

基于 SNMP 的拓扑增强识别算法^①



曾 戈, 李 银, 李 睿

(东莞理工学院 网络空间安全学院, 东莞 523808)

通信作者: 李 睿, E-mail: rui.li@dgut.edu.cn

摘 要: 网络拓扑发现对于许多关键网络管理任务来说至关重要. 然而, 随着网络规模的不断增大, 网络结构的愈发复杂, 之前的基于 SNMP 的网络拓扑发现算法存在难以有效识别子网类型和多 IP 设备, 拓扑效率、准确率低等问题. 针对上述问题, 本文提出了基于 SNMP 的拓扑增强识别 (SNMP-based topology enhanced identification, SNMP-TEI) 算法. 首先, 启发式地确定子网 IP 地址并对其发送探针, 根据探测结果来判断子网类型, 在确定子网类型后及时终止探针注入防止网络负载过大; 其次通过 MIB-II 记录的系统信息设置设备指纹, 结合设备类型识别算法对终端主机 IP 进行设备指纹鉴定, 以达到识别多 IP 设备的目的. 实验结果表明, 此方法在仿真网络中可有效识别子网和多 IP 设备, 同时降低了网络负载, 探测准确率达到 96.43%.

关键词: 网络管理; SNMP; 网络拓扑发现; 子网识别; 多 IP 设备识别

引用格式: 曾戈, 李银, 李睿. 基于 SNMP 的拓扑增强识别算法. 计算机系统应用, 2023, 32(2): 226-233. <http://www.c-s-a.org.cn/1003-3254/8993.html>

SNMP-based Topology Enhanced Identification Algorithm

ZENG Ge, LI Yin, LI Rui

(School of Cyberspace Security, Dongguan University of Technology, Dongguan 523808, China)

Abstract: Network topology discovery is important for many key network management tasks. However, as the network scale expands, the network structure gets complex. The previous SNMP-based network topology discovery algorithms cannot effectively identify subnet types and multi-IP devices, and they have low topology efficiency and accuracy. In view of the above problems, this study proposes an SNMP-based topology enhancement identification (SNMP-TEI) algorithm. Firstly, the subnet IP address is heuristically determined, and probes are sent to it, so as to judge the subnet type according to the detection results. In addition, probe injection is stopped in a timely manner after the subnet type is determined, so as to prevent the network load from being too large. Secondly, the device fingerprint is set through system information recorded by MIB-II, and a device type identification algorithm is used to identify the device fingerprint of the terminal host IP, so as to identify multi-IP devices. The experimental results show that this method can effectively identify subnets and multi-IP devices in simulated networks and reduce the network load, with a detection accuracy of 96.43%.

Key words: network management; simple network management protocol (SNMP); network topology discovery; subnet identification; multi-IP device identification

网络拓扑是用来表示网络逻辑连接关系和物理连接关系的一种方法^[1,2]. 通过网络拓扑结构, 网络管理员可以清晰地管理网络中的资产, 了解资产分布; 直观地

了解当前网络的运行情况, 及时发现网络故障, 进行根源分析^[3]. 此外, 网络管理员可以基于网络拓扑评估网络的性能, 评估保护网络免受恶意入侵和攻击技术的

① 基金项目: 国家重点研发计划 (2021YFB3101300); 国家自然科学基金面上项目 (61972089)

收稿时间: 2022-06-13; 修改时间: 2022-09-07; 采用时间: 2022-09-27; csa 在线出版时间: 2022-11-18

CNKI 网络首发时间: 2022-11-21

有效性,为资源配置开发改进设计^[4]。显然,网络拓扑对于网络管理具有重要意义,而网络拓扑发现技术成为构建网络拓扑的关键。

当前,随着计算机技术和网络技术的飞速发展,下游应用生态将得到快速拓展,进一步促进了网络规模的扩大^[5]。复杂网络带来的动态性、多样性、异构性和庞大性成为网络拓扑发现技术的重点和难点,传统的单机网络管理和维护模式已不再适用^[6]。SNMP (simple network management protocol) 协议目前广泛应用于网络中,其 MIB (manager information base) 记录了丰富的拓扑信息,基于 SNMP 的网络拓扑发现方法^[7]具有算法设计易、网络负载低、发现效率高的优点,因此,该算法已成为研究者常于使用的拓扑发现手段之一。

此前基于 SNMP 的网络拓扑发现算法存在两个问题: (1) 该算法都是通过获取路由设备的路由表,根据表中的路由条目进行广度优先或深度优先遍历骨干网络。直连路由表条目会被认定为连接一个子网。然而,网络中两个路由设备之间的子网存在两种情况:一种是只有一条链路连接两个路由设备,本文称为链路子网,如图 1(a) 所示;另一种是两个路由设备之间存在提供网络服务的网络设备,本文称为多网口子网,如图 1(b) 所示。之前的基于 SNMP 的网络拓扑发现算法为对这两种子网均直接探测,会因未考虑存在链路子网的情况而生成错误的网络拓扑结构且注入大量的探针。(2) 由于特定的网络需求,网络中的某些主机通常与多个子网相连,其 IP 地址与 MAC 地址不再是唯一的。当拥有多 IP 的设备出现在待测网络中,此前的基于 SNMP 的网络拓扑发现算法可能会将它识别成多个不同的设备。

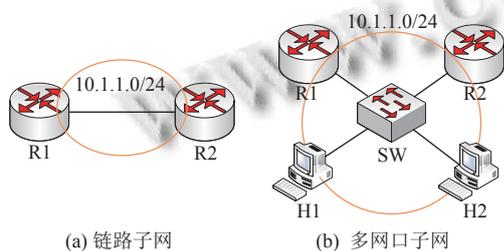


图1 子网类型

针对问题 1,本文提出基于 ICMP (Internet control message protocol) 的子网类型识别方法,对子网内人们惯于使用的 IP 地址发送 ICMP 探针,根据探测出的活跃设备来判断子网类型。在识别链路子网提高拓扑准确率的同时,也减少了链路子网的冗余探测,大大减少

了探针数量和节省了拓扑时间。针对问题 2,本文提出基于 SNMP 的多 IP 设备判别方法,采用 MIB-II 中保存的系统信息作为设备指纹,并建立设备指纹与设备 ID 的映射关系。在探测主机时,依据系统信息来匹配 IP 所属的主机。在识别链路子网提高了拓扑准确率的同时,利用哈希映射的快速查找原理保证了识别效率。相比其他拓扑发现算法,依赖的网络协议仅有 SNMP,使得可拓展性更强、适用面更广。实验结果表明,本文方法在仿真网络中不仅有效识别了链路子网和多 IP 设备,而且减少了探针数量、节省了拓扑发现时间,探测准确率达到了 96.43%。

本文第 1 节介绍相关工作;第 2 节介绍本文提出的基于 SNMP 的拓扑增强识别算法;第 3 节对本文提出的基于 SNMP 的拓扑增强识别算法进行仿真实验,并与相关算法的实验结果进行对比分析;第 4 节总结全文并展望下一步工作。

1 相关工作

基于 SNMP 的网络拓扑发现算法主要步骤为:将探测源模拟成一个网管站,收集各待测 SNMP 代理服务器的 MIB 对象,并从 MIB 对象中提取拓扑信息。利用这些信息,先找到一个路由器,然后获得与该路由器相连的所有子网地址、子网内的活跃设备,以及直接相邻的其他路由器。再以这些新发现的路由器为索引,重复上述步骤,直到获取待测网络的整个拓扑信息^[8]。

对于网络拓扑发现算法,研究者通常注重于如何提高网络设备及其连接关系的拓扑完整性。贝尔实验室的 Breibart 等^[9]提出了基于 MAC 地址转发表的数据链路层拓扑发现算法。他们根据转发原理总结了网络节点之间的连接关系判别引理,并证明了引理的正确性。Jiang 等^[10]提出的基于 MAC 地址转发表的拓扑发现算法,对交换机和主机之间的 3 种不同连接关系的拓扑发现进行了论述。基于地址转发表的网络拓扑发现算法对于地址转发表的完整性有很高要求,因此会注入大量探针维护其完整性,从而增加网络的负载。虽然基于 SNMP 的算法适用于骨干网络的拓扑发现,但是对于子网中的网络设备发现效率不高。因此研究者开始采用以 SNMP 为主,其他协议为辅的多协议协作的网络拓扑发现算法。Yin 等^[11]提出的基于 SNMP、ARP (address resolution protocol)、ICMP 的拓扑发现算法,根据 Bridge-MIB 找出 ARP 表中的交换机 IP 和

主机 IP, 再根据交换机中 MAC 地址转发表获得与主机的连接关系. 该方法能更为精准地发现网络拓扑, 但是具有复杂连接关系的子网拓扑发现效果并不理想. Zhou 等^[12]提出了基于 SNMP、LLDP (link layer discovery protocol) 的多协议网络拓扑发现算法. 具体做法是当探测到无 SNMP 服务的设备, 则通过 LLDP MIB 获取各个端口连接的 IP 地址以及网络设备的连接关系. 该方法能提高拓扑发现准确度, 但对于协议的依赖更为严重. 潘爽等^[13]提出的多协议融合的网络拓扑发现技术结合基于 CDP (cisco discovery protocol)、SNMP 的设备发现方法对逻辑拓扑发现和物理拓扑发现算法进行优化, 增加了应用层拓扑, 缺点是较为依赖设备指纹库. Nakamura 等^[14]提出的拓扑发现算法使用 SNMP 获取流量信息并分析拓扑结构, 其缺点是未考虑到多设备之间流量相似的场景. 钟成龙^[15]利用 LLDP 获取网络邻居节点、SNMP 获取拓扑信息的网络拓扑发现算法拥有较高的准确率和较低的时间复杂度, 但是其缺点是两种协议缺一不可, 可拓展性较差.

研究者近年来同样致力于如何提高拓扑发现的时间效率以及如何更具体地识别网络设备类型. Li 等^[16]提出的算法解决了路由表冗余、路由表错误的问题, 并设计了一个基于异步多线程算法的 SNMP 软件开发工具包 (包括编码、解码、网络操作等). Wang 等^[17]提出基于 SNMP 的子网信息去冗算法. 通过子网列表和下一跳路由表的交集来获得更为精确的子网信息, 提高拓扑发现的效率. Wang 等^[18]提出的网络拓扑发现算法改良了 SNMP 的数据采集方式. 通过替换 SNMP 数据包的冗余字段, 使得一次操作可以完成大量的数据采集指令, 从而提高数据采集效率. 该算法虽然提高了拓扑发现效率, 但是待测网络需要使用这种改造的 SNMP, 局限性同样巨大. Pandey 等^[19]基于 MIB 的网络设备类型识别算法和 VLAN 逻辑拓扑发现算法. 利用不同的 MIB 来识别网络设备类型, 如 Bridge-MIB、Printer-MIB; 利用 Q-Bridge-MIB 获取 VLAN 信息. 杨凯江等^[20]提出了识别边界设备的网络拓扑发现算法和多区域拓扑合成算法. 具体做法是建立边界设备指纹库, 通过探测匹配的方式发现防火墙等设备, 以及利用边界设备作为不同区域拓扑的连接点达到多区域网络拓扑的合成. 该算法虽然能识别部分边界设备, 但是过于依赖已有的信息, 对于陌生网络中的边界设备无能为力.

基于 SNMP 的拓扑发现算法最大的优点在于其利用

了包含丰富拓扑信息的 MIB 对象, 使得算法设计相对简单, 且无需向网络中注入大量的探针, 运行效率较高. 但缺点也显而易见, 由于 MIB 中信息定时更新, 因此通过此方式并不能实时读取网络信息, 更为严重的是对于不支持、不开放 SNMP 的网络设备, 该算法束手无策.

2 SNMP-TEI 算法

为了解决上述问题, 本节提出了 SNMP-TEI 算法. 其核心思想是采用广度优先遍历待测网络, 在骨干网络中探测到直连子网时, 采用 ICMP 探针探测子网地址, 根据活跃地址判断子网类型; 在子网中探测到终端主机时, 采用系统信息作为设备指纹, 并依据该设备指纹判断 IP 地址是否属于同一设备.

2.1 子网类型识别

在递归探测路由器时, 首先通过 ipRouteTable 读取路由表, 我们希望通过路由表发现该路由器的邻居, 因此本文使用一种原始路由表去冗方法. 首先需要过滤掉包含环回地址、本机地址的表项. 其次需要逐一判断下一跳地址是否属于路由器的直连子网地址, 如果属于某一子网, 那么将该下一跳地址代替该子网地址, 后续将直接探测下一跳地址而非探测子网. 如此, 既能避免同一邻居的重复探测, 又能避免耗时的子网探测. 最后, 对剩下的直连子网采用 ICMP 探测对该子网进行类型识别.

首先, 构建 ICMP 探针对经常使用的 IP 地址进行探测. 众所周知, 子网中相对靠前和靠后的 IP 地址是人们经常使用的. 例如: 子网 10.1.1.0/24 中的 10.1.1.1-10.1.1.10 和 10.1.1.250-10.1.1.254. 对这些地址发送完探针之后, 通过 ipNetToMediaTable 查看子网的活跃地址. 如果活跃地址仅仅只有子网直连的两台路由设备的接口 IP 地址, 那么这两台路由设备是直接相连的, 为链路子网, 随后立即终止余下子网地址的 ICMP 探测, 避免进行冗余操作; 如果发现了其他活跃 IP 地址, 则为多网卡子网, 继续对余下子网 IP 地址进行探测. 该算法流程如图 2 所示.

基于地址转发表的拓扑发现算法对于路由器、交换机中的 ARP 表、MAC 地址转发表的完整性具有很高的要求. 通常使用该类算法都是需要向待测网络注入大量的 ICMP 探针以保持各种地址表完整. 传统子网探测手段是对待测子网所有 IP 的逐一探测, 而本文算法是更有目的性的 ICMP 探测, 在识别子网类型时能及时终止对链路子网中未使用 IP 地址的探测. 因此相对于传统的子网探测手段来说, 子网类型识别的

ICMP 探测并不会消耗额外的时间和带宽,反而能够减少不必要的探针注入及其带来的时间损耗。

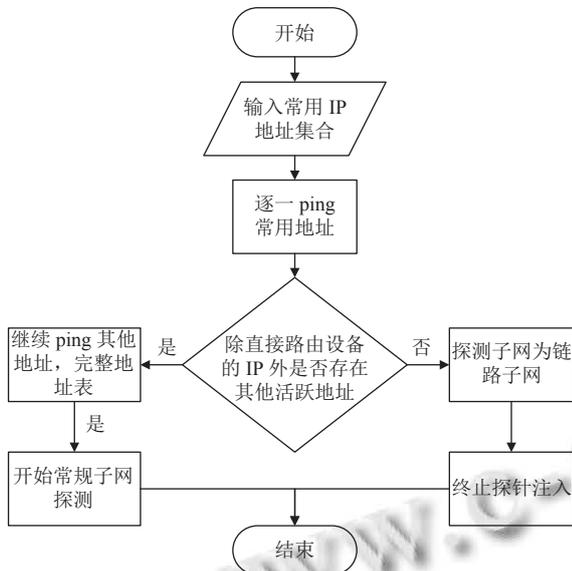


图2 子网类型识别流程图

2.2 多 IP 设备识别

网络拓扑中的每个节点需要独一无二的标识来表示这个节点. 鉴于 IP 地址在一个局域网中具有唯一性, 那么使用设备的 IP 地址作为设备 ID 是可靠的. 至于存在多 IP 的设备, 路由器使用 IP 地址集中最大的 IP 地址作为设备 ID, 多 IP 终端主机则使用首次发现的 IP 地址作为设备 ID.

在进行探测时, 首先需要将网络设备分类成路由器、交换机和终端主机, 其次才能确定网络节点连接关系. 随着技术的进步, 路由器已经可以使用 Bridge-MIB, 交换机也已经具备转发功能, 依靠 Bridge-MIB 和 ipForwarding 的设备类型识别方法^[9] 已经不再适用. Q-Bridge-MIB 中的 dot1qNumVlans 记录了该设备上配置的 VLAN 数量, 通常只有交换机能配置 VLAN, 而其他设备只能使用默认的 VLAN. 因此本文提出一种新的设备类型识别方法: 对于一台设备, 当 dot1qNumVlans>1 为交换机; dot1qNumVlans=1 且 ipForwarding=1 为路由器; dot1qNumVlans=1 且 ipForwarding≠1 时为终端主机.

单网卡多 IP、多网卡多 IP 终端主机的识别问题采用 MIB-II 中的系统信息来确定物理机, 再利用哈希映射快速检索信息的方法来提高匹配速度. 在完成设备类型识别, 探测终端主机时, 选择基于 MIB-II 系统信息的四元组表示设备指纹, 如表 1 所示.

表1 系统信息四元组

| 字段 | 描述 |
|-------------|---------------|
| sysName | 节点名 |
| sysLocation | 节点的物理地址 |
| sysObjectID | 节点供应商的权威标识 |
| sysDescr | 节点的硬件、OS、软件描述 |

拓扑发现程序维护一个全局的设备 ID 到终端主机的系统信息的映射集合, 每次探测终端设备时读取其 sysName、sysLocation、sysObjectID、sysDescr, 并在映射集合中查找是否已存在该设备信息. 如果已存在, 那么将原有的 IP 与当前探测 IP 归为同一终端设备; 如果不存在, 则将新的设备指纹和设备 ID 加入映射集合. 该算法流程如图 3 所示.

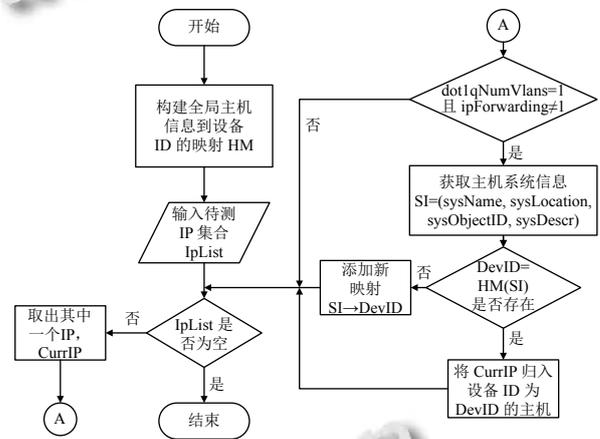


图3 多 IP 设备识别流程图

2.3 算法设计与分析

本文的 SNMP-TEI 算法是在之前的网络拓扑发现算法的基础上加入上述的子网类型识别和多 IP 设备识别. 算法的主要步骤如下.

- 1) 以探测源的网关地址作为探测起点, 初始化主机系统信息映射集合、路由设备集合.
- 2) 如果路由设备集合为空, 跳到步骤 10), 否则跳到步骤 3).
- 3) 选择一个路由设备 IP, 由于冗余链路中运行 STP (spanning tree protocol), 某些接口是阻塞的, 因此对当前路由设备 IP 进行活跃性探测. 如果当前 IP 活跃跳到步骤 4), 否则跳过探测.
- 4) 读取 ipRouteTable 获取当前 IP 的路由表, 去冗余后得到当前网络节点的连接关系表.
- 5) 如果连接关系表为空, 返回步骤 2), 否则跳到步骤 6).

6) 选择一个连接关系, 如果是邻居 IP 则加入路由设备集合, 继续选择下一个连接关系; 如果是直连子网则进行子网类型识别。

7) 读取 ipNetToMediaTable 获得子网活跃 IP 集合. 遍历活跃 IP 集合, 通过设备类型识别算法识别其中所有交换机并归入交换机集合。

8) 通过数据链路层网络拓扑发现算法^[9]完成子网内网络设备之间的连接关系发现。

9) 遍历交换机集合. 去除已经匹配的接口, 从 ARP 表中找到剩余接口连接的 MAC 地址对应的 IP 地址. 通过多 IP 设备识别算法确定剩余接口 IP 的连接关系. 结束后返回步骤 5)。

10) 结束。

SNMP-TEI 算法流程如图 4 所示。

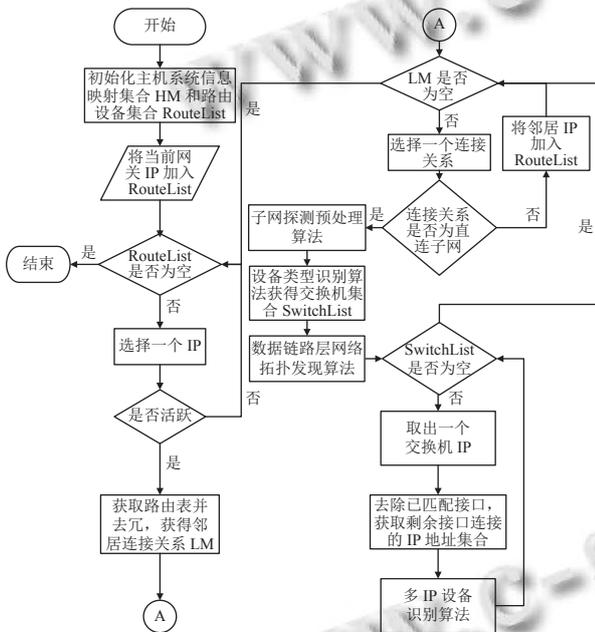


图 4 SNMP-TEI 算法流程图

对上述算法分析可知, 时间复杂度为 $O(nn_i mm_j^2)$, 主要集中在子网设备之间的连接关系判别, 其中 n 为路由设备个数, n_i 为路由设备邻居个数, m 为子网内交换机个数, m_j 为交换机接口个数. 子网类型识别算法时间复杂度为 $O(u)$, 主要集中在探针扫描, 其中 u 为探针注入数, 空间复杂度为 $O(1)$; 多 IP 识别算法由于采用哈希映射查找, 所以时间复杂度仅为 $O(1)$, 空间复杂度为 $O(h)$, h 为待测网络主机个数。

将本文算法与文献 [9,11,12,15] 算法进行比较, 具体结果如表 2 所示, 其中 τ 为网络总节点数、 e 为最大

邻居节点数. 网络拓扑发现算法力求在面对各种复杂的网络结构都尽最大可能地发现完整拓扑, 包括各种网络设备的发现及设备之间连接关系的发现. 文献 [11,12] 忽视了子网内设备之间连接的复杂性, 虽然算法复杂度低, 但是网络拓扑发现完整性较差; 文献 [9] 对网络场景分析贴近现实, 但仍然不足以解决存在链路子网和多 IP 设备的场景. 文献 [15] 主要依赖 LLDP 协议获取拓扑信息, 虽然准确性高、时间复杂度低, 但是可应用场景严重受限. 本文算法依据链路子网无其他活跃 IP 以及多 IP 设备指纹不变的网络特性构建网络拓扑发现算法, 能够有效应对该类场景, 从而达到提高拓扑发现准确率的目的, 且对网络协议依赖性低, 可拓展性更好。

表 2 各算法对比结果

| 算法 | 路由器发现 | 交换机发现 | 交换机连接发现 | 链路子网发现 | 多IP设备发现 | 算法复杂度 |
|----------|-------|-------|---------|--------|---------|------------------|
| 文献[9] | √ | √ | √ | × | × | $O(nn_i mm_j^2)$ |
| 文献[11] | √ | √ | × | × | × | $O(nn_i mm_j)$ |
| 文献[12] | √ | × | × | × | × | $O(n_i m)$ |
| 文献[15] | √ | √ | √ | × | √ | $O(\tau e)$ |
| SNMP-TEI | √ | √ | √ | √ | √ | $O(nn_i mm_j^2)$ |

3 实验分析

3.1 实验环境描述

基于本文提出 SNMP-TEI 算法, 使用华为网络仿真平台 eNSP 构建虚拟仿真网络对其进行验证. 仿真网络采用经典的 3 层架构, 如图 5 所示. 核心层部署 2 台三层交换机, 通过聚合两条链路相连; 汇聚层部署 4 台三层交换机, 为每个子网的网关, 并与 2 台核心交换机相连; 接入层部署 5 台二层交换机, 负责终端主机的网络接入. 此外部署边界路由器 1 台, 终端主机 11 台。

3.2 实验结果分析

根据文献 [12] 的思路, 我们使用 $\langle N_i, N_j \rangle$ 来表示节点 N_i 和节点 N_j 的连接关系. 首先准确率 φ 定义如下:

$$\varphi = \frac{l}{\tau} \quad (1)$$

其中, l 是拓扑结果中发现的正确节点连接数, τ 是待测网络中的节点连接总数。

其次拓扑结果上的错误率 θ 定义如下:

$$\theta = \frac{\varepsilon}{T} \quad (2)$$

其中, ε 是拓扑结果中发现的错误节点连接数, T 是拓

扑结果中的节点连接总数.

式 (1) 只考虑了正确连接, 当错误连接导致拓扑结果趋于完全图时, 式 (1) 不再能有效表示拓扑发现算法的准确性. 因此使用 $1-\theta$ 加权系数, 定义加权准确率 φ' 如下:

$$\varphi' = (1-\theta)\varphi \quad (3)$$

文献 [9,11,12,15] 算法和本文算法在仿真实验网络中探测 10 次, 探测结果如图 6 所示, 探测时间如图 7 所示, 子网扫描时间如图 8 所示, 探测源下行流量如图 9 所示, 探测源上行流量如图 10 所示. 拓扑结果图中的蓝色节点表示一个网络设备, 绿色节点表示一个链路子网, 节点上的 IP 地址表示节点的设备 ID.

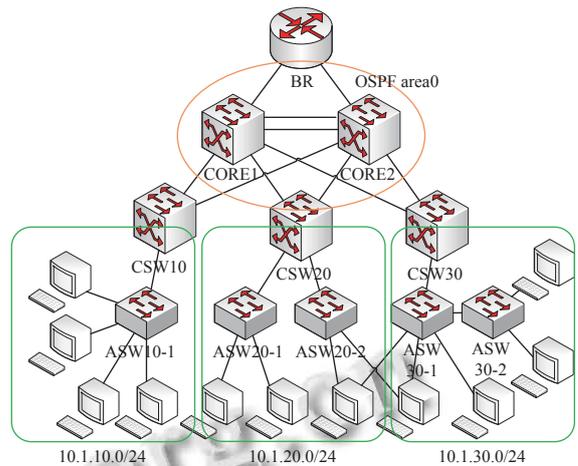


图 5 仿真实验网络拓扑图

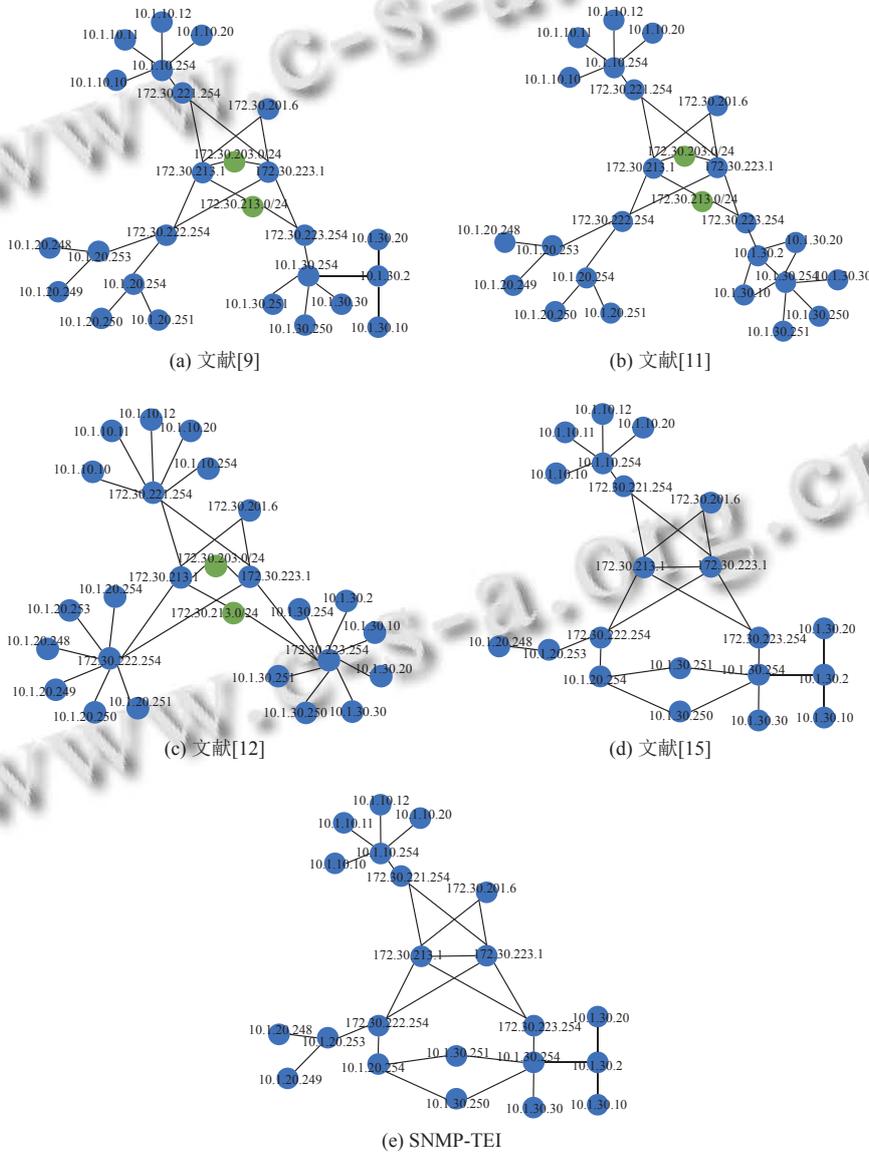


图 6 各算法拓扑结果

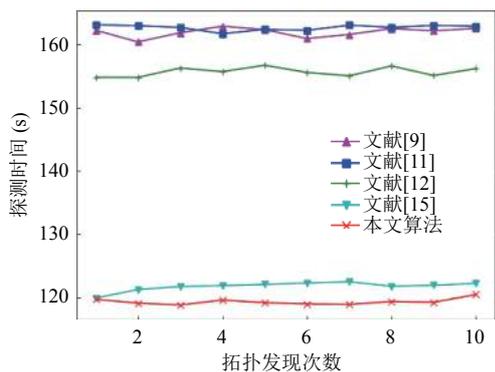


图7 探测时间

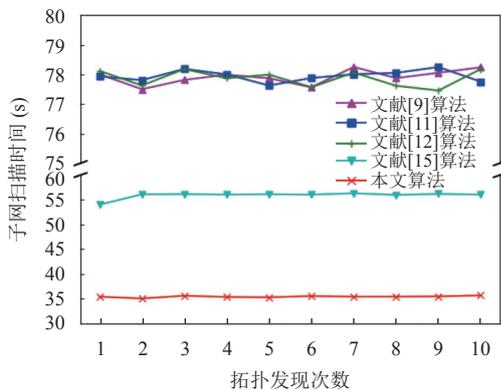


图8 子网扫描时间

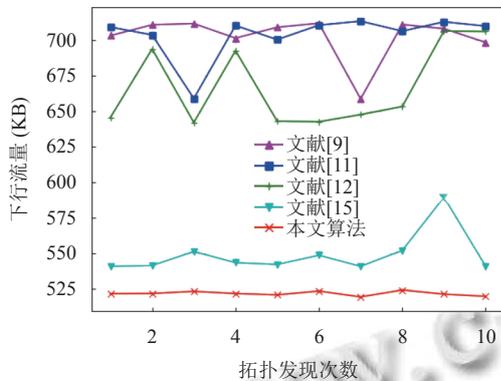


图9 探测源下行流量

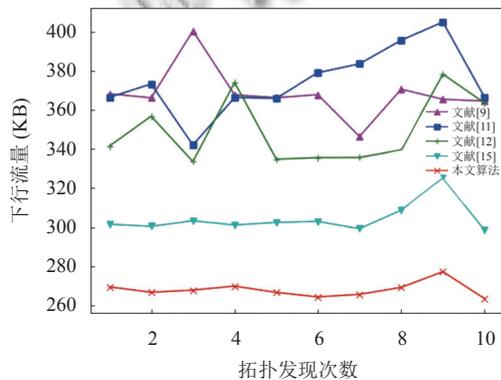


图10 探测源上行流量

在本次实验中,多 IP 主机 A 拥有两个 IP 地址: 10.1.20.250、10.1.30.250,多 IP 主机 B 拥有两个 IP 地址: 10.1.20.251、10.1.30.251;直连路由表条目中存在两个链路子网: 172.30.203/24 和 172.30.213/24. 根据图 6 和式 (1)–式 (3) 计算拓扑准确率如表 3 所示.

表 3 各算法拓扑准确率 (%)

| 算法 | 拓扑准确率 | 加权准确率 |
|----------|-------|-------|
| 文献[9] | 75 | 54.31 |
| 文献[11] | 71.43 | 46.81 |
| 文献[12] | 39.29 | 16.26 |
| 文献[15] | 92.86 | 92.86 |
| SNMP-TEI | 96.43 | 96.43 |

通过表 3 可知,因为文献 [9,11,12] 算法均未能识别链路子网和多 IP 主机,所以拓扑准确率较低.其中文献 [9] 发现的错误连接仅有链路子网和多 IP 主机,文献 [11] 只能发现简单子网内设备间的连接关系,且发现错误连接较多,因此两者拓扑准确率相近,但加权准确率相差较大;文献 [12] 不能发现子网内设备的连接关系,且发现错误连接多,因此拓扑准确率和加权准确率最低.文献 [15] 依靠 LLDP 协议获取网络邻居节点的方式,亦能解决多 IP 设备的识别这一问题,拓扑准确率较高,但是要求网络节点必须同时开启 SNMP 和 LLDP 服务,使得可拓展性较差.而 SNMP-TEI 算法仅利用 SNMP 协议完成链路子网和多 IP 设备的识别,使得发现完整性更高,仅有 1 条聚合链路未能发现.由图 7–图 10 可得,相比文献 [9,11,12] 算法,SNMP-TEI 算法通过基于 ICMP 的子网类型识别方法,减少链路子网的探针注入,使得探测源的平均上行流量减少约 95 980 B,平均下行流量减少约 169 497 B,平均扫描时间和平均探测时间缩减约 41 s.相比文献 [15] 平均上行流量减少约 36 305 B,平均下行流量减少约 27 426 B,平均扫描时间缩减约 2 s,平均探测时间缩减约 20.5 s.

通过上述的仿真实验结果,表明 SNMP-TEI 算法有效地解决了此前网络拓扑发现算法难以识别链路子网、无法识别多 IP 设备的不足,并且其高效性、准确性和可拓展性得到了验证.

4 结语

本文提出了 SNMP-TEI 算法,经过仿真实验检验,有效地识别了子网拓扑和准确地识别了多 IP 设备,拥有更好的可拓展性和更高的性能.虽然网络拓扑发现技术经过数十年的研究发展,国内外学者在如何提高拓扑发现的完整性和高效性的问题上提出了层出不穷

的方案,但是对于日渐重要的网络安全方面却关注甚少.例如安全研究人员关注的网络欺骗技术^[21]已广泛应用在各种网络中,网络拓扑发现如何在部署这些网络防御手段的网络中继续进行仍然是一个极具挑战性的工作.因此,今后的网络拓扑发现应当与网络安全紧密结合在一起,方能更好地适应将来计算机网络的发展.

参考文献

- Behara S, Sandeep N, Yaragatti UR. Design and implementation of transformer-based multilevel inverter topology with reduced components. *IEEE Transactions on Industry Applications*, 2018, 54(5): 4632–4639. [doi: [10.1109/TIA.2018.2836911](https://doi.org/10.1109/TIA.2018.2836911)]
- El-Moukaddem F, Torng E, Xing GL. Maximizing network topology lifetime using mobile node rotation. *IEEE Transactions on Parallel and Distributed Systems*, 2015, 26(7): 1958–1970. [doi: [10.1109/TPDS.2014.2329851](https://doi.org/10.1109/TPDS.2014.2329851)]
- Zhou YT, Deng ML, Ji FZ, *et al.* Discovery algorithm for network topology based on SNMP. *Proceedings of 2015 International Conference on Automation, Mechanical Control and Computational Engineering*. Atlantis Press, 2015. 1623–1628.
- Alderson D, Li L, Willinger W, *et al.* Understanding internet topology: Principles, models, and validation. *IEEE/ACM Transactions on Networking*, 2005, 13(6): 1205–1218. [doi: [10.1109/TNET.2005.861250](https://doi.org/10.1109/TNET.2005.861250)]
- Sanchez-Navarro I, Mamolar AS, Wang Q, *et al.* 5GTopoNet: Real-time topology discovery and management on 5G multi-tenant networks. *Future Generation Computer Systems*, 2021, 114: 435–447. [doi: [10.1016/j.future.2020.08.025](https://doi.org/10.1016/j.future.2020.08.025)]
- Ahn SJ, Yoo SK, Chung JW. Design and implementation of a web-based Internet performance management system using SNMP MIB-II. *International Journal of Network Management*, 1999, 9(5): 309–321. [doi: [10.1002/\(SICI\)1099-1190\(199909/10\)9:5<309::AID-NEM339>3.0.CO;2-8](https://doi.org/10.1002/(SICI)1099-1190(199909/10)9:5<309::AID-NEM339>3.0.CO;2-8)]
- Chen BR, Chen LM, Hong DK, *et al.* Research and application of automatic discovery technology of distribution data network topology based on unified MIB interface. *Proceedings of 2020 Asia Energy and Electrical Engineering Symposium (AEEES)*. Chengdu: IEEE, 2020. 565–571.
- Chang YC, Lin HT, Chu HM, *et al.* Efficient topology discovery for software-defined networks. *IEEE Transactions on Network and Service Management*, 2021, 18(2): 1375–1388. [doi: [10.1109/TNSM.2020.3047623](https://doi.org/10.1109/TNSM.2020.3047623)]
- Breitbart Y, Garofalakis M, Jai B, *et al.* Topology discovery in heterogeneous IP networks: The NetInventory system. *IEEE/ACM Transactions on Networking*, 2004, 12(3): 401–414. [doi: [10.1109/TNET.2004.828963](https://doi.org/10.1109/TNET.2004.828963)]
- Jiang J, Xu XL, Cao N. Research on improved physical topology discovery based on SNMP. *Proceedings of 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*. Guangzhou: IEEE, 2017. 219–222.
- Yin JB, Li YM, Wang Q, *et al.* SNMP-based network topology discovery algorithm and implementation. *Proceedings of 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery*. Chongqing: IEEE, 2012. 2241–2244.
- Zhou SP, Cui LG, Fang C, *et al.* Research on network topology discovery algorithm for Internet of Things based on multi-protocol. *Proceedings of 2018 10th International Conference on Modelling, Identification and Control (ICMIC)*. Guiyang: IEEE, 2018. 1–6.
- 潘爽, 苏亚维. 多协议融合的网络拓扑发现技术研究. *物联网技术*, 2021, 11(9): 14–17.
- Nakamura M, Hayashi N, Takada A, *et al.* Multiple-layer-topology discovery method using traffic information. *Proceedings of 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*. Tainan: IEEE, 2021. 160–165.
- 钟成龙. 国产大飞机机载网络拓扑发现研究与应用 [硕士学位论文]. 成都: 电子科技大学, 2022.
- Li J, Zhang XF, Shen WH, *et al.* Network topology discovery based on SNMP. *Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security*. Emeishan: IEEE, 2013. 194–199.
- Wang ZC, Yan Z, Zhang DD, *et al.* An algorithm and implementation of network topology discovery based on SNMP. *Proceedings of 2016 1st IEEE International Conference on Computer Communication and the Internet (ICCCI)*. Wuhan: IEEE, 2016. 283–286.
- Wang H. Improvement and implementation of wireless network topology system based on SNMP protocol for router equipment. *Computer Communications*, 2020, 151: 10–18. [doi: [10.1016/j.comcom.2019.12.038](https://doi.org/10.1016/j.comcom.2019.12.038)]
- Pandey S, Choi MJ, Won YJ, *et al.* SNMP-based enterprise IP network topology discovery. *International Journal of Network Management*, 2011, 21(3): 169–184. [doi: [10.1002/nem.756](https://doi.org/10.1002/nem.756)]
- 杨凯江, 马恩宁, 段晓雪, 等. 网络拓扑主动发现关键技术研究. *网络安全技术与应用*, 2021, (2): 107–109.
- 贾召鹏, 方滨兴, 刘潮歌, 等. 网络欺骗技术综述. *通信学报*, 2017, 38(12): 128–143.

(校对责编: 孙君艳)