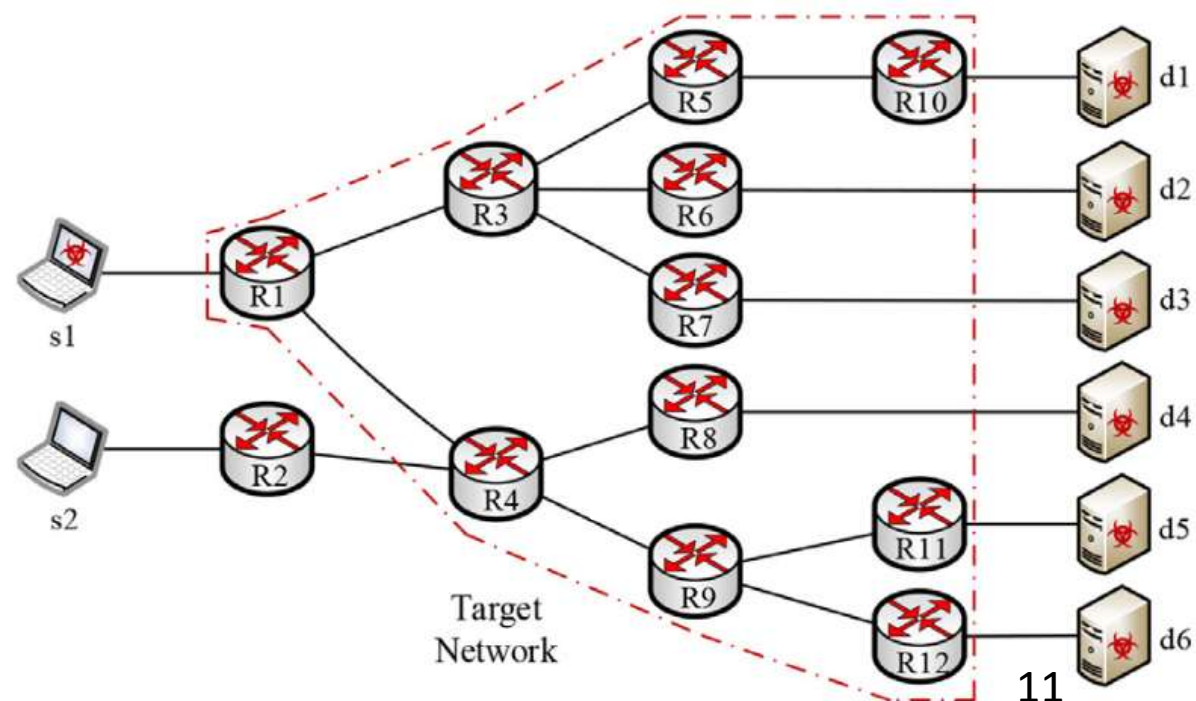
- 针对网络层析成像攻击的**防御措施尚不完善**：尽管防御Traceroute攻击的技术已经相对成熟，但针对网络层析成像攻击的防御方法仍然相对匮乏
- 忽略关键节点：忽略了对关键节点的直接**识别与保护**，而是侧重于生成具有欺骗性的网络拓扑视图
- 相似性不足：未能充分确保其与原始拓扑的相似性，这可能导致混淆后的网络结构与真实网络结构**存在较大差异**



• 相关延迟

- 相关延迟 $y_{i,j}$ 定义为从源节点到目标节点i和目标节点j的路径中共享链路
- 计算步骤
 - 测量端到端的路径延迟Y
 - 构建路由矩阵R
 - 计算相关延迟 $Y=Rx$

	(R1, R3)	(R1, R4)	(R4, R9)	...
(d1, d2)	1	0	0	...
(d1, d3)	1	0	0	...
...	...	...	...	...
(d5, d6)	0	1	1	...



- 拉普拉斯谱相似度

- 假设原始拓扑的拉普拉斯矩阵为 L_1 ，混淆拓扑的拉普拉斯矩阵为 L_2

- 原始拓扑特征值 $\lambda_1 \leq \lambda_2 \leq \lambda_3 \cdots \leq \lambda_n$

- 混淆拓扑特征值 $\lambda_1^* \leq \lambda_2^* \leq \lambda_3^* \cdots \leq \lambda_n^*$

- 谱距离

- 计算两图特征值之间的欧氏距离: $d_L(L_1, L_2) = \sqrt{\sum_{i=1}^n (\lambda_i - \lambda_i^*)^2}$

- 计算相似度

- 将谱距离转换为相似度函数: $S_L(L_1, L_2) = \frac{1}{1+d_L(L_1, L_2)}$

- 该函数的取值范围为 $[0,1]$ ，谱距离越小，相似度越高

- 树编辑距离

- 树编辑距离是衡量两棵树结构相似度的一种度量方法，具体指通过一系列编辑操作（插入、删除或替换节点）将一棵树转换为另一棵树所需的最小操作成本

- 基本操作

- 插入:在树中插入一个新节点
 - 删除:在树中删除一个节点
 - 连接:将一个节点与另外一个节点相连

- 公式

- $$\text{simi} = \frac{\text{TED}(L, L^*)}{\text{TED}(L, Z) + \text{TED}(L^*, Z)}$$
 - 该公式的取值范围为[0,1]，simi越小，相似度越高



- 图中心性

- 度中心性

- 在无向网络中，可以使用一个节点的度数来衡量这个节点的重要性
 - $C_D(v) = \frac{\text{degree}(v)}{n-1}$ ，其中 $C_D(v)$ 是节点 v 的度中心性， $\text{degree}(v)$ 是节点度数， n 是网络中节点的总数
 - 仅考虑直接连接，忽略节点的全局位置或间接影响

- 特征向量中心性

- 不仅关注自身节点的度数，还考虑与其相连节点的质量
 - $\lambda x = Ax$ ，其中 λ 是最大特征值， x 是对应的特征向量



AntiTomo: Network topology obfuscation against adversarial tomography-based topology inference



T	目标	生成具有 欺骗性、安全性、低延迟、高效率 的混淆网络拓扑
I	输入	Topology Zoo中 三个不同规模的网络 : N1(14 个节点, 13 条链路, 9 个终端节点)、N2(39 个节点, 38 条链路, 23 个终端节点)、N3(101 个节点, 100 条链路, 51 个终端节点)
P	处理	1.通过随机生成多个候选树来形成候选森林 2.遍历候选森林中的每个侯选树, 计算 其相关延迟和相似度 , 并选择最优候选树作为混淆拓扑
O	输出	混淆网络拓扑

P	问题	如何防御基于网络层析成像的拓扑推断攻击, 保护网络的信息
C	条件	攻击者不与内部节点协作, 仅通过外部测量推断网络拓扑
D	难点	防止攻击者通过混淆拓扑推断出真实网络拓扑
L	水平	2022 SCI 1区

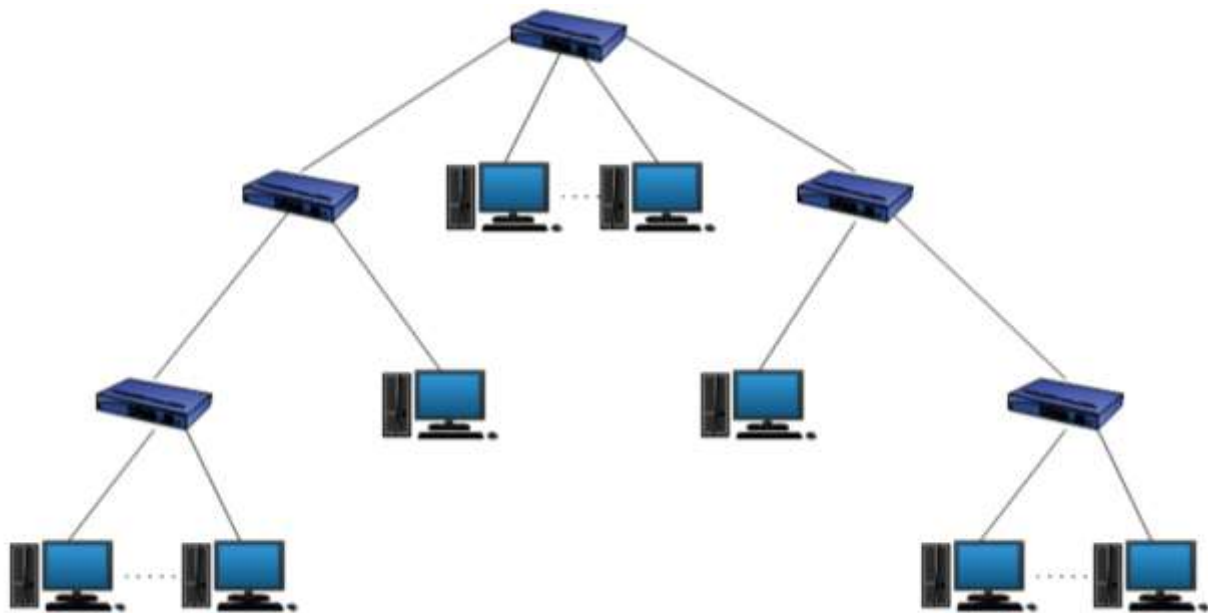
- 网络模型

- 网络节点

- 边缘节点是指可以**直接与外部用户连接**的节点
 - 内部节点是指**连接在网络内部的节点**，用户无法进行直接访问

- 网络采用的是**最短路径优先路由协议**，也就是说在网络中，任意两个节点都有一个固定的最短路径

- 内部节点**不会响应**追踪路由的探测包，即攻击者无法通过Traceroute工具直接获取网络拓扑结构





- 创新说明

- 欺骗性

- 确保伪装拓扑的**节点数和链路数**与真实拓扑接近 $|N^* - N| < K, |L^* - L| < Q$

- 安全性

- 通过比较攻击者推断的**混淆网络布局与真实网络布局之间的相似性**来衡量安全性

- 低延迟

- 伪造的混淆网络拓扑需要**尽可能少的增加网络延迟**，以免影响正常用户的体验

- 高效性

- 快速生成伪装拓扑，因为攻击者可能持续探测，需要定期更新混淆网络拓扑以保持防御效果



- 候选森林算法

- 随机生成多个**候选树**，构成**候选森林**。每棵候选树代表一个潜在的混淆拓扑
- 基本流程
 - 首先创建一个空的候选森林，用于存放生成的候选树
 - 随机生成候选树的节点数 $|N^*|$ 应该满足 $|N^*| \in [|N| - \varphi_n, |N| + \varphi_n]$
 - 从节点子集中随机挑选两个未连接的节点，添加一条链接
 - 重复第三步步骤，直到链路数达到 $N-1$ ，形成一棵树
- 优势
 - 随机生成的候选树满足**节点数**和**链接数**分布的约束条件（欺骗性）
 - 随机性确保候选拓扑与真实拓扑无明确映射关系（安全性）



- 混淆拓扑选择方法

- 遍历候选森林里面所有的候选树，并且计算每个候选树和真实树的**相关延迟总和**

$$Y = y_{1,2} + \cdots + y_{1,D} + y_{2,3} + \cdots + y_{2,D} + y_{D-1,D}$$

- 计算每个候选树的**相关延迟增长率** $cost(L, L^*) = \frac{Y_{L^*} - Y_L}{Y_L}$ ，以衡量延迟增长
- 遍历候选集合里面所有的候选树，并且使用编辑树距离来衡量**候选树和真实树相似度** $simi(L, L^*)$
- 使用目标函数 $T = \lambda_{simi} simi(L, L^*) + \lambda_{cost} cost(L, L^*)$ 来决策每个候选树的好坏，选择目标函数最小的网络拓扑作为真实网络拓扑的混淆网络拓扑



• 数据资源

网络拓扑	节点	链路数	终端数	来源
N1	14	13	9	Claranet
N2	39	38	23	Iris
N3	101	100	51	Colt

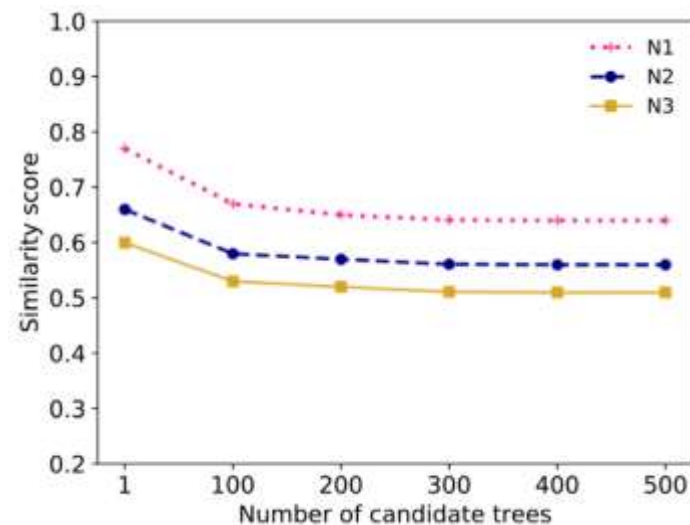
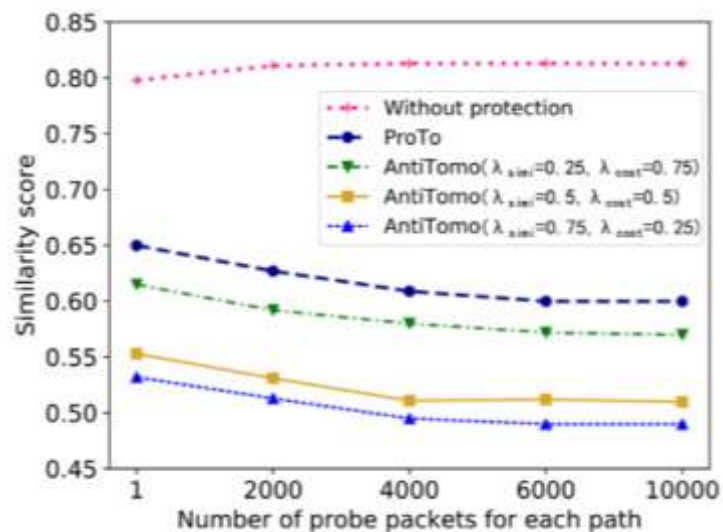
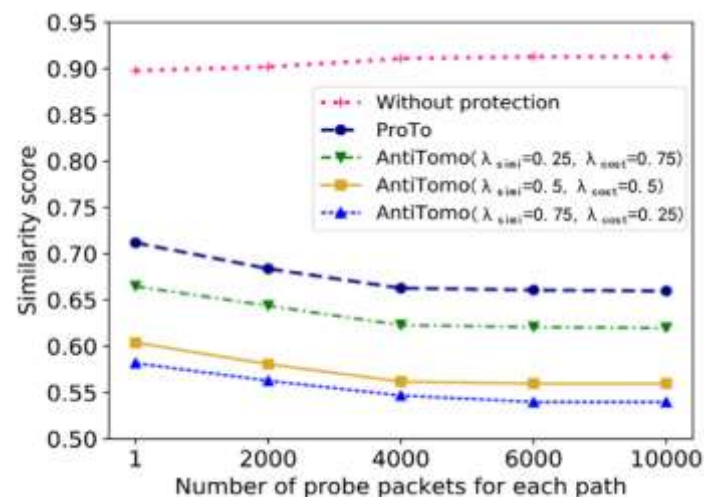
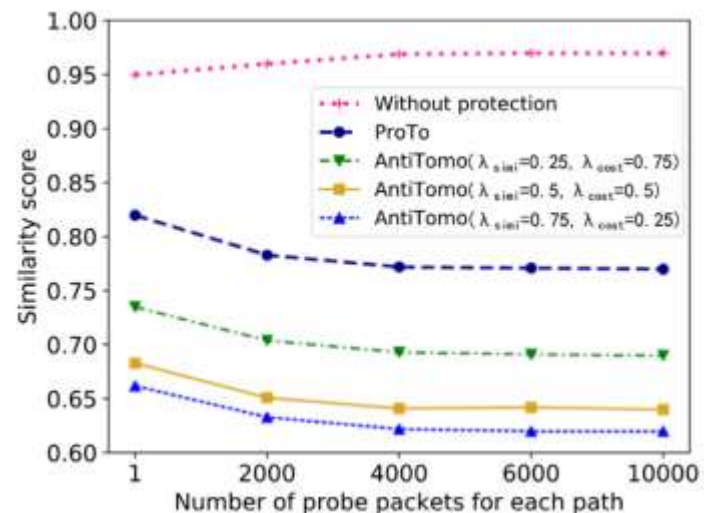
• 对比方法

- 无保护：代表目标网络**没有使用**任何网络拓扑混淆机制。即攻击者在**没有任何防护**的情况下进行基于网络层析的拓扑推断
- ProTo：通过随机生成网络拓扑矩阵并据此生成虚假的拓扑来进行网络拓扑混淆

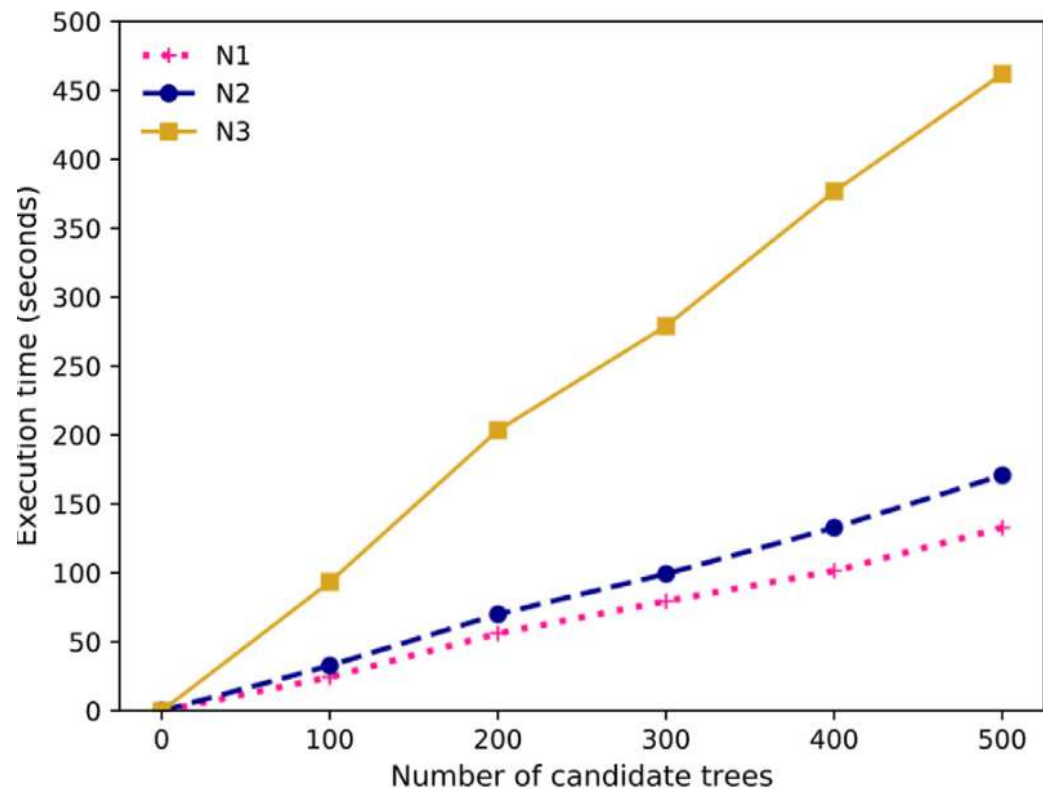
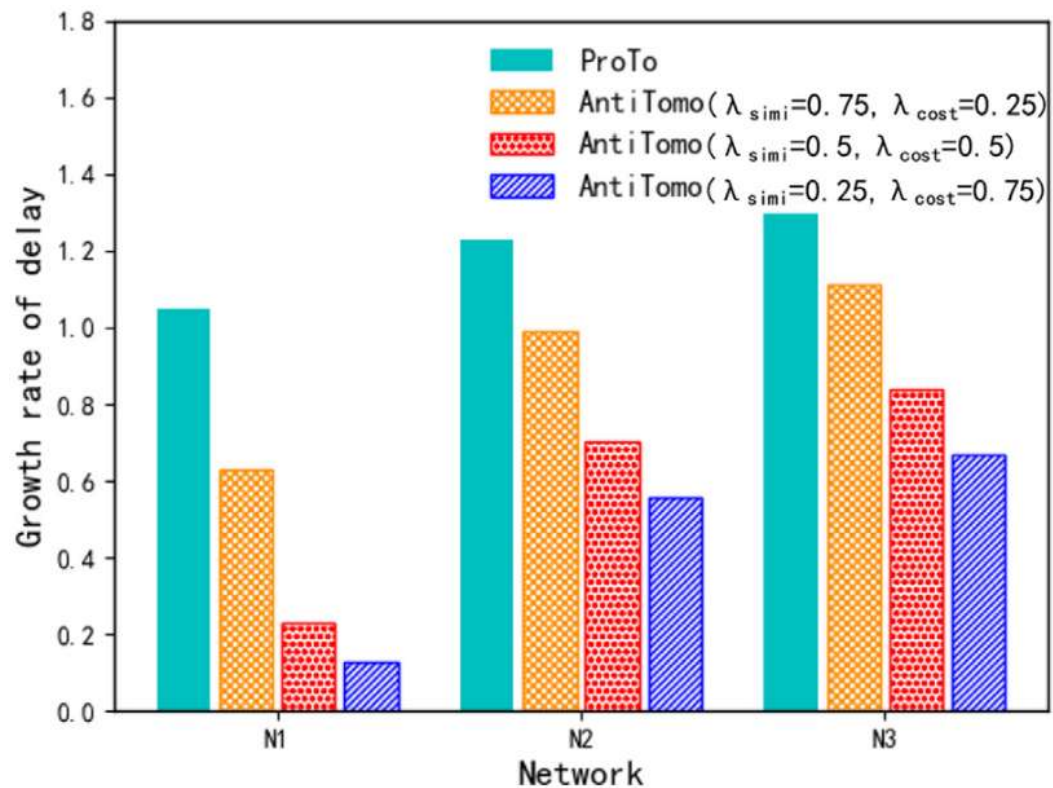
• 重复实验

- 每个实验重复100次，取其平均值以减少随机性影响

实验结果



实验结果



- 当 λ_{cost} 值增大时，延迟的增长速率会下降
- 随着候选树数量的增长，执行的时间也会增长



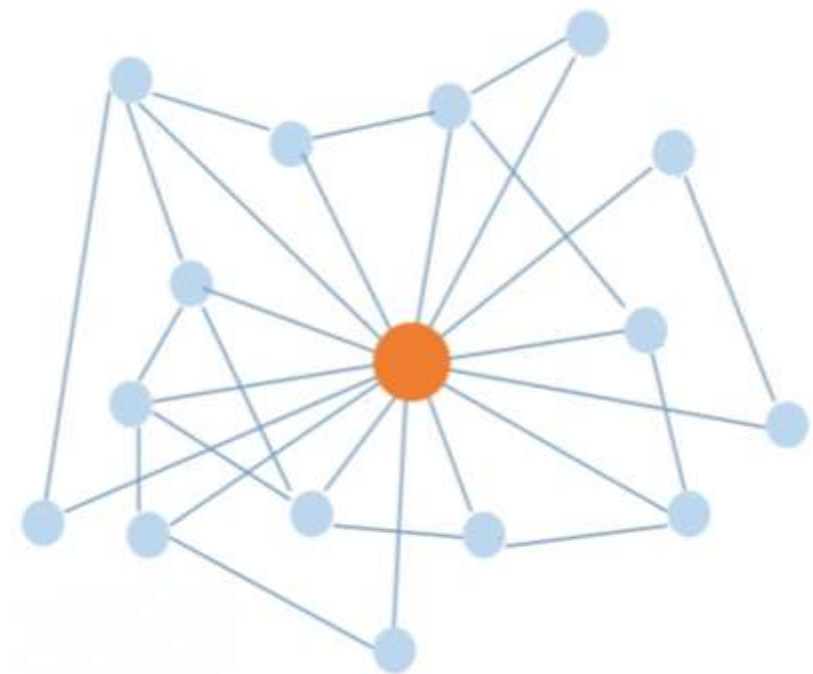
EigenObfu: A Novel Network Topology Obfuscation Defense Method



T	目标	对网络拓扑结构中的重要节点进行保护
I	输入	从Internet Topology Zoo和TopoHub获取的九种不同的网络拓扑结构，这些网络拓扑结构分为小、中、大三种规模，每种规模有三种不同的网络拓扑结构
P	处理	1. 将网络拓扑结构表示为邻接矩阵，选择网络中的重要节点进行保护 2. 修改邻接矩阵中网络节点的连接方式，生成混淆网络拓扑集合 3. 从网络拓扑集合中选择与原始拓扑谱相似性最高的网络拓扑
O	输出	混淆网络拓扑

P	问题	仅仅使用度中心性的衡量方式只看直接邻居数量，忽视了网络网络拓扑的全局结构信息
C	条件	网络拓扑结构数据
D	难点	既要用全局视角找到真正高价值节点，又要在巨大的组合空间里快速挑出既安全、连通又高度相似的假拓扑
L	水平	2024 SCI 1区

- EigenObfu
 - 引入特征向量中心性
 - 特征向量中心性不仅考虑节点的直接连接数，还考虑节点与其他重要性节点的连接情况，提供了一种更加全局和精确的节点重要性度量方式
 - 优化问题建模
 - 混淆拓扑必须连通，即其拉普拉斯矩阵的第二小特征值需满足 $\lambda_2 > 0$
 - 安全约束：混淆拓扑的关键节点集 K 必须与原始拓扑的关键节点集 K^* 无交集
 - 高效的部分搜索策略
 - 在保证结果质量的前提下，显著降低计算复杂度，适用于大规模网络





• 算法流程

– 候选拓扑生成

- 确定关键节点，使用**特征向量中心性**，计算节点的重要性，选取排名最高的前 r 个节点组成关键节点集 K
- 对网络拓扑的邻接矩阵进行修改，若涉及的两个节点均为非关键节点，则以 $1-p$ 的概率使其连通，以 p 的概率使其断开；而若涉及的两个节点中存在至少一个关键节点，则以相反的概率处理

– 候选拓扑选择

- 计算候选拓扑的拉普拉斯矩阵特征值，**保留满足连通性和安全约束的候选拓扑**
- 从有效候选集中选择与原始拓扑**最相似**的混淆拓扑

- 候选拓扑生成

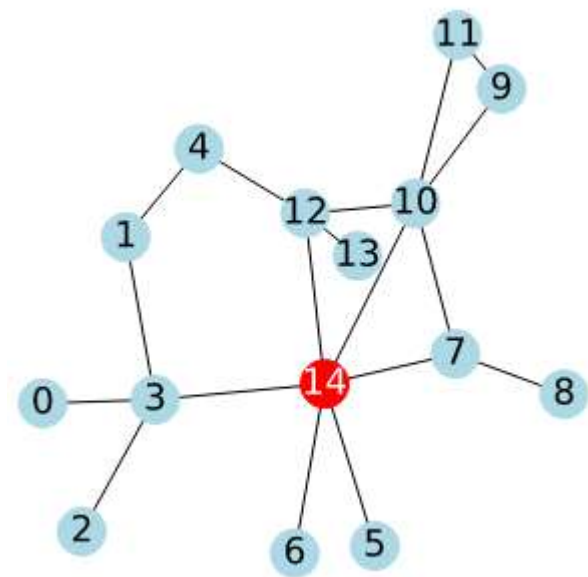
- 确定关键节点

- 对原始拓扑结构的邻接矩阵进行特征值分解，得到主特征值 $e_{\max}$ ，其元素表示节点的特征向量重要性

- 选择中心性最高的前 r 个节点组成关键节点集合 K

- 邻接矩阵修改规则

- 关键节点行(对应 K 中的节点)
 - 若元素为0，以概率 p 改为1(增加虚假连接)
 - 若元素为1，以概率 $1-p$ 改为0(移除真实连接)
 - 非关键节点行(其他节点)
 - 若元素为0，以概率 $1-p$ 改为1(增加虚假连接)
 - 若元素为1，以概率 p 改为0(移除真实连接)



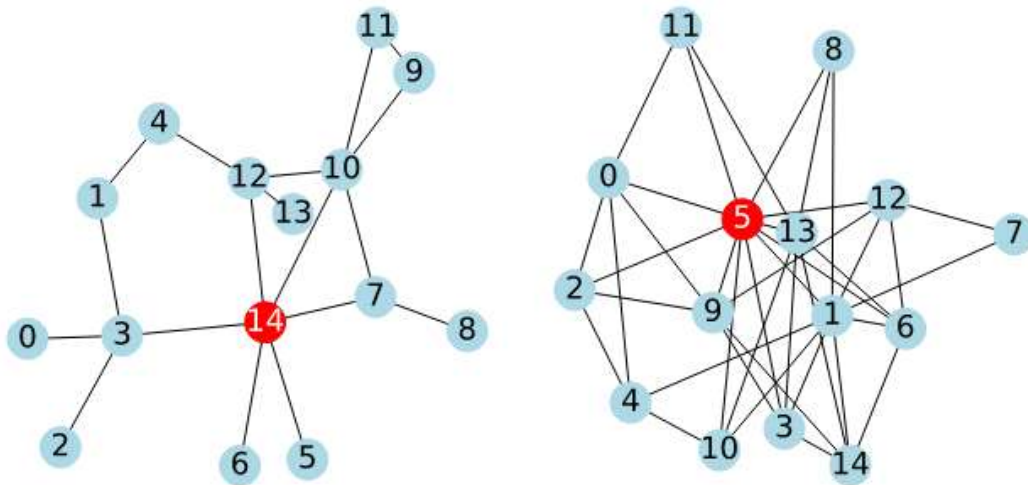
- 候选拓扑选择

- 生成混淆拓扑选择集合 θ

- 根据候选拓扑生成算法，生成M个满足安全约束和连通性约束的混淆网络拓扑，形成网络拓扑集合 θ

- 选择最优混淆网络拓扑

- 通过贪心算法遍历整个网络拓扑集合 θ ，计算其与原始网络拓扑的拉普拉斯谱相似性，选择拉普拉斯谱相似性最高的拓扑作为最终结果

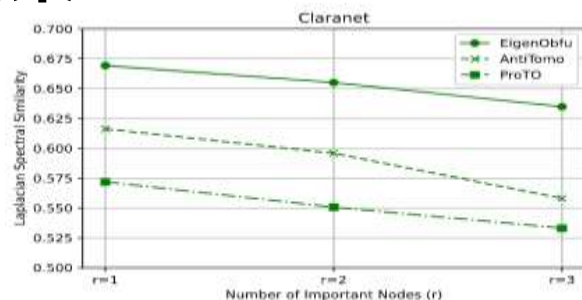




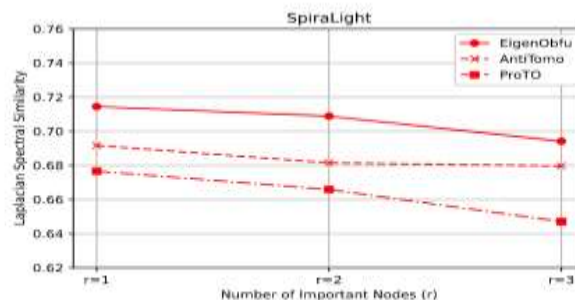
• 数据资源

网络拓扑	节点	链路数	关键节点	百分比
Claranet	15	18	1/2/3	6.67%/13.33%/20.00%
SpiraLight	15	16	1/2/3	6.67%/13.33%/20.00%
HiberniaUK	15	15	1/2/3	6.67%/13.33%/20.00%
gabriel/50/0	50	99	1/2/3/4/5/8/10	2%/4%/6%/8%/10%/16%/20%
gabriel/50/5	50	93	1/2/3/4/5/6/7/8/9	2%/4%/6%/8%/10%/16%/20%
gabriel/50/3	50	90	1/2/3/4/5/6/7/8/9	2%/4%/6%/8%/10%/16%/20%
gabriel/150/7	150	297	3/6/9/12/15/18	2%/4%/6%/8%/10%/12%
gabriel/150/8	150	291	3/6/9/12/15/18	2%/4%/6%/8%/10%/12%
gabriel/150/9	150	288	3/6/9/12/15/18	2%/4%/6%/8%/10%/12%

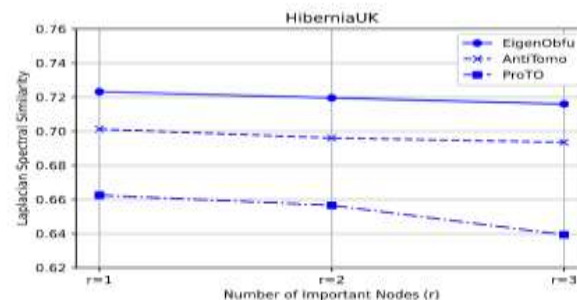
实验结果



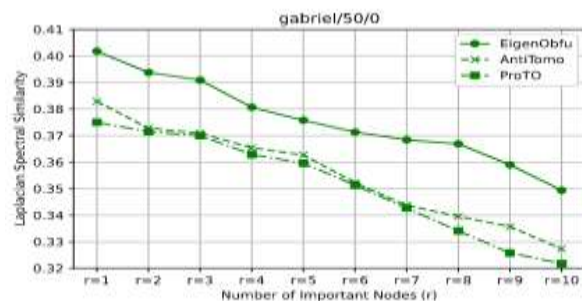
(a)



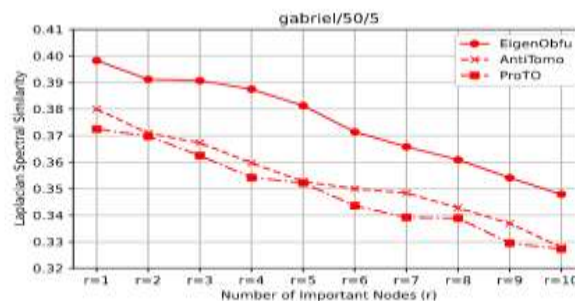
(b)



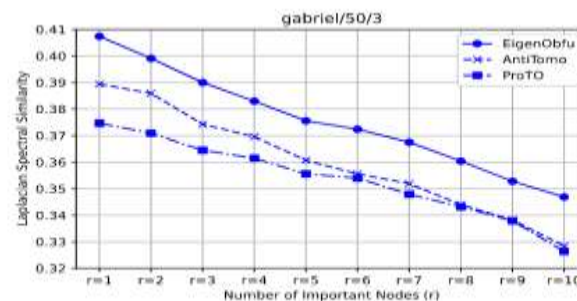
(c)



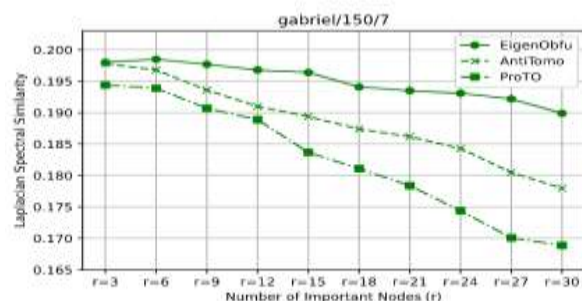
(d)



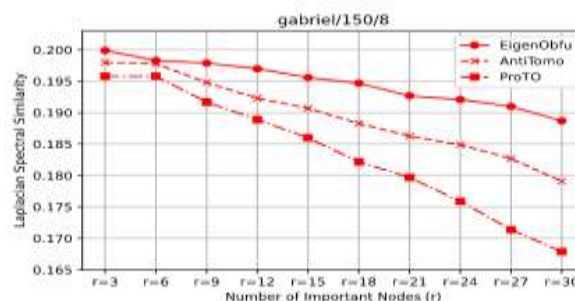
(e)



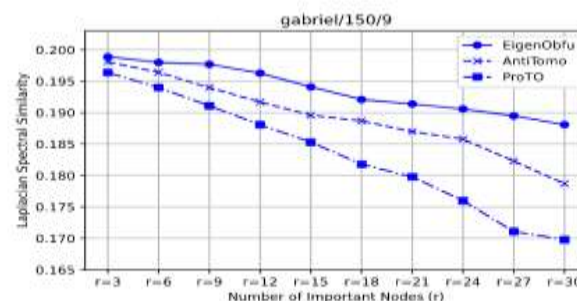
(f)



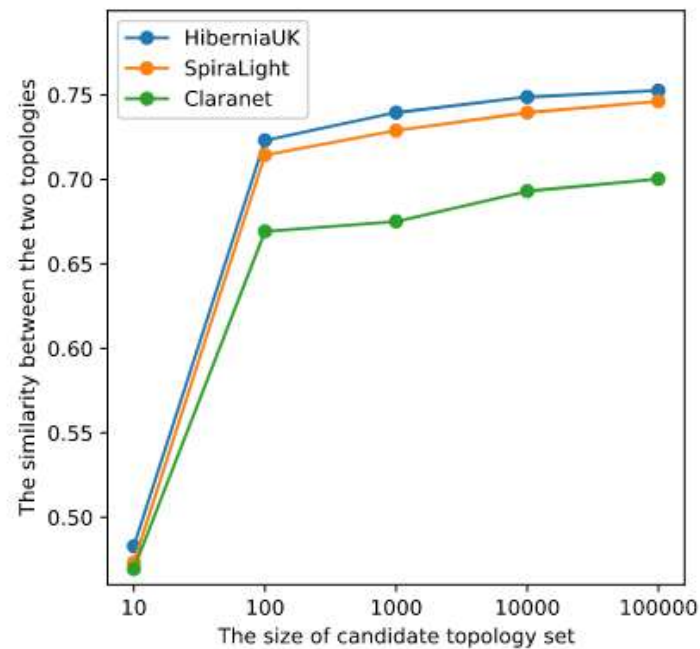
(g)



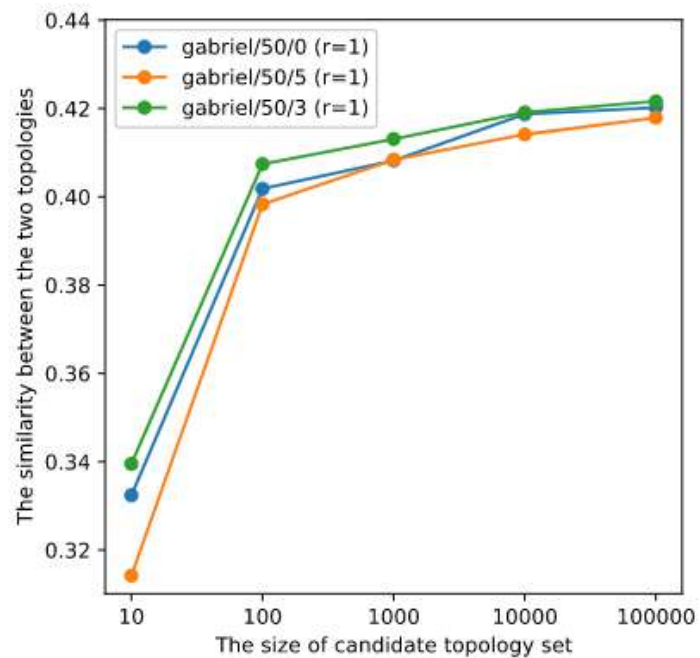
(h)



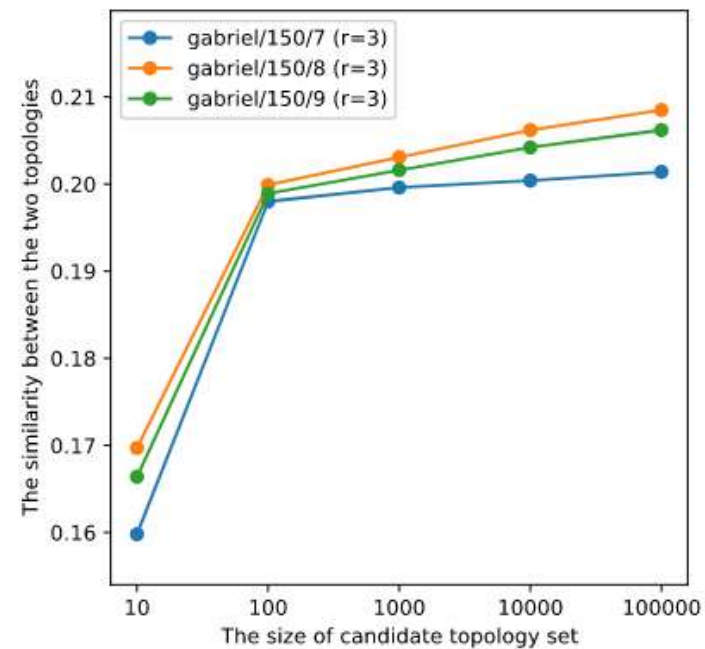
(i)



(a)



(b)



(c)

- 当候选集合从100开始时，相似度变化较小



特点总结与未来展望



- 算法创新
 - 将混淆网络拓扑的生成问题建模为一个多目标优化问题，综合考虑欺骗性、安全性、低成本和高效率等因素
 - 首次将特征向量中心性引入网络拓扑混淆问题，能够更全面地衡量网络中节点的重要性，相比传统的基于度中心性的方法，特征向量中心性可以更好地识别关键节点
- 算法优势
 - 在多个不同规模的网络拓扑上进行了比较实验并且在保持混淆拓扑与原始拓扑相似性方面表现良好，有助于降低部署成本
- 未来工作
 - 设置反制措施，例如利用蜜罐来引诱攻击者进入提前设计好的陷阱
 - 对节点和链路没有同时进行保护

- [1] Liu Y, Xing C, Zhang G, et al. AntiTomo: Network topology obfuscation against adversarial tomography-based topology inference[J]. Computers & Security, 2022**
- [2] Zhu Z, Zhu G, Zhang Y, et al. EigenObfu: A Novel Network Topology Obfuscation Defense Method[J]. IEEE Transactions on Network Science and Engineering, 2024**
- [3] Hou T, Qu Z, Wang T, et al. Proto: Proactive topology obfuscation against adversarial network topology inference[C]//IEEE INFOCOM 2020-IEEE Conference on Computer Communications. IEEE, 2020**

知人者智，自知者明。胜人者有力，自胜者强。知足者富。强行者有志。不失其所者久。死而不亡者，寿。

谢谢！

