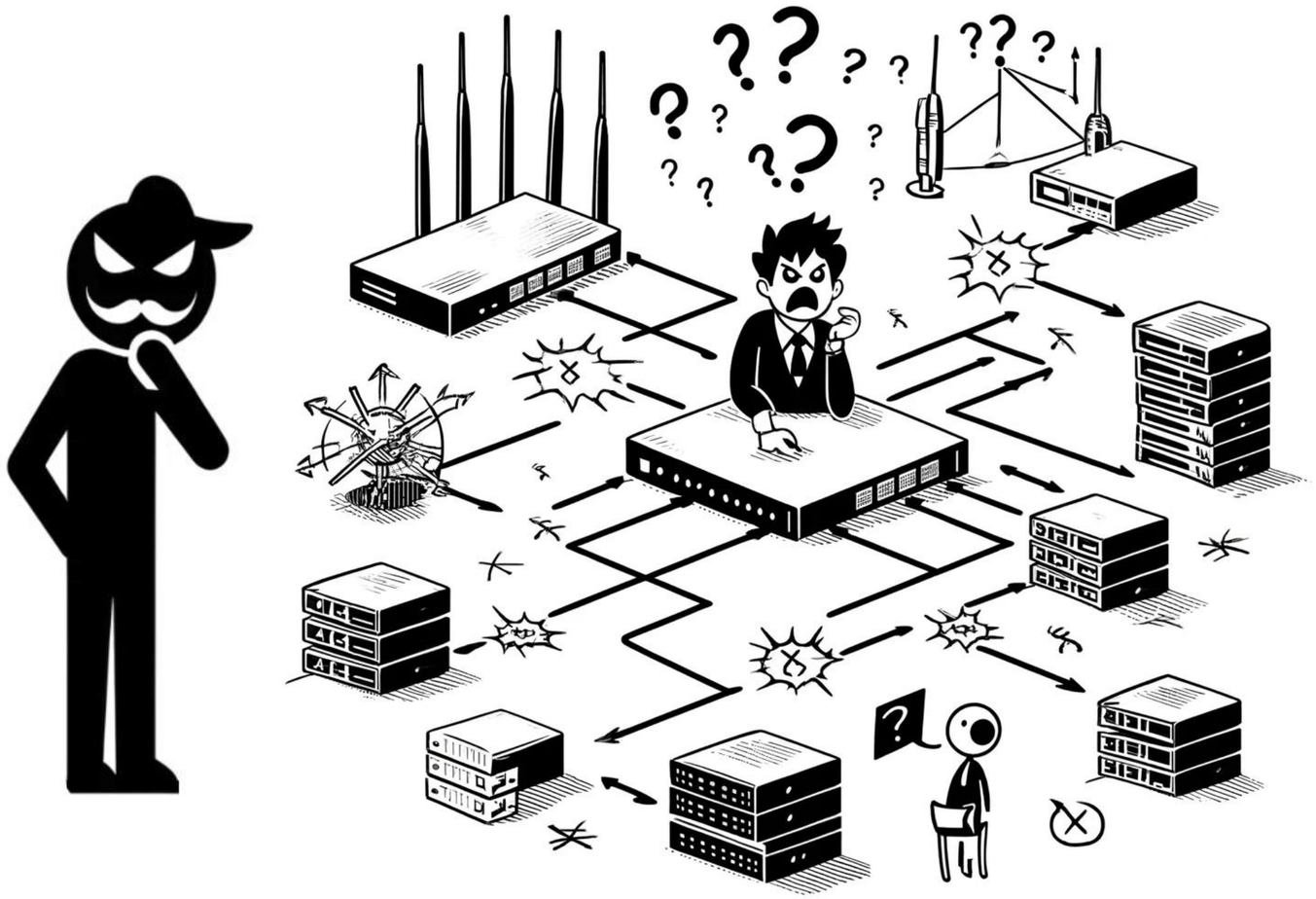
拜占庭攻击下评估网络布尔层析成像性能分析与研究

本人毕设答辩PPT

研究背景



实例1：路由器入侵攻击

场景

一个大型企业的内联网中，攻击者通过漏洞入侵了几台核心路由器。

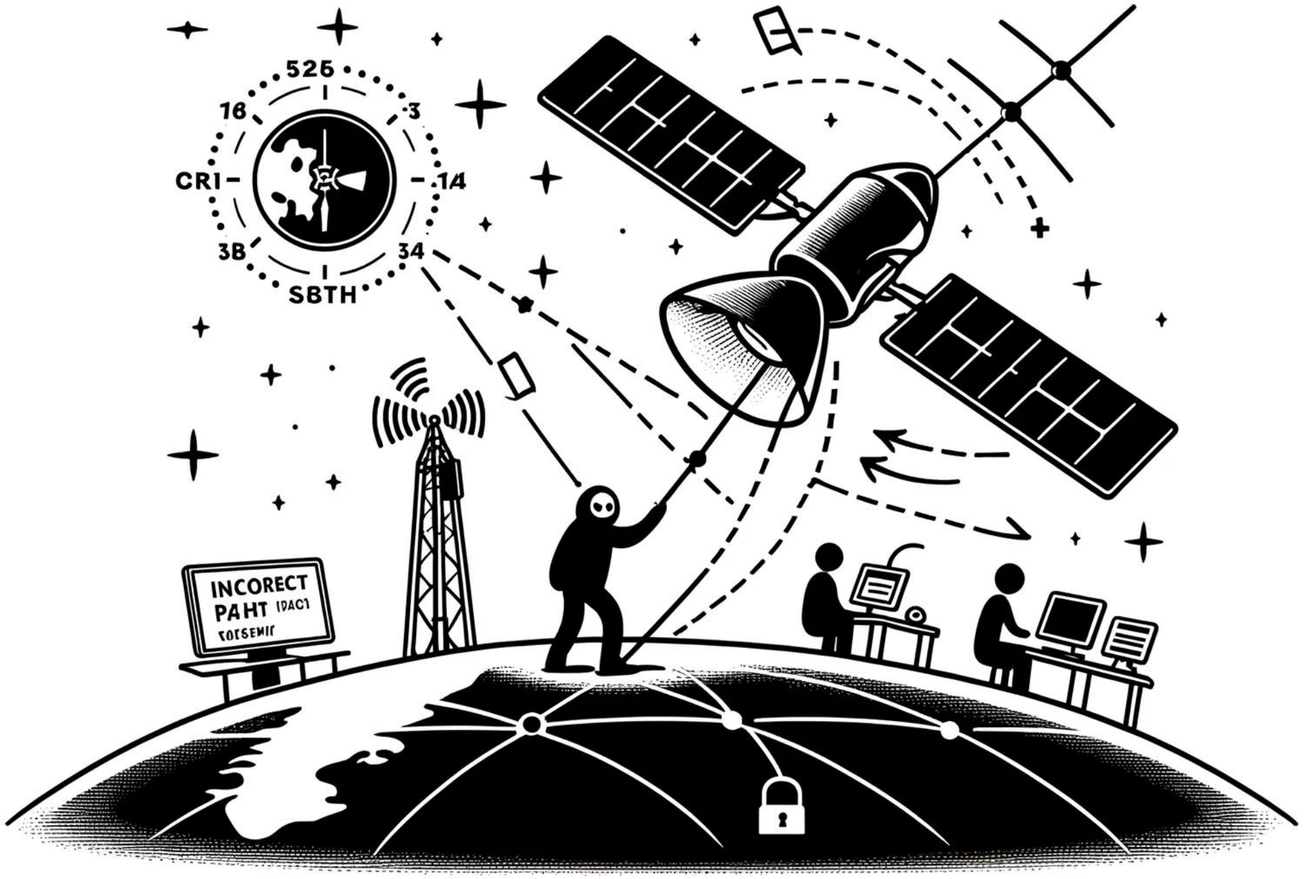
攻击行为

攻击者篡改了这些路由器的路由表和状态报告，使得路由器报告虚假的链路状态信息。

影响

网络布尔层析成像技术无法准确识别真正的拥塞链路，导致网络管理员误判网络健康状态，可能会错误地调整网络流量，进一步加剧实际的网络拥塞。

研究背景



实例2：卫星通信干扰

场景

在一个全球卫星通信网络中，攻击者通过入侵一个关键地面站，篡改从该站发送到卫星的数据。

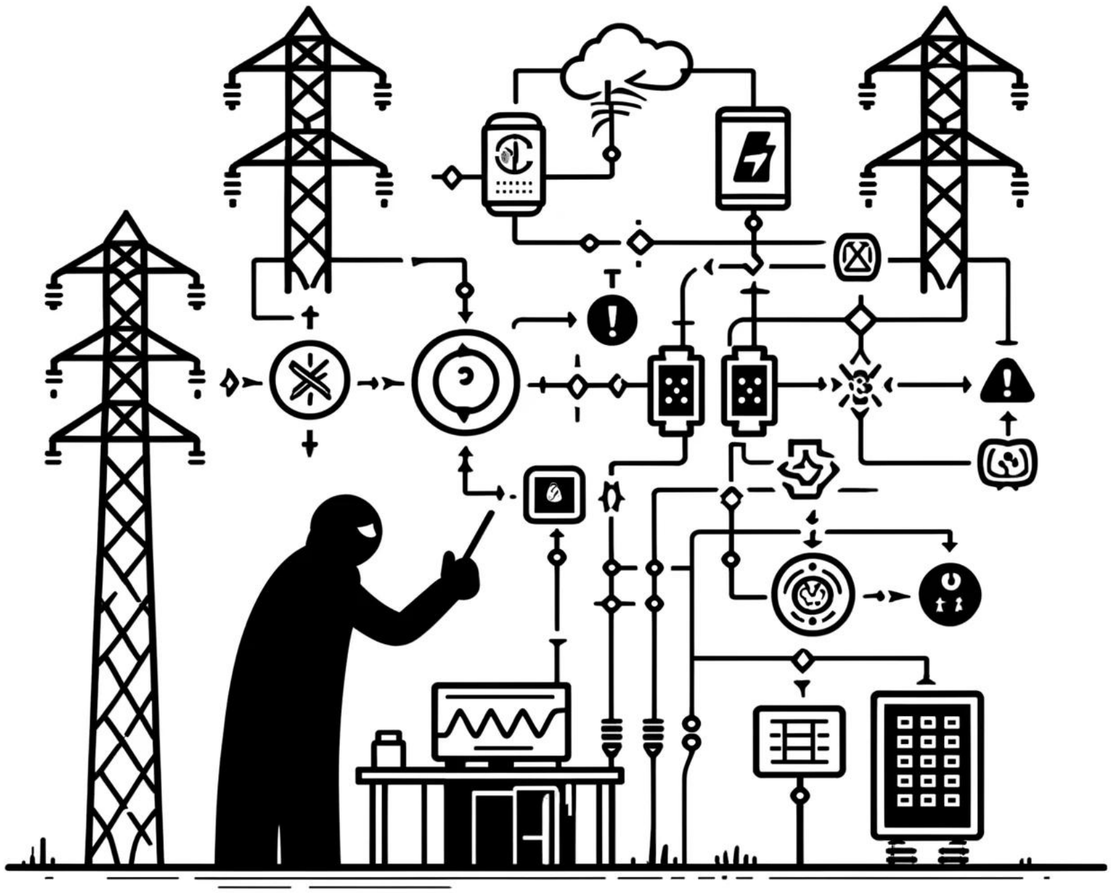
攻击行为

攻击者使得地面站向卫星发送错误的状态报告，导致卫星返回的路径状态信息不准确。

影响

网络布尔层析成像技术无法识别真实的链路状态，可能会在关键数据传输任务中做出错误的路径选择，导致数据丢失或传输延迟，影响关键任务的完成。

研究背景



实例3：智能电网传感器篡改

场景

智能电网中，攻击者通过网络钓鱼攻击获取了多个关键传感器的控制权。

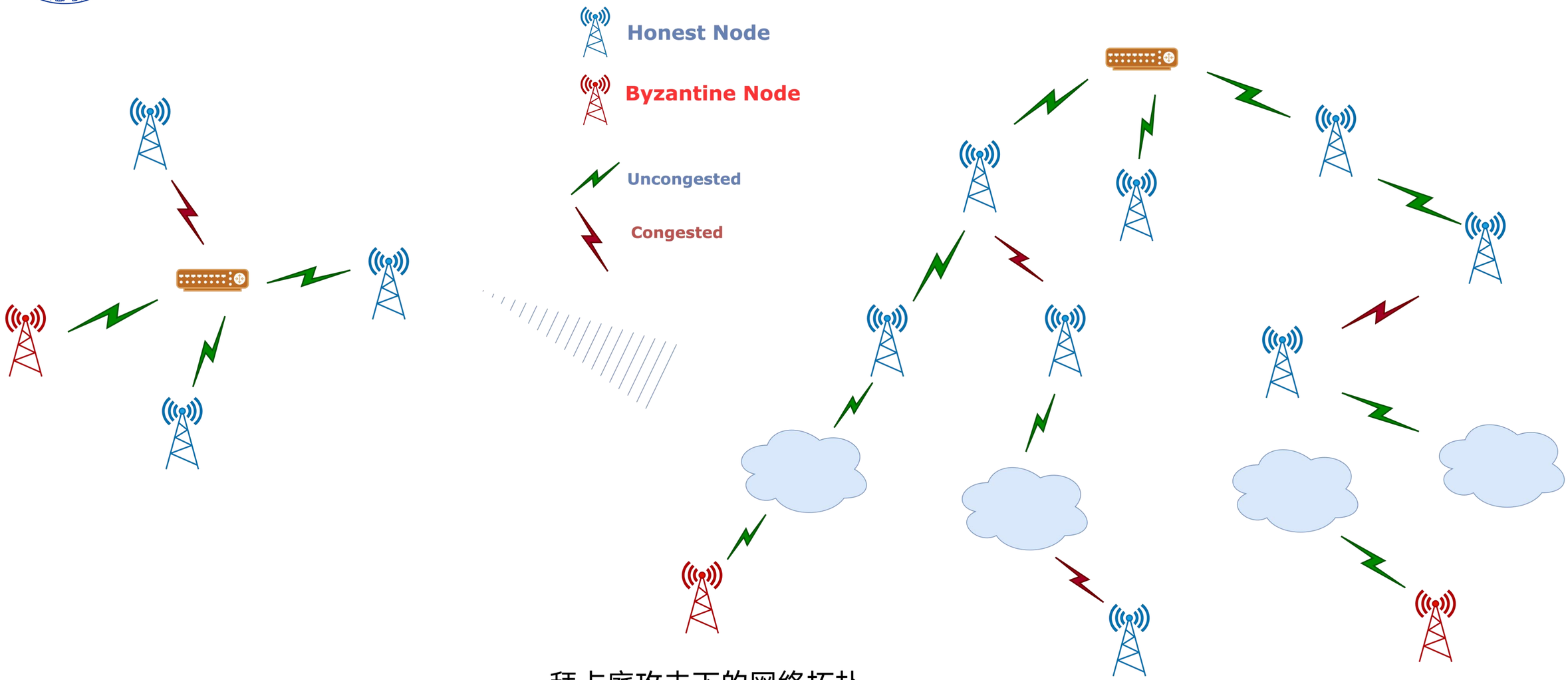
攻击行为

攻击者篡改传感器数据，使得电网管理系统接收到错误的电力传输状态信息。

影响

网络布尔层析成像技术无法准确评估电力传输路径的健康状况，可能导致管理系统做出错误的负载调整决定，引发部分区域的电力短缺或过载，影响电网的稳定性和可靠性。

研究背景



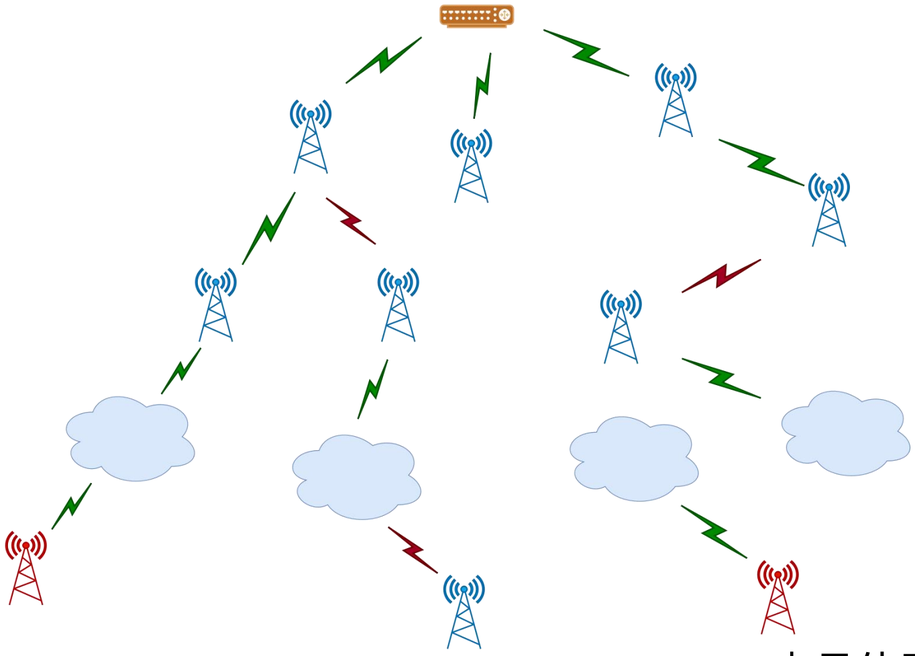
拜占庭攻击下的网络拓扑

目 录

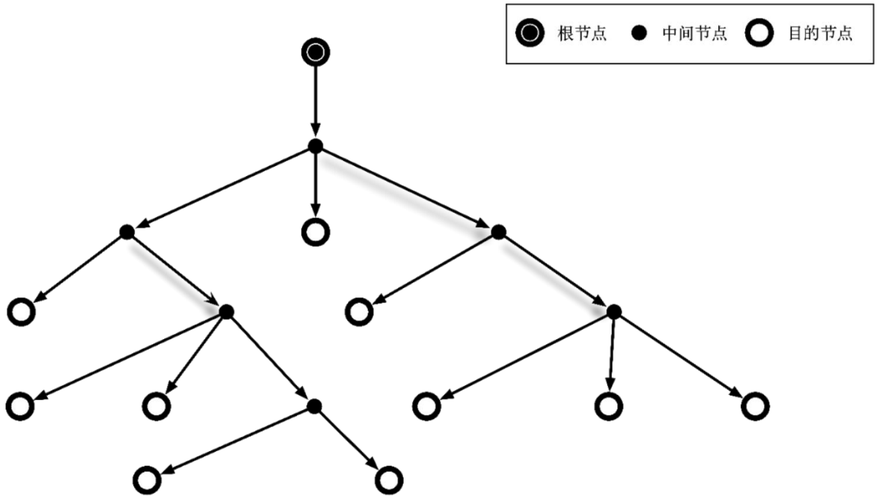
CONTENTS

基础知识

1.1 拓扑的抽取



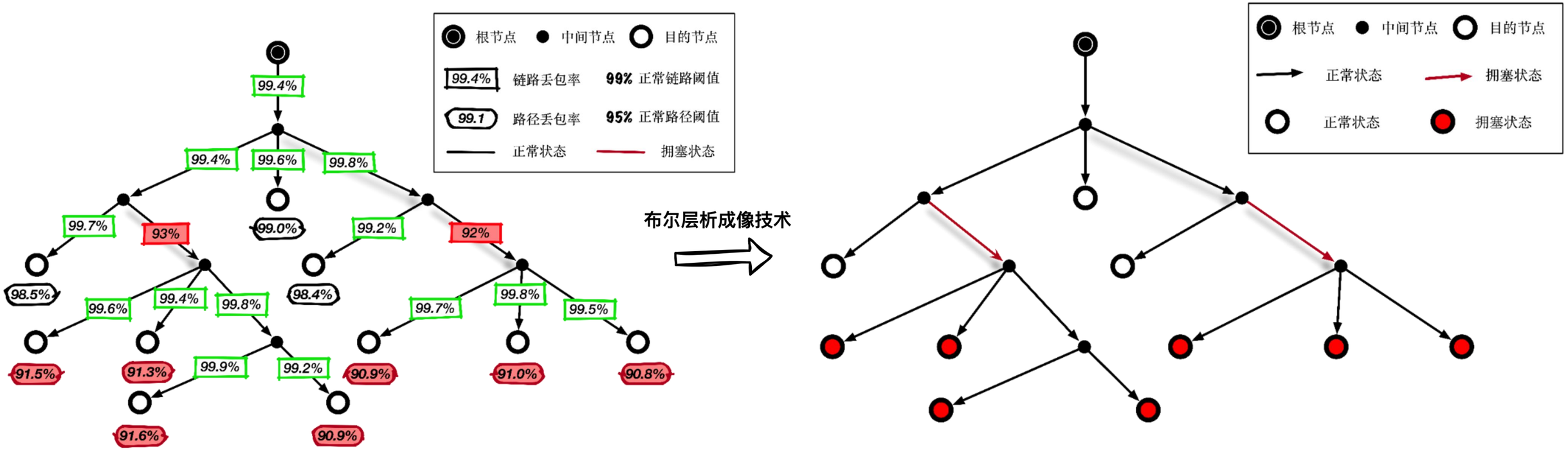
Abstracted to



由具体网络转换为**抽象**拓扑

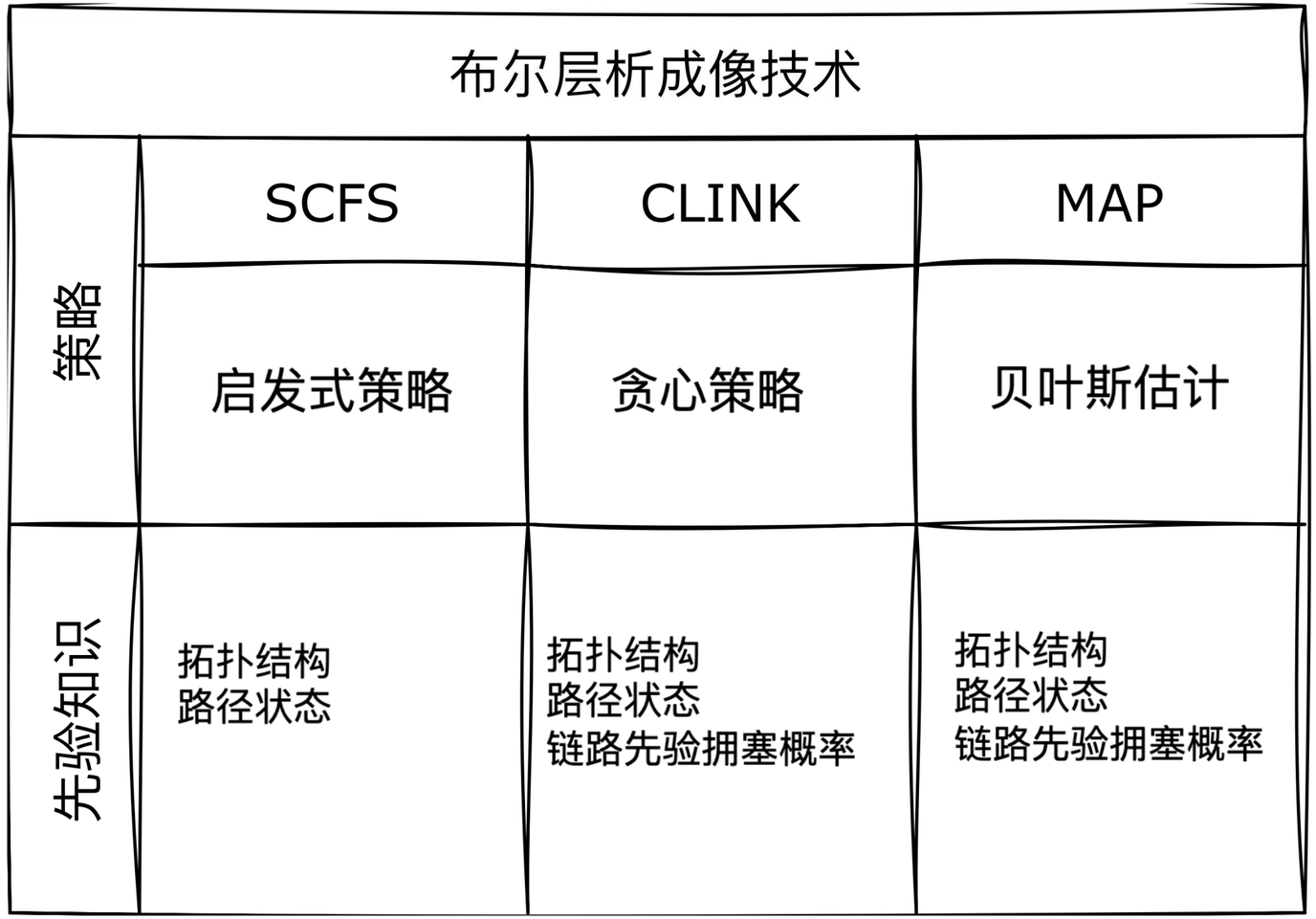
拓扑来源：www.topologyzoo.org

1.2 网络布尔层析成像



网络状态的**代数表示**方式转化为**二元表示**

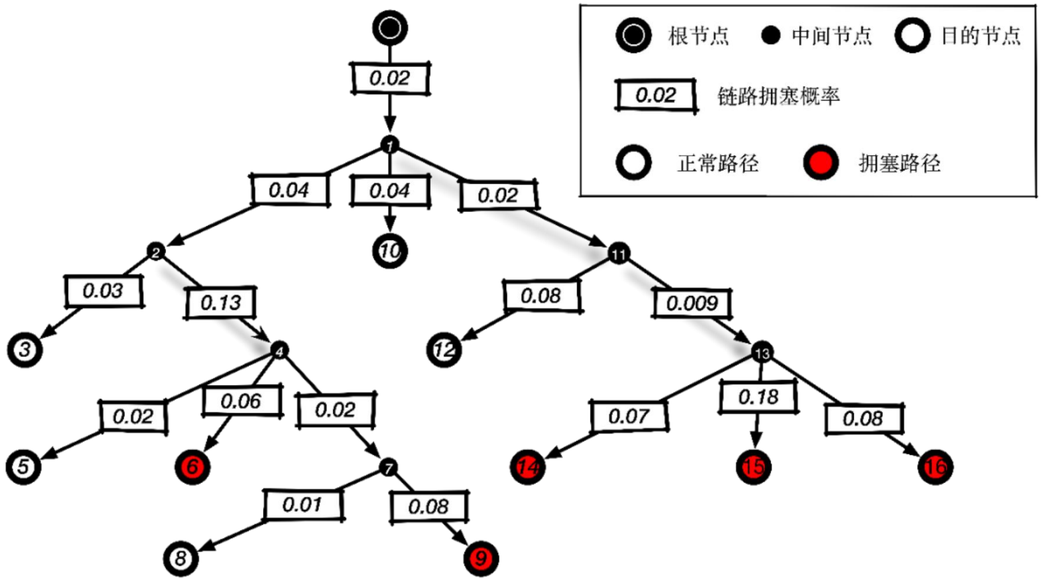
1.2 网络布尔层析成像



不同的策略带来了不同的优缺点

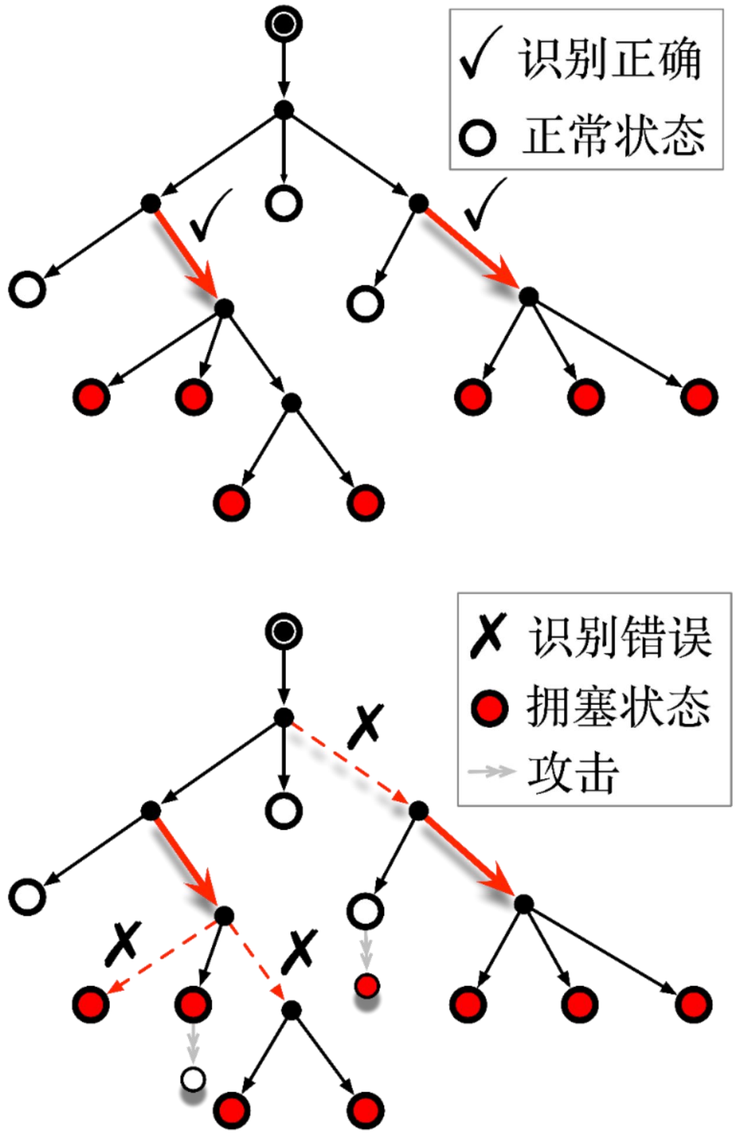
1.2 网络布尔层析成像

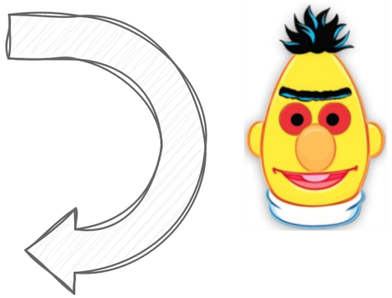
布尔层析成像技术	
SCFS	1. 得到拓扑结构及路径拥塞状况 2. 基于最大似然估计(MLE), 得到最大坏子树 3. 选取最大坏子树的根链路为拥塞链路，即链路6、链路9和链路13
CLINK	1. 得到拓扑结构、路径拥塞状况及链路先验拥塞概率 2. 最小化 $\log \frac{1-p_k}{p_k} / \lvert Domain(e_k) \rvert$ 每次将一条路径的拥塞归因于一条链路 3. 由 $\arg\min\{\log \frac{1-p_k}{p_k} / \lvert Domain(e_k) \rvert\}$ 输出链路15，值为1.52 4. 依次输出链路13、链路9、链路6
MAP	1. 得到拓扑结构、路径拥塞状况及链路先验拥塞概率 2. 基于贝叶斯概率模型，得出已知路径状态，链路的可能状态中最大后验概率的情况 3. 得出拥塞概率最大的链路为链路6、链路9及链路13



图为某一时刻对网络状态的端到端测量，
各链路的先验拥塞概率由过往的测量快照得出

1.3 拜占庭攻击

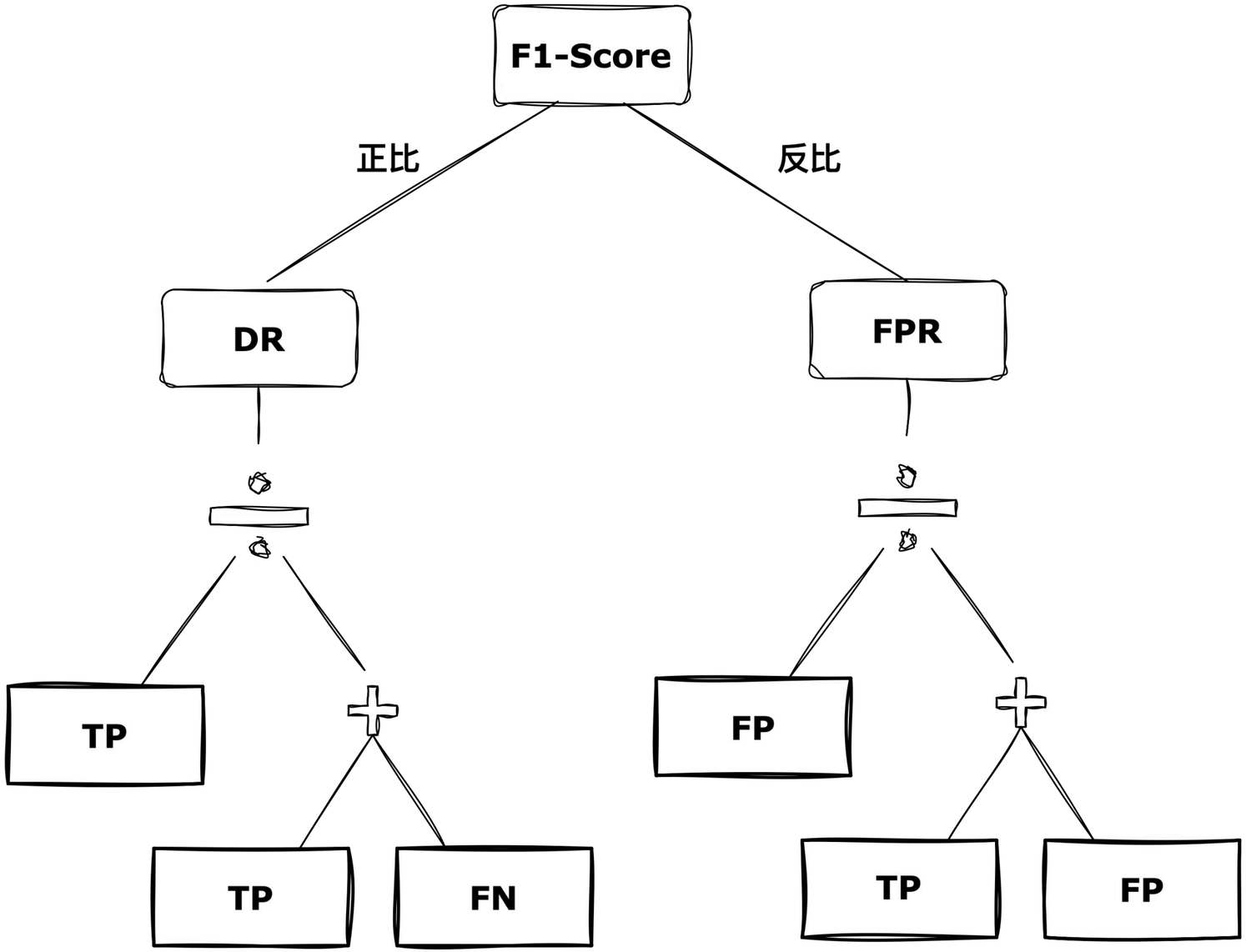




迫使被攻击节点
对测量者做出不诚实的回答

左图为拜占庭攻击下的布尔层析成像

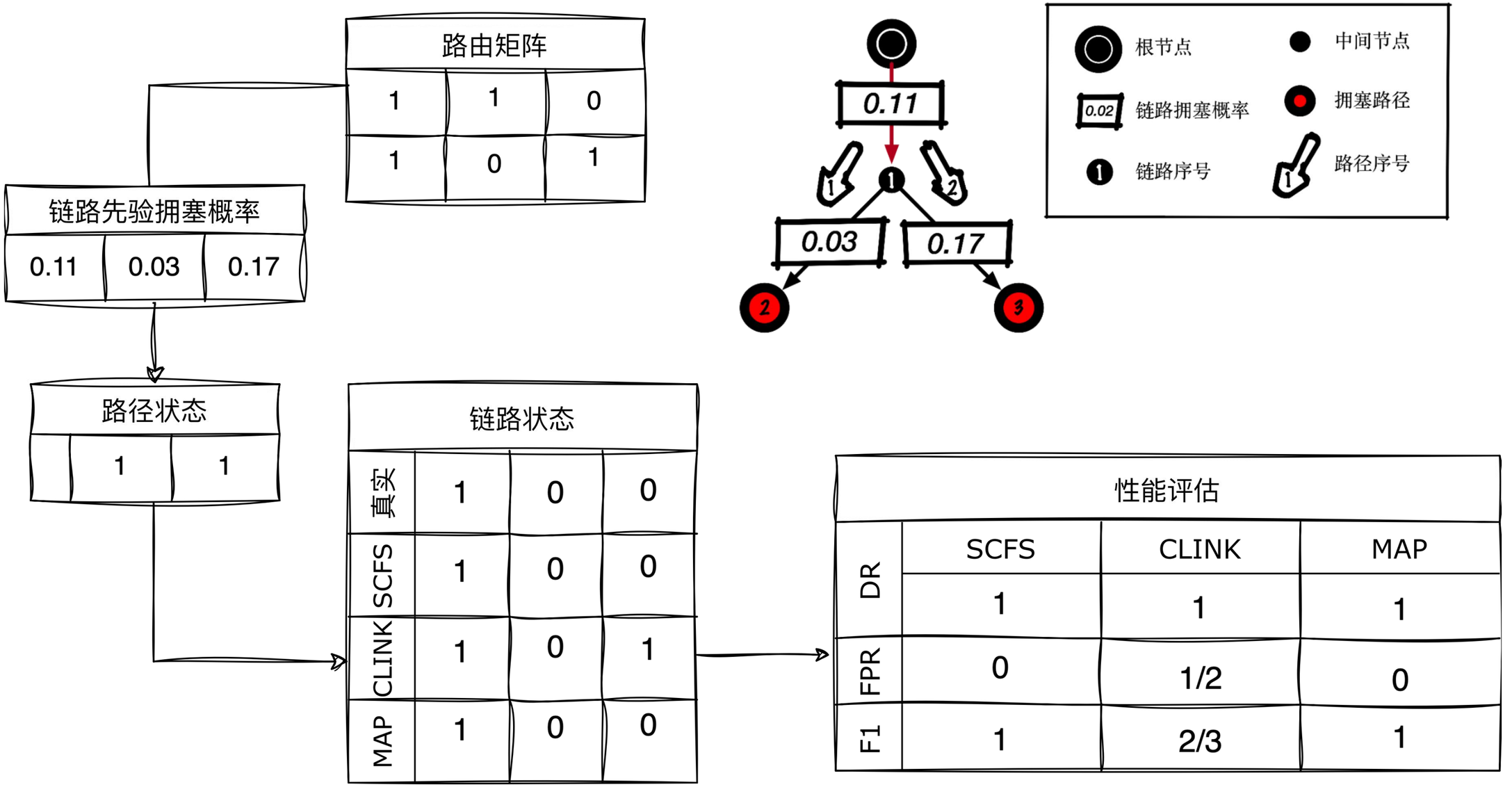
1.4 评价指标



性能评估过程所用到的评价指标

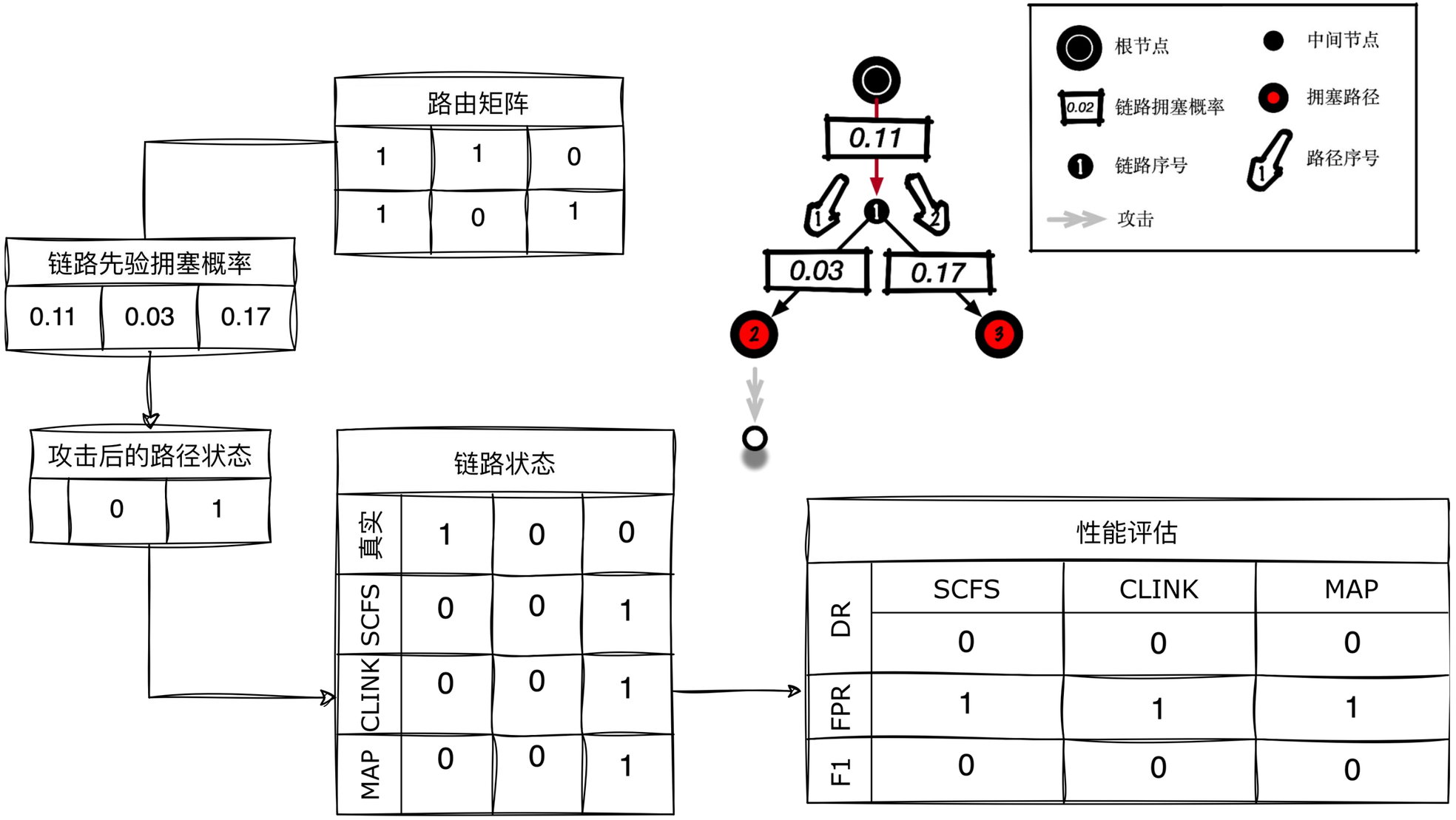
主要工作

2.1.1 网络模拟



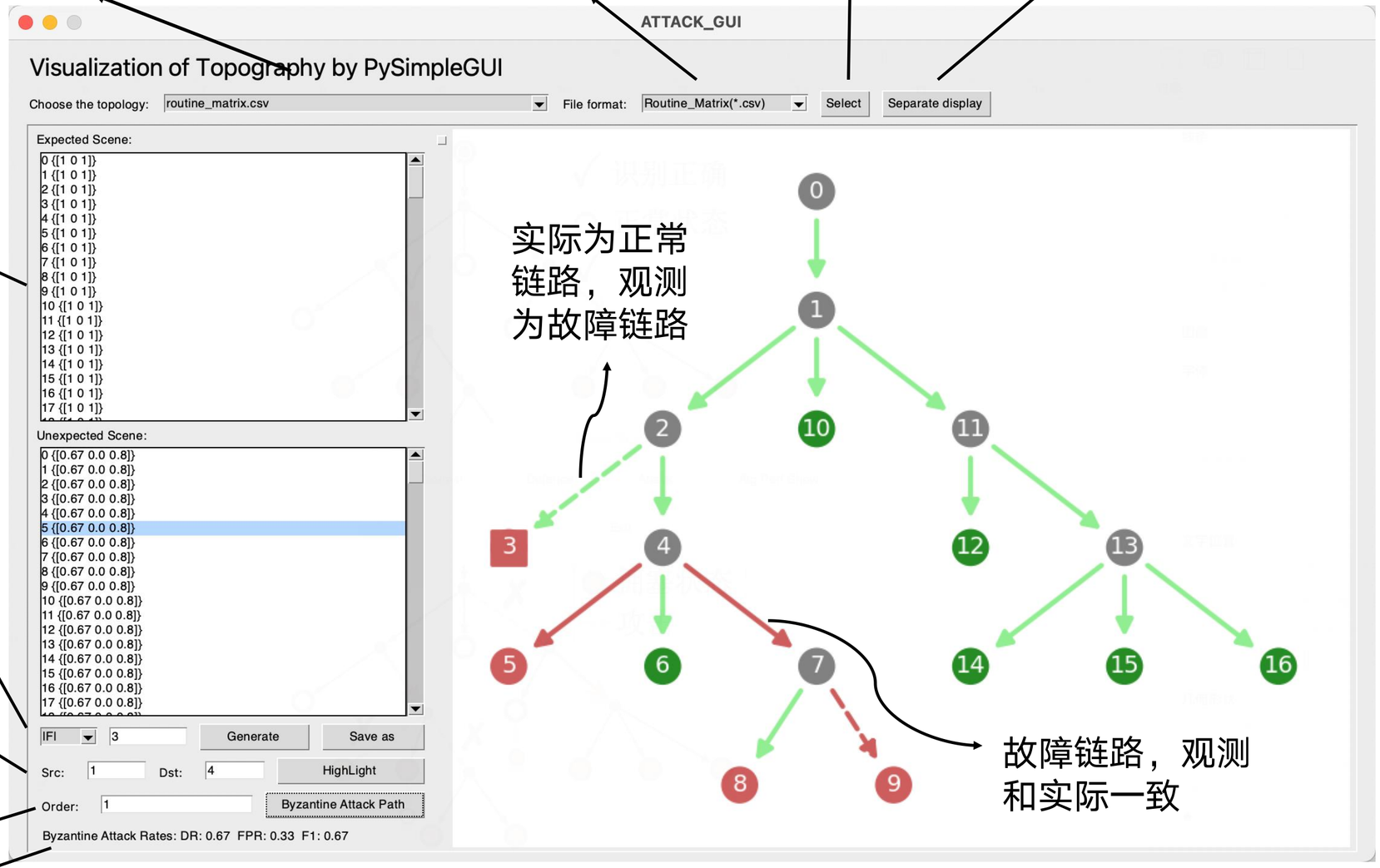
网络拓扑、布尔层析成像及性能评估参考流程

2.1.2 攻击模拟



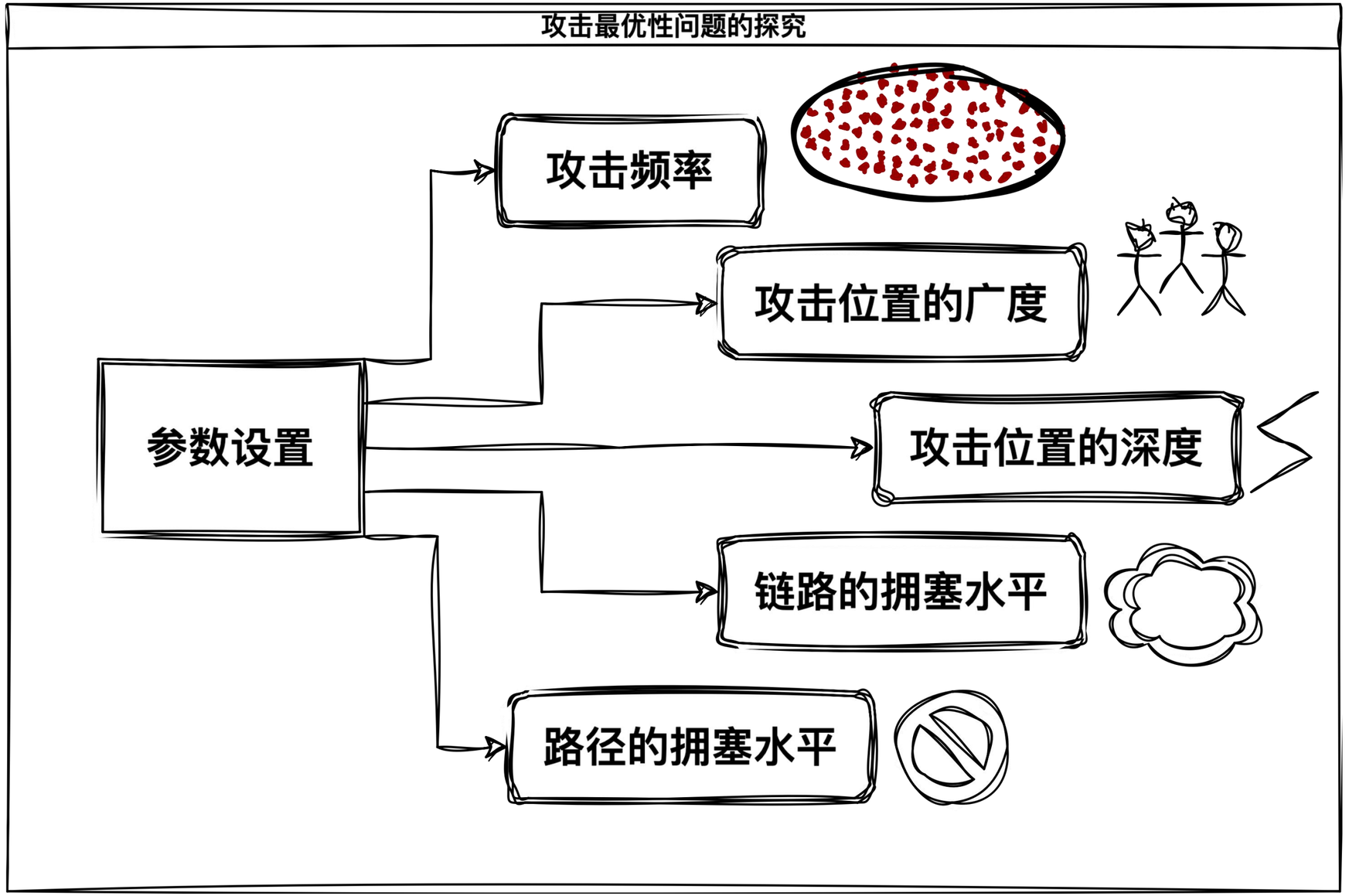
网络拓扑、攻击、布尔层析成像及性能评估参考流程

2.2 攻击有效性



布尔层析成像技术及攻击的可视化界面: https://gitee.com/eric-teng/nbt-byz-att-gui

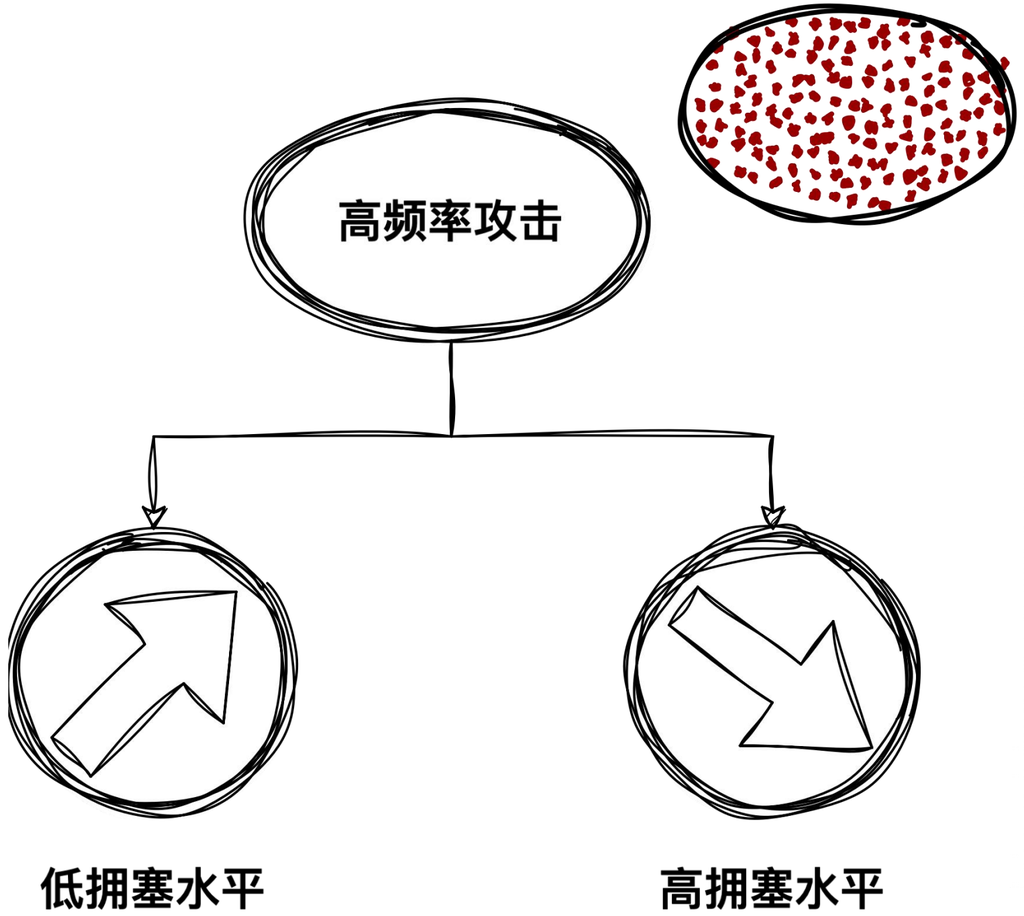
2.2 攻击优化性

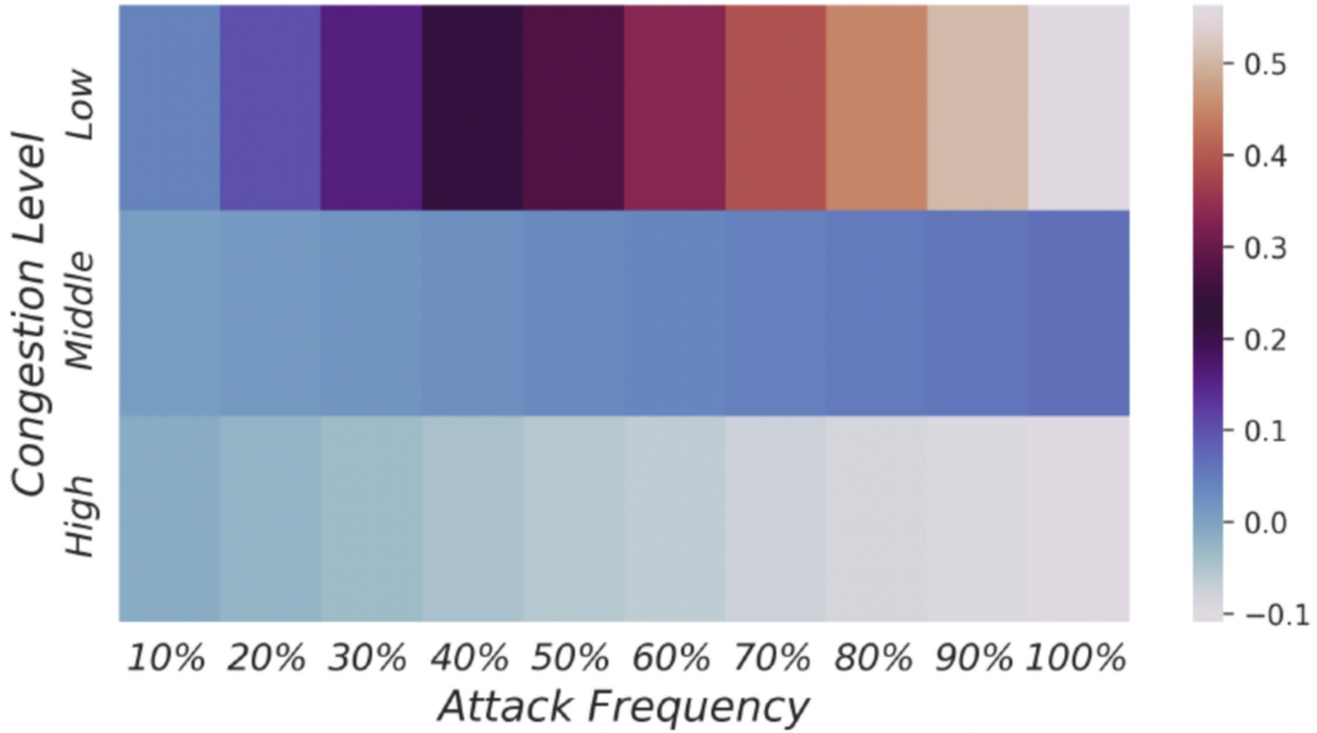


代码及示例图样都已开源：https://gitee.com/eric-teng/eval_nbt_vs_byzantine

实验结果

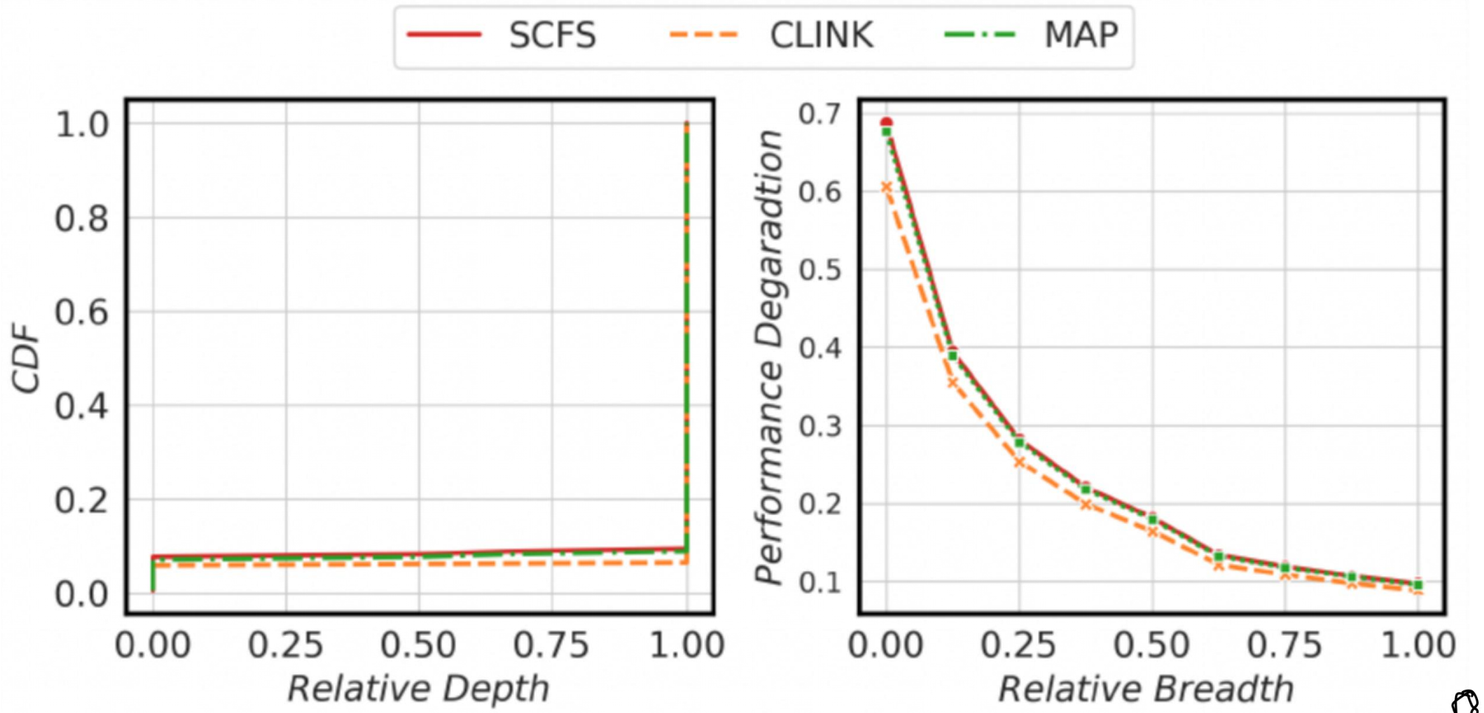
3.1 攻击频率vs攻击效果

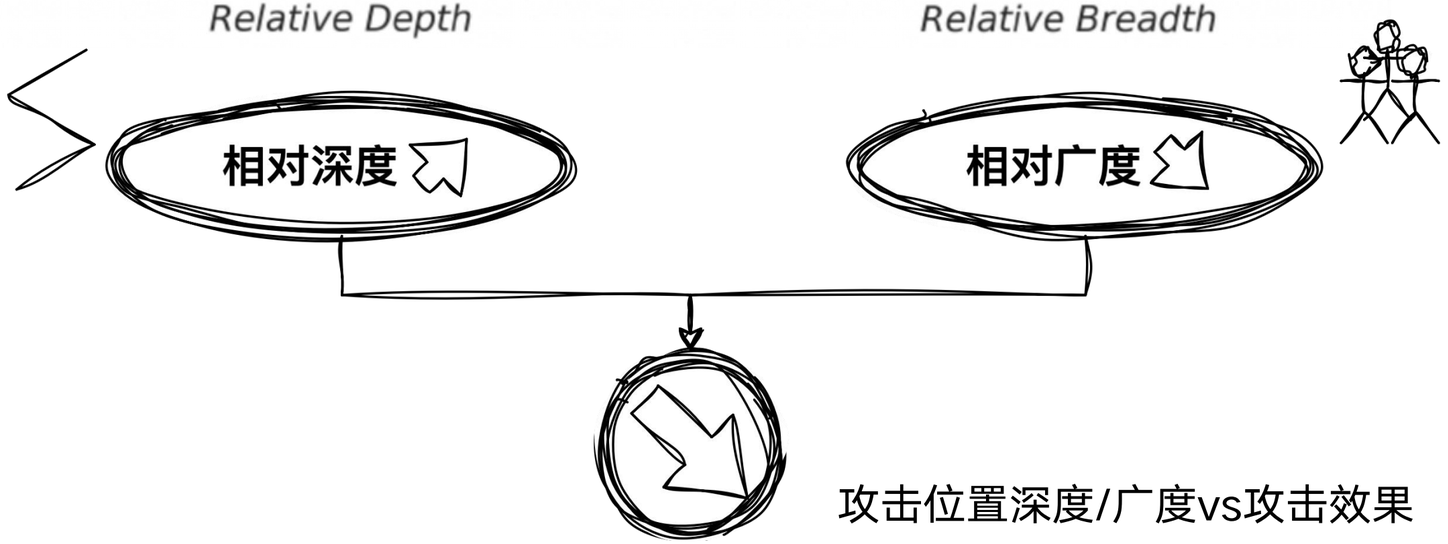




攻击频率vs攻击效果vs拥塞水平

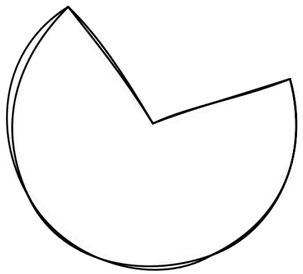
3.2 攻击位置深度/广度vs攻击效果



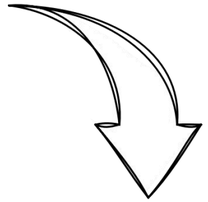


攻击位置深度/广度vs攻击效果

3.3 链路拥塞水平vs攻击效果



攻击效果普遍
呈下降趋势



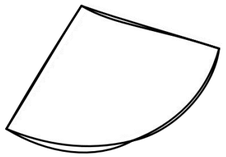
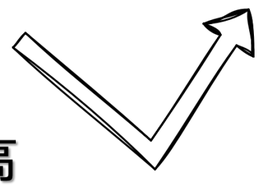
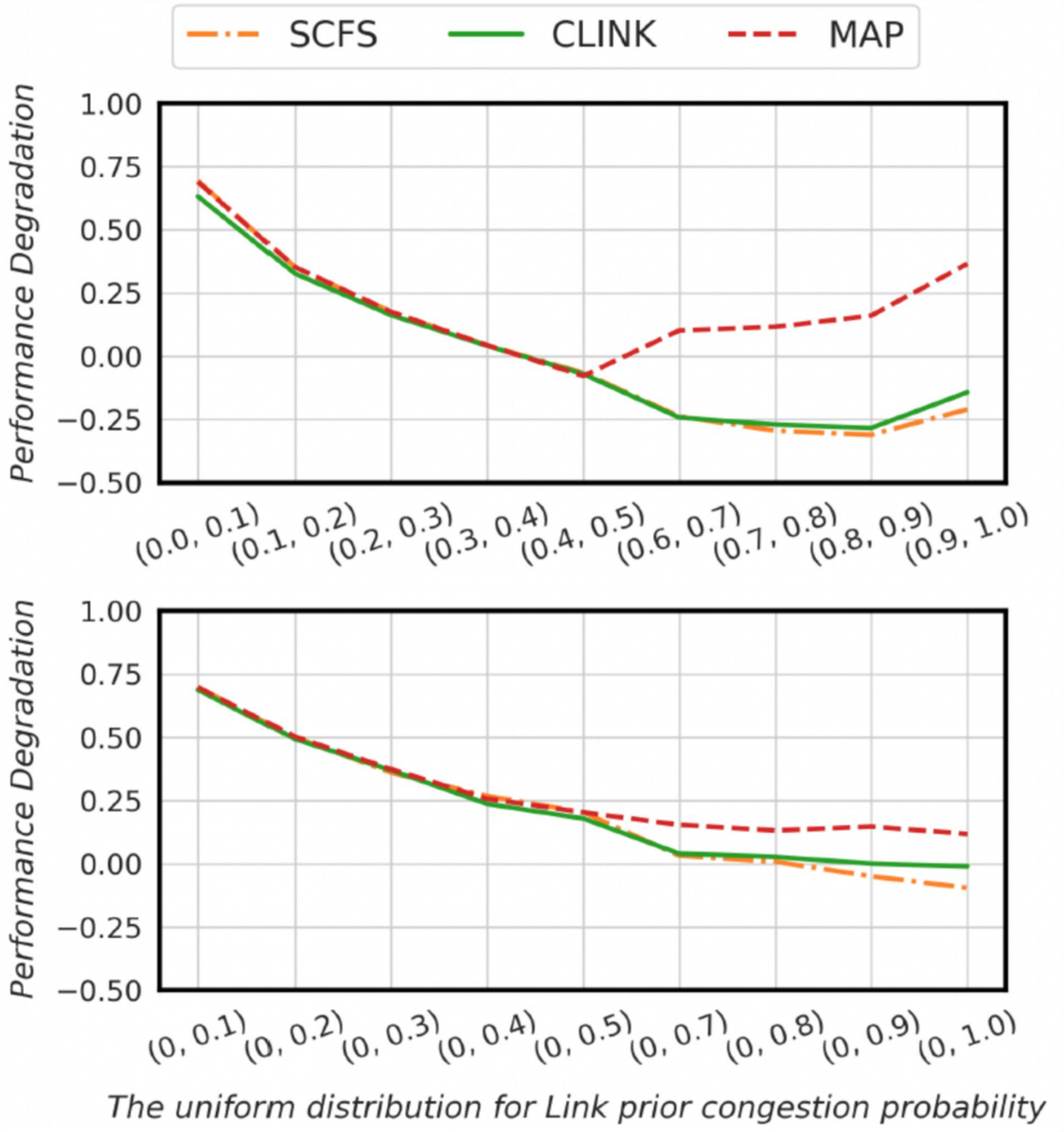


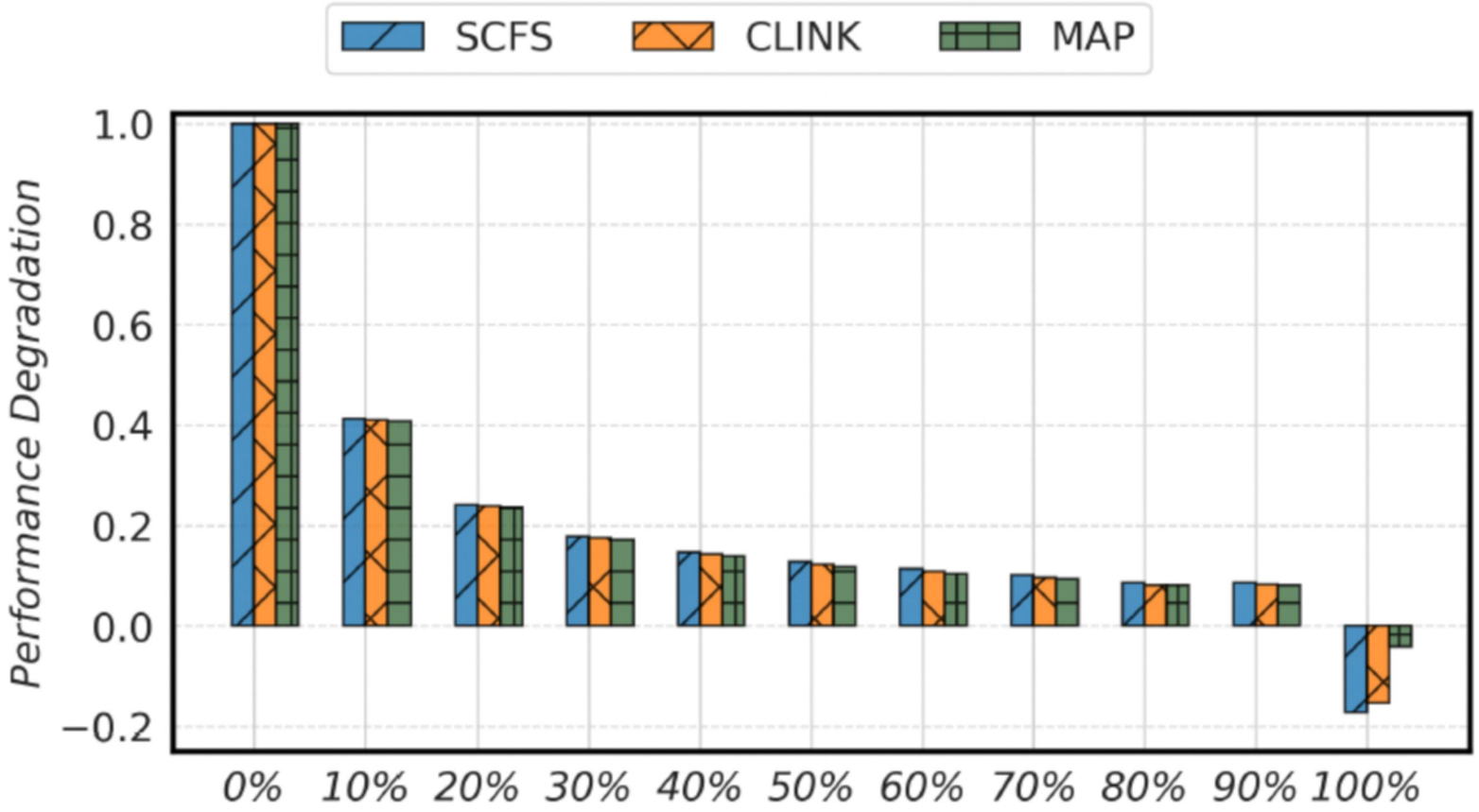
图1中MAP的准
确率在0.5后升高





链路拥塞水平vs攻击效果

3.4 路径拥塞水平vs攻击效果



路径拥塞水平vs攻击效果

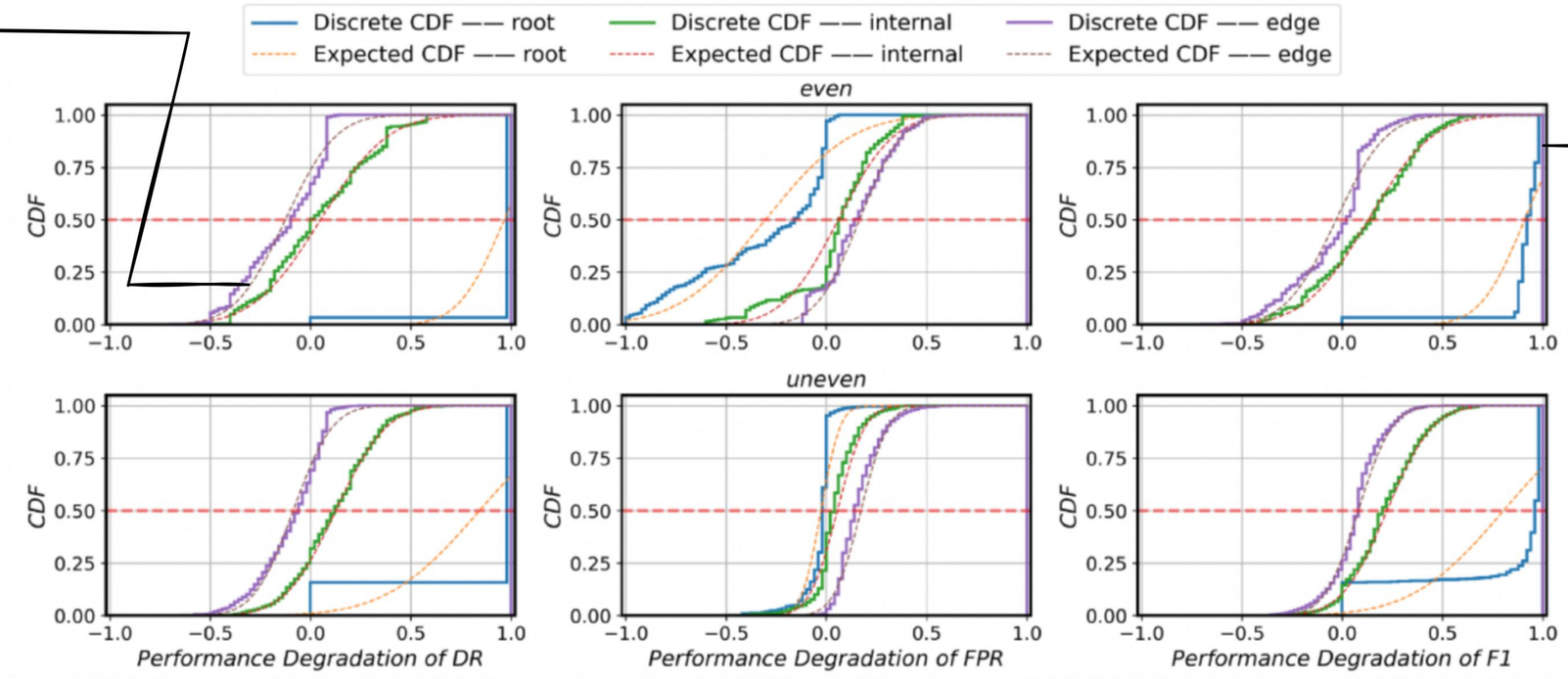
随着路径拥塞水平的升高，攻击效果逐渐降低

结论分析

4.1 不同的攻击链路

中间链路和边缘链路被攻击的时候，由于可能会使中间链路及边缘链路的权重增大，使得在某些时候性能反而会有提升

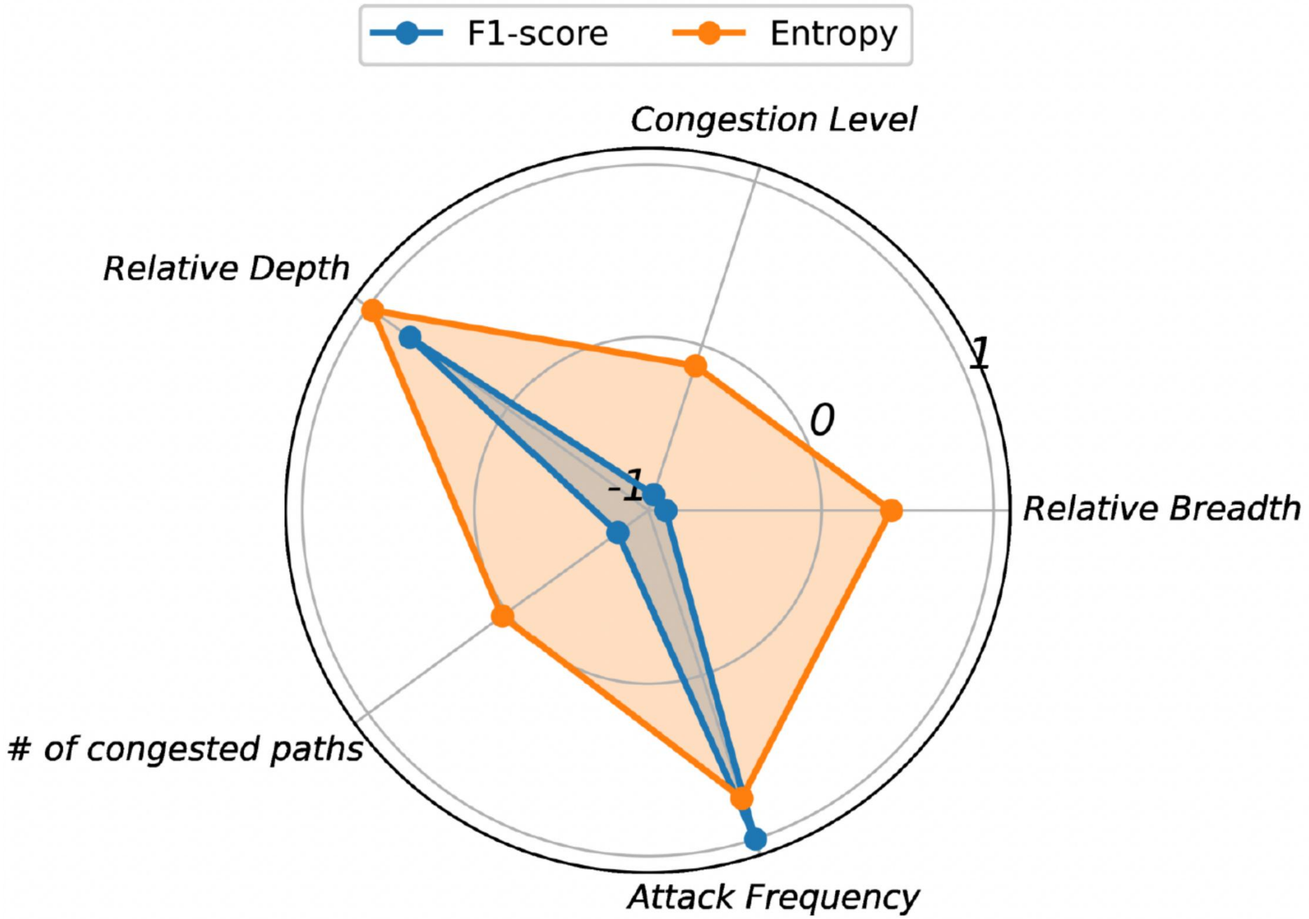
对于根链路而言，攻击一旦影响，损失是最大的



不同拥塞概率分布下，链路位置不同导致的性能下降差异

4.2 熵

雷达图		
	强相关	弱相关
F1	All	-
熵	深度、频率	拥塞强度、攻击广度



各参数同F1/熵的相关系数雷达图

总结与展望

5 总结与展望

本文贡献:

- ✓ 验证了布尔层析成像算法在拜占庭攻击下的脆弱性以及攻击的普适性
- ✓ 解释了拜占庭攻击对网络拓扑中不同种类链路的不同影响
- ✓ 探讨了网络布尔层析成像技术下，拜占庭攻击效果的优化性问题

未来研究方向:

- ✓ 动态网络场景下的攻击方案设计
- ✓ 基于强化学习的网络攻防对抗技术
- ✓ 基于Stackelberg竞争博弈理论的对抗战略研究

研究成果

2023 IEEE Global Communications Conference: Selected Areas in Communications: Satellite and Space Communications

Evaluating Network Boolean Tomography under Byzantine Attacks

1st Haotian Deng
School of Cyberspace Security
Beijing University of Posts and Telecommunications
Beijing, P. R. China 100876
haotian_deng@bupt.edu.cn

School of Cyberspace Security
Beijing University of Posts and Telecommunications
Beijing, P. R. China 100876

***Abstract*—It is vital to closely track the operation statuses of network-internal links. Accurate knowledge of the operation statuses of network-internal links is vital for the management of many networks like the Internet, the satellite communication network, etc. Network boolean tomography can identify congested links just using end-to-end path status observations, and is able to work efficiently even without any available cooperation of internal nodes. Nevertheless, it heavily assumes that all the path status observations collected are true while some Byzantine attacks, e.g., the label flip attacks, could violate this assumption. In this paper, we present a performance evaluation of network boolean tomography under Byzantine attacks. Our results against various attacking rates, locations, and scales all show that Byzantine attacks could cause a significant performance degradation of network boolean tomography, suggesting a pressing need of developing the detection and countermeasure techniques.**

***Index Terms*—network boolean tomography, congested link identification, end-to-end measurement, Byzantine attacks**

I. Introduction

Network boolean tomography [1] is a potent tool for localizing traffic congestion or jamming in communication networks. It could be well applied to various types of networks, like the Internet, IoT, satellite, and space communication networks, where it helps identify and understand the effects of signal jamming, transmission interference [2], and bandwidth consumption attacks, etc. Note that though the structure of the satellite network is rather dynamic, its routing topology is technically virtualized as static, making netowrk boolean tomography also an appealing tool for monitoring network performance of satellite networks. To evaluate internal communication jamming is a fundamental aspect of network management. It enables network administrators to quickly detect and troubleshoot issues, plan for future capacity needs, harden network security, optimize costs associated with network usage, and so on. However, almost all of today's communication networks are known vulnerable to a wide range of attacks [3], [4], including Byzantine attacks [5], which can significantly impact the performance of network boolean tomography.

Network boolean tomography first quantifies and gathers the binary status of paths (i.e., "good" or "bad") by comparing their performance observations to a predefined threshold, e.g. in Fig. 1(a), the observed packet loss ratio of a path greater than 1% will indicate that it gets a bad or congestion status; otherwise, its status is good [6]. These observed path statuses then are reasoned by the Bayesian framework of Maximum A Posteriori (MAP) attribution to identify congested links. However, the MAP problem here is normally NP-hard. To circumvent the NP-hardness, [7] proposed the "CLINK" algorithm for a greedy identification, while the "SCFS" algorithm of [6] chose to remove any prerequisite of links' prior congestion probabilities and simplified it as a Maximum Likelihood Estimation (MLE) problem. Besides the NP-hardness, there were also works to address other issues like probing [8], scalability [9], [10], dynamic routing, identifiability [11], sparsity [12], and so on.

Nonetheless, most of the existing works on network boolean tomography assume a benign scenario. More specifically, they tacitly require all the measurements obtained to be dependable. This becomes increasingly demanding in today's Internet, in the context of the growing number and sophistication of both cyber threats and attacks [3]. One commonly-discussed threat would be Byzantine attacks [5], where the compromised participants will not always behave in accordance with the measurement protocol [13], but can report their results dishonestly during the measurement collection procedure. As illustrated in Fig. 1(b), after the third edge node (i.e., the one with its congested/bad status changed to "good") from the left dishonestly tells its path status observation as "good"

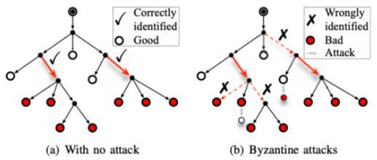


Fig. 1. Illustration of network boolean tomography [6] with and without attacks. There are two congested links depicted in red and bold solid arrows. In (a), both congested links are correctly identified while in (b), not only neither of them are detected, but three other links are even wrongly identified.

* Corresponding author: Shengli Pan was also with the Key Laboratory

Evaluating Network Boolean Tomography under Byzantine Attacks

Haotian Deng (✉ : haotian_deng@bupt.edu.cn) and
Beijing University of Posts and Telecommunications (BUPT), Beijing, China 100876

Introduction

- Require knowledge of peer networks' link performances to better deploy services, but have no direct monitoring access.
- Rely on end-to-end measurements to indirectly infer these link performances of peer networks, normally using MAP strategy.
- The ill-posed nature of above inference problems gives

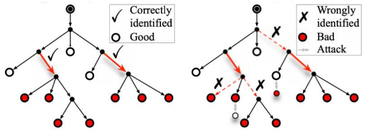
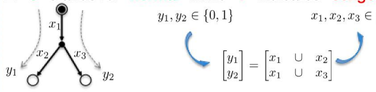


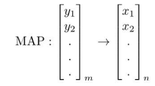
Fig. 1. Illustration of network boolean tomography [6] with and without attacks. There are two congested links depicted in red and bold solid arrows. In (a), both congested links are correctly identified while in (b), not only neither of them are detected, but three other links are even wrongly identified.

Preliminaries

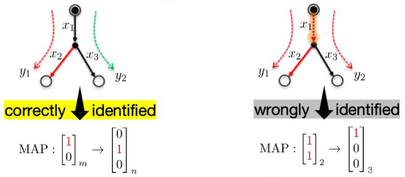
- "0" stands for "normal" while "1" indicates "congestion".



- Network boolean tomography employs the MAP strategy to infer unknown statuses of each link from path status observations.
  - # of links > # of paths



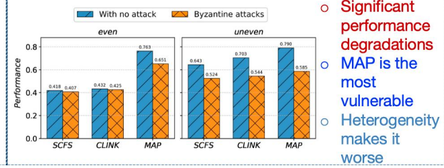
- End nodes could be the Byzantine ones that are able to falsify the observation results of path statuses, e.g., reporting "1" for being congested while a path gets a "normal" status of "0".



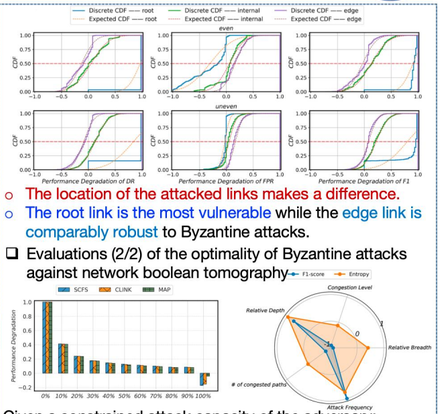
- Under a Byzantine adversary setup, does network boolean tomography still perform well? If not, what degradation will it have?

Evaluations

- Simulation setup: > 170 real networks from the "Topology Zoo" dataset[1]; 1000 times repeated for each scenario; 20 times repeated for Byzantine attack.
  - [1]http://www.topology-zoo.org/index.html
- Evaluations (1/2) of the effectiveness of Byzantine attacks against network boolean tomography



  - Significant performance degradations
  - MAP is the most vulnerable
  - Heterogeneity makes it worse



  - The location of the attacked links makes a difference.
  - The root link is the most vulnerable while the edge link is comparably robust to Byzantine attacks.
- Evaluations (2/2) of the optimality of Byzantine attacks against network boolean tomography

Given a constrained attack capacity of the adversary:
  - "Depth" of the attacking surface is "better" than the "breadth".
  - Accordingly, heavier the attack, better the attack gain.

Conclusion

- The inference uniqueness against the ill-posed nature of network boolean tomography makes it vulnerable to Byzantine attacks.
- Network heterogeneity, attack location, and attack depth all will make a great difference to the attack gain.
- Attack-resilient network boolean tomography techniques are needed, e.g., AI empowered network boolean tomography.

➢ 第一作者论文成果

Evaluating Network Boolean Tomography under Byzantine Attacks, IEEE GLOBECOM, 2023. (CCF-C, IEEE通信领域两大旗舰会议之一)