网络层析成像研究综述*)

钱 峰 胡光岷

(电子科技大学宽带光纤传输与通信网技术教育部重点实验室 成都 610054)

摘 要 网络层析成像技术作为通信网络、层析成像技术和统计学理论相结合的产物,是一种全新的网络链路级参数推理、拓扑结构识别和OD(Origin-Destination)流估计的技术。在简要介绍网络层析成像的基本概念和数学模型的基础上,本文从网络链路级参数的推理、网络拓扑结构识别和OD流的估计3方面介绍了网络层析成像的研究现状,分析和展望了一些有价值的新发展,并指出了下一步的研究方向。

关键词 网络层析成像,网络链路级参数推理,拓扑结构识别,OD(Origin-Destination)流估计

A Survey of Network Tomography Technologies

QIAN Feng HU Guang-Min

(Key Laboratory of Broadband Optical Fiber Transmission and Communication Networks UESTC of China, Ministry of Education, Chengdu 610054)

Abstract As a result of combination of tomography technology, statistics theory and communication networking, network tomography is a novel technology about acquiring and processing information. In this paper, the cnception and mathematical model of network tomography network are briefly introduced. Next, the up-to-date research work on Link-Level Network Inference, topology identification and Origin-Destination Tomography are introduced and some efficient network tomography techniques are analyzed emphatically. Some valuable applications are explained and forecasted. Finally, the research direction in the network tomography in the future is proposed.

Keywords Network tomography, Link-level network inference, Topology identification, Origin-destination tomography

1 引言

层析成像(Tomography)技术也称计算机层析(断层)成像(Computerised Tomography)技术,简称CT技术,是上世纪70年代初首先在医学工程上得以成功应用并蓬勃发展起来的一项新技术。它的出现不仅促进了现代医学技术的发展,而且促进了计算机的应用,对电子学、数学、生物电子学及生物基础理论的研究和发展起了积极的推动作用。目前,CT技术在医学工程上已经形成一套完善的理论和方法,广泛应用于医学临床诊断和病理研究。与此同时,在医学工程上已成功应用的一些成熟的理论和方法还被应用于射电天文学、雷达探测、电子显微镜图形学、无损探伤、地震学、地质勘探等非医学领域[1~3]。

随着互联网的飞速发展,网络已成为人们生活不可缺少的一部分,同时网络的结构也在发生着根本的变化。为了成功地设计、控制和管理网络,就必须很好地了解和掌握网络的内部特性。目前,主要通过网络测量的方法来获取网络性能内部特性和识别网络拓扑结构[4]。网络测量的方法有不同的分类方法,按照测量过程中测量设备是否主动发送探测包可分为主动测量和被动测量两类;按照测量系统所处的位置,又可分为基于路由器的测量、端到端的测量以及路由器协助的测量。网络测量的内容很广泛,包括网络拓扑发现、时延、丢包率、带宽测量、网络距离测量、路由器调度策略和"瓶颈"缓冲器容量测量,以及路由器流量监测。

目前广泛使用路由器测量方法,也就是常说"内在"的方法,在网络节点或者网络节点之间直接、主动或者被动测量,它有许多潜在的限制:

①对一般用户是不可能得到的。

②可能不会覆盖到你所感兴趣的路径上。

③在网络高负载的情况下,不可能进行测量。

④存在大尺度网络上测量和测量数据收集的问题。

⑤每个测量点测得的数据组成一个端到端的路径数据信息是很困难的任务。

这就导致"外在"方法的引进。在假定没有节点的配合下,通过端到端的测量来诊断问题。已经有许多实际工具来测量端到端的性能,如Ping和traceroute等诊断工具广泛用来确定IP网络连通性、round-trip丢失、延迟。Pathchar和traceroute用来估计链路级的可用带宽、包延迟和丢失速率。但这些方法有几个潜在的缺陷:

①由于ICMP包在路由器里处理低优先级,因此测量得到的延迟不能代表正常流量的延迟。

②有些工具需要一些特殊的假设。比如路由节点不能存在防火墙、相对称的正向/反向链路、需要存储与转发路由器。

③ICMP包不能被网络管理员容忍,经常被ICMP包过滤器过滤掉,以致不能响应。

④需要得到路由器的协作。

随着网络朝着分布化、非协作、异质管理和基于边缘控制的方向演变,这些缺陷限制了这些工具的使用能力。

*)国家自然科学基金项目(No:60572092)、四川省青年科技基金和电子科技大学青年科技基金。钱 峰 博士生,研究方向为统计信号信号处理、计算机网络和网络层析成像。

为了弥补这些不足，国际上多个研究机构都在寻找其它途径来研究网络的整体性能及其相互影响，将已在医学、地震学、地质勘探等领域成功应用的成熟理论和方法应用于通信网络领域，衍生出了网络层析成像（Network Tomography）[5,6]。它是基于一种端到端的技术来获取网络中那些不能直接观察到的信息，它通过发送多种探测包（probe packet）给指定的接收器（服务器），观察并分析接受器所获得的信息；通过统计和推断来获得各种网络信息，包括链路级的参数和拓扑结构等信息。从反问题求解角度来看，网络层析成像进一步还可以包括网络 OD（Origin-Destination）流量强度估计，它实际是对网络链路级（Link-Level）参数推理的反过程，其目的就是从可测量得到的各链路级的测量数据中估计出路径级的网络参数。这两者求解都反映了网络层析成像反问题求解的本质，因此可以归纳到网络层析成像同一个主题下。

综上所述可知，网络层析成像技术在没有网络节点协作的条件下，通过主动发包探测方法或者被动收集网络内部有用信息的方法，网络层析成像技术通过统计学方法能够很好地推理出大尺度网络所有链路上的 QoS 参数，比如丢包速率和延迟分布等、识别网络拓扑结构和 OD（Origin-Destination）流的估计。

目前网络层析成像主要由两个部分组成：第一部分为测量数据的收集，其中主要研究如何收集网络内部的相关有用信息；第二部分为统计推理[7]，它主要是根据通过收集的数据来发现网络内部的信息和规律。根据数据收集的方法可以把网络层析成像分为：基于主动发探测包方法的主动网络层析成像技术（Active Network Tomography）和基于被动方法的被动网络层析成像技术（Passive Network Tomography）。

2 网络层析成像基础

大尺度网络推理的问题根据数据获取类型和感兴趣的性能参数来区分。为了区分这些问题，先定义链路与路径的基本概念。如图 1 所示，链路（Link）是指两个节点之间没有中间节点直接相联系，而且可以是单向或者双向的。路径（Path）是指两个节点之间相联系，中间有一个和多个链路，信息从源节点发送到目的节点沿着一条路径，该路径一般要经过好几个节点。Vardi[8] 是研究大尺度网络推理问题的第一人。由于网络推理与医学层析成像类似，因此把它称为“网络层析成像（network tomography）”。网络层析成像可以分为两类：①基于端到端的路径级网络流测量，得到链路级的参数估计[12~16,32~35]；②基于链路级网络流测量 OD 路径级网络流强度估计[8,26~28]。

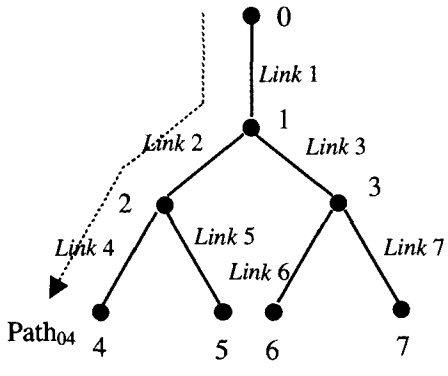


图 1 网络的逻辑拓扑结构

网络层析成像可以用线性模型来建模，该模型用下式表示：

$$y=A\theta+\varepsilon \tag{1}$$

式中：y 为可测量的向量，比如在网络不同测点测量到的发包数目、端到端的延迟。θ 为包参数向量，比如每条链路（Link）的平均延迟、包成功传输概率对数或者随机的 OD 流向量。A 为路由矩阵，ε 为可能是测量数据 y 产生的加性噪声，也可能是 θ 关于其均值的随机偏差。

(1)式的线性模型可以进一步表示为时变的形式：

$$y_t=A_t\theta_t+\varepsilon_t \tag{2}$$

式中：t 表示时间。这时估计的问题涉及到时变参数的追踪，实际上，(2)式表示的时变情节更能反映实际网络的动态本质。有几种方法用来追踪非平稳网络行为，包括经典的卡尔曼滤波器方法[9~11]。

式(1)、(2)估计问题是反问题的典型例子。在信号处理领域、统计学和应用数学的很多参考文献中，反问题求解主要依靠噪声 ε 的本质特征和 A 矩阵。由于它不能直接求解，因此一般需要用迭代算法来求解。一般来说 A 不是满秩，所以产生了方程的可辨识性问题：要么能解决参数线性联合的问题，要么能用统计方法引入正则性和促使可辨识性。在大多数网络层析成像问题中，噪声向量 ε 为逼近的独立高斯、泊松、二项式、多项式分布。当噪声向量 ε 为独立高斯分布时，递归线性最小二乘法能用于共轭、Gauss-Seidel 和其他迭代方程的求解。当噪声向量 ε 为泊松、二项式和多项式分布时，更多的统计方法比如说加权最小非线性二乘法、利用 EM 算法的极大似然法以及利用 MCMC 算法的 MAP 算法用来求解方程。

3 网络层析成像研究概况

3.1 网络链路级（Link-Level）参数推理

网络链路级参数推理是指：从可测量得到的路径级（Path-Level）数据中估计出网络链路级的参数，比如丢包速率、延迟分布等。网络中节点能够协作的话，网络链路级的参数能从直接的测量中估计出来。执行类似功能的工具有很多，如 pathchar(pchar)、traceroute、clink 和 pipechar 等，它们通过发送 ICMP 包来估计网络链路级的丢包、带宽。但是许多路由器不能产生或者响应 ICMP 包或者以非常低的优先级来处理 ICMP 包，因此需要发展出网络链路级参数推理方法，以达到不依赖节点的协作或者对节点协作最小化的要求。

当今的链路级网络层析成像研究主要集中在延迟分布、丢包速率和带宽的参数估计上，更一般的问题扩展到其他参数（比如可用带宽和服务原则）的重建。马萨诸塞州立大学的 MINC[12] 工程是多播网络层析成像方面研究的领先者，激活了当今这个领域研究工作的发展[12~16, 32~35, 36]。

在网络层析成像问题中有许多关键的假设，用于决定测量的框架和数学模型，这些假设为：①路由矩阵 A 假定为已知的，而且在整个测量时间内都是固定的。虽然网络路由矩阵是定时更新的，但是这些变化是以几分钟的间隔发生。当然，路由矩阵的动态特性限制了能收集和用作推理的数据的数量。②目前大多数方法通常都是假设每个链路上的性能特征是相互统计独立的，在许多例子中还假设是暂时平稳的。③在链路级的网络延迟层析成像，一般假定在源节点和目的节点可以获得同步时间。

网络通信有两种方式：单播与多播。在单播通信中，每个

包只向一个而且仅仅是一个目的节点。在多播通信中，源节点可以有效地把每个包向一组目的节点。在每个分叉点的路由器上，多播包被复制和延着分支路径传送出去。同样，链路级的网络层析成像可以分为多播网络层析成像和单播网络层析成像。

3.1.1 多播网络层析成像技术

基于多播探测的网络层析成像技术[13]是网络层析成像技术的第一种方法。假如一个多播探测包从源节点0发送到目的节点2，而不是被目的节点3接收，则马上能决定在链路3发生了丢包。通过进行这样的重复测量，能够估计链路2和3上的丢包速率。这些估计和测量能够用来计算链路1上的丢包速率。

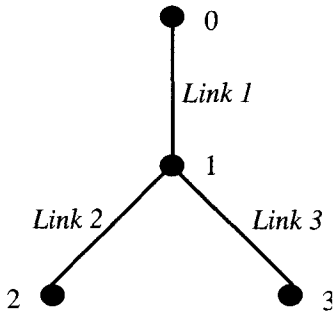


图2 网络的逻辑拓扑结构

为了举例说明，θ_1，θ_2，θ_3 表示网络中链路1、链路2、链路3的传输成功概率的对数。$\hat{p}_{2|3}$ 表示在节点2与节点3同时收到多播探测包数目与在节点3收到的多播探测包数目的比率。因此，$\hat{p}_{2|3}$ 是在链路3探测包成功的条件下，链路2的经验传输成功概率，它能为 θ_2 提供一个简单估计。以同样的方式定义 $\hat{p}_{3|2}$，$\hat{p}_i$，$i=2,3$，是节点 i 接收到的多播探测包的数目与发送到节点 i 多播探测包的数目的比值。

$$\begin{pmatrix}\log \hat{p}_2\\ \log \hat{p}_3\\ \log \hat{p}_{2|3}\\ \log \hat{p}_{3|2}\end{pmatrix}\approx\begin{pmatrix}1&1&0\\1&0&1\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}\theta_1\\ \theta_2\\ \theta_3\end{pmatrix} \tag{4}$$

$\{\theta_i\}$ 最小二乘算法估能够计很容易用来计算方程的超定系统[13,14,37,38]，从大尺度网络层析成像问题中衍生出更有效也更复杂的算法。

同样的方法能够用于处理网络层析成像的延迟分布。每条测量路径上都有延迟，最小延迟假设是已知的。从源节点0向目的节点2和3发送一个多播探测包和测得的各自延迟数据。从节点0到节点1之间的链路对目的节点2和目的节点3都是相同的。在这两个端到端，延迟测量的差别主要是由于节点1到2和节点1到3的链路差别。估计延迟分布的目的是估计出每条链路上的延迟分布。比如，假如得到目的节点2的延迟等同于已经知道的最小延迟，则节点3的额外延迟主要是从节点1到节点3的链路延迟。收集到节点2的端到端延迟的最小测量数据用来构建节点1到3的链路的延迟分布的直方图估计。在大的和一般的拓扑结构中，估计变得越来越复杂。已经发展出基于多播延迟网络层析成像的许多先进算法，它们用于抽象的二叉树估计[17,37]。

3.1.2 单播网络层析成像技术

单播测量比多播测量更困难，但许多网络不支持多播，基于单播的网络层析成像技术在很大程度上是基于实际应用考虑。基于单播的网络层析成像困难在于：虽然单播测量要求估计端到端路径的丢包和延迟分布，但不是路径级到相应链路上独一无二的映射。比如，假如探测包从节点0发送到节点2和3，n_k 和 m_k 分别代表目的节点 k 发送探测包的数目和接收到探测包的数目，$k=2,3$。

$$\begin{pmatrix}\log \hat{p}_2\\ \log \hat{p}_3\end{pmatrix}=\begin{pmatrix}1&1&0\\1&0&1\end{pmatrix}\begin{pmatrix}\theta_1\\ \theta_2\\ \theta_3\end{pmatrix} \tag{5}$$

式中：$\hat{p}_k=m_k/n_k$ 和 θ_j，$j=1,2,3$，表示每个链路传输成功的概率。很显然，由于A不是满秩，因此 $\{\theta_j\}$ 不存在独一无二的解。

为了克服单播丢包网络层析成像方程欠定的问题[14,18]，使用基于单播背靠背包对方法来克服这个问题。这些测量方法有机会收集更多统计信息，以帮助解决丢包速率和延迟分布。包对中的两个包，一个紧接着另一个发送。目的节点可能是不一样的，但它们经历的路径中有一部分链路是一样的。在队列服从标准尾部丢弃策略的网络中，假如两个背靠背包通过一个共同的链路，其中一个包成功通过这个链路，那么另一个包很有可能也能成功通过这个链路。尾部丢弃策略意味着一个包被丢弃仅仅当它刚到达队列和缓存器里面，没有足够的空间。在主动队列策略中，比如RED策略[39]，包能够以一定的概率丢弃，即使包已经进入了队列里面。每个包对的两个包经过相同的链路后，其延迟都是类似的。这些论都能够在实际网络中得到验证[16,40]。假如一个包传输成功，则另一个传输成功的概率也相当于一致的。这样的方法能够用于多播网络层析成像。

在带宽网络层析成像例子中[19]，通过单播包头域数据的灵活应用来解决解的非唯一性问题。每包头数据中的TTL字段反映了一个包存活时间。在每个路由器，当这TTL计数器减为0时，下一个路由器就放弃这个包。Nettimer使用"追尾"方法来收集测量数据：许多包对从源节点发出，每个包对可以有一个大的包紧跟着一个小的包。大的包的TTL字段在测量周期内是变化的，目的是大的包仅仅能够传播部分路径，使用小的包测量端到端的延迟主要包含大的包经历的传输延迟，以能够推理出大的包经历子路径的带宽。对图2网络拓扑结构，Nettimer可能从节点0沿着链路1和2发送包。假如大一点的包的TTL字段设定为1，则追尾那个更小的包，可测量链路1的传输延迟。

3.2 网络拓扑结构识别

在大多数网络层析成像问题中，都是在预先或者假定知道网络或者路由的拓扑结构条件下，处理网络性能参数的估计问题。网络拓扑结构由式(1)中的A来表示，因此已知A对大多数网络层析成像问题是非常重要的。然后，A并不是经常很容易知道的。现在有许多关于网络拓扑结构映射的工具，比如traceroute，但它主要依赖于网络路由器的合作，而且traceroute仅仅能揭示traceroute能准确发挥作用和希望知道那一部分网络的拓扑结构。随着网络规模的变大和网络私有权和隐私权关注的增加，这些合作的情况在实际中可能不会经常遇到。

在traceroute这种普通工具不能应用的情况下，有许多基于端到端的测量方法用来识别网络拓扑结构。这些测量方法是测量目的节点之间的相关程度[20~25]。这些方法大多数主要关注只有单个源节点和多个目的节点的树状拓扑结构的识别。它假设从源节点到接收节点的路由是固定的。由于是

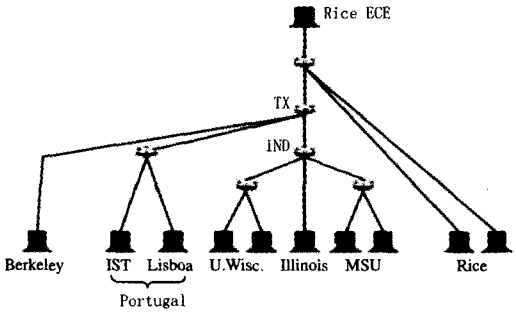
端到端的测量，因此仅仅只能识别到用不同目的节点的路径之间的分枝点所定义的逻辑拓扑结构。

现存大多数拓扑结构方法，关键是收集两目的节点的测量数据，找到一个能够随着两个目的节点之间经过共同链路或者队列数目增加而单调上升的函数。延迟协方差是一个简单的例子。假如两个目的节点一定比例的路径是相同的，那么到两个目的节点之间端到端延迟之间的协方差反映了共有链路值的和(假定在不是共同的链路上延迟是不相关的)。当到两个目的节点之间的路径共有的链路越多，则协方差的值就越大。

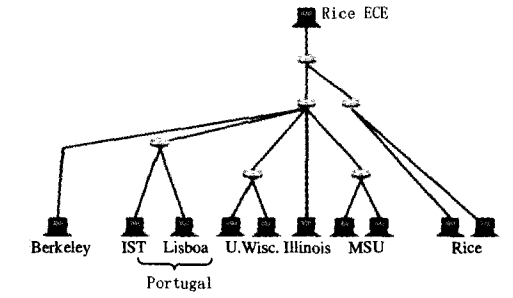
从估计不同的端到端测量数据中得到丢包数、延迟事件、延迟相关、延迟差异这些度量，可用来处理单调特征[20~25]。使用这些度量识别网络拓扑结构能够视为是如下最大似然估计问题。估计得到的度量 $X\equiv\{x_{i,j}\}$，其中 i,j 代表不同的目的节点对，能够被解释成真实的度量值 $Y\equiv\{y_{i,j}\}$ 被一些噪声和随机偏移所污染的值。估计得到的度量 x 根据密度函数 $P(x|\gamma,T)$ 的这样一个随机分布，它的精确形式主要依赖于污染的模型，它的参数为潜在的拓扑结构 T 和真的度量值。估计得到的度量 x 是一个固定的量，因此当 $p(x|\gamma,T)$ 被认为是 T 和 γ 的函数，$p(x|\gamma,T)$ 是 T 和 γ 的似然函数。由下式可以得到最大似然树：

$$T^{*}=\arg\max_{T\in F}\max_{\gamma\in G}p(x|y,T) \tag{6}$$

其中：F 表示连接源节点与目的节点之间的所有可能拓扑结构的集合。G 代表满足单一性特性的所有度量的集合。



(a) 用于网络实验的真实的网络拓扑结构



(b) 估计得到的网络拓扑结构

图 3 网络拓扑结构识别

似然最优化是非常艰难的[12]，我们不知道有任何方法能够求全局最大值，除了对所有可能拓扑结构集合进行 the brute force 检查。考虑 N 个目的节点的网络，可能拓扑结构集合 F 的集合个数最少有 $N!/2$。比如 N=10，有超过 1.8×10^{6} 种树结构。搜索空间的爆炸性增长排除了 the brute force 搜索算法，除非网络在逻辑上非常小。而决定全局优化树的在大多数例子中是被禁止的，因此基于确定性的次优化算法和蒙特卡洛优化算法能够提供拓扑结构的优良的估计。对基于确定性的次优化算法而言，确定性二叉树分类算法(DBT)[21]是一个代表性的例子。DBT 算法递归选择和归并/聚集过程，该过程产生一个从目的节点到源节点的二叉树。DBT 算法的贪心质能够导致一个非常次优化的结果。为了避免这些缺陷，MCMC 方法用来非常快地寻找“拓扑空间”，集中在最高可能性地区[24]。MCMC 方法最大有利的特征是从全局上识别拓扑结构而不是在某时刻次优化的小部分上识别。

为了举例说明网络拓扑结构的识别问题，考虑使用如图 3(a)所描述的网络拓扑结构。这个真实的拓扑结构是在莱斯大学的目的节点连接许多北美节点和一些欧洲的节点。在这个例子中，使用 traceroute 获得真实的网络拓扑结构。端到端的测量使用特殊目的的“sandwich”单播探测包获得一系列满足单一性特征的度[24]，“sandwich”探测包是基于延迟，但是只是基于两个节点之间的延迟差，所以不需要时间同步。图 3(b)描述了识别得到的网络拓扑结构。识别得到的拓扑结构一般与实际的拓扑结构相吻合。

3.3 网络 OD 流量强度估计

网络 OD(Origin-Destination)流量强度估计实际是网络链路级(Link-Level)参数推理的反过程，其目的就是从可测量得到的各链路级的测量数据中估计出路径级的网络参数。到目前为止，主要是从路由器接口上测量得到的链路流量数据估计出 OD 流量数据。在自己拥有的网络中，在网络内路由器上收集到的统计数据比直接测量所有 OD 对流量数据要简单得多。OD 流量矩阵反映了所有 OD 对之间的流量强度大小，它是任何路由算法的关键输入。由于 OSPF 路由协议的链路的权值就是相应路径上的流量数据，理想的情况是：一个数据驱动的 OD 矩阵应当是路由优化程序的中心。

当前获得 OD 网络流数据有两种方法：一是间接的方法，收集 OD 网络流数据[8,26~28]；二是直接用 NetFlow 等软件来收集 OD 网络流数据[27,29]。但是这两种方法都需要网络中路由器的协作，这对自己拥有的网络是没问题的。在路由器上用 NetFlow 收集链路流量数据相应地要比用直接方法收集 OD 网络流数据简单得多，因此收集到的链路流量数据可以通过线性的反问题来得到 OD 网络流数据的估计。这个反问题在详尽的细节上并没有显而易见的属性。首先，被估计的 OD 网络流向量不是一个固定参数的向量，而是一个用 x 表示的随机向量。其次，在线形性方程(1)中 ϵ 为 0。尽管 A 还是像其他已经被讨论过的例子里面那样单一，统计学方法[8,26~28]用来恢复完整的 x。而且最近大部分研究工作主要在处理数据的时变和非平稳方面。

Vardi[8]是第一个进行 OD 网络层析成像问题研究的人。他研究在一般拓扑结构的情况下，将独立同分布(i. i. d)泊松模型用于 OD 网络流字节数建模。他详细说明了泊松模型条件下的同一性情况和发展出了一种基于链路数据的 EM 算法，用于估计泊松模型的参数。为了减轻泊松模型条件下使用 EM 算法的困难，他使用一种矩方法来估计并简要地讨论了使用正态模型逼近泊松模型。相应工作用来处理链路数据简单集的特殊例子[28]也发展出一种 EM 算法。文[33]使用贝叶斯和 MCMC 估计方法。

Cao[27]等人使用实际采集的数据来修订泊松模型并用于解决 OD 网络层析成像的非平稳性问题。该方法与直接采集的 OD 流进行比较，发现是有效的。从一系列链路流数据中估计得到的时变或者非平稳的网络流矩阵，在只有 4 个 OD

对的子网中是有效的。根据与实际用 Cisco's NetFlow 工具采集的 OD 流数据相比，直接端到端的测量不是经常有效的，因为它们要求额外的 CPU 资源，它能够减低包处理的效率，并当网络很大的时候，会加重管理的负担。

$X=(x_1,x_2,\cdots x_n)^T$ 是不能直接测量的向量，代表网络中给定的时间间隔内所有 OD 对相应的字节数据。这里 T 为转置矩阵。X 虽然为了方便起见被设定为一个列向量，但实际上是"流量矩阵"。一个很自然的方法是列举所有 OD 值到一个向量，目的是能够列举所有的路由器，然后为了获得 OD 向量，我们把 OD 流表示成(1,1),(1,2),…,(1,I),(2,1),(2,2),…(2,I),(I,1),(I,2),…,(I,I),(i,j)代表从第 i 个端节点到第 j 个端节点。$Y=(y_1,y_2,\cdots,y_n)^T$ 是能直接测量到的向量，代表在一个给定的时间间隔内，在每个路由器链路接口上能够直接测量到的输入/输出字节。比如说，x 的成分相当于字节的树木从一个特定节点到另一个特定节点，而 Y 中的成分相当于从源节点发出的字节而不管它们的目的节点。因此 y 中的每个成分都是 x 选择了的参数之和。所以：

$$Y=AX$$

式中 A 为路由矩阵，由 0 和 1 组成的 $m\times n$ 矩阵，由网络中的路由表所决定。一般情况下，都考虑文[34]只有一个固定的路由表，也就是说从探测包的源节点到到目的节点仅仅只有一个固定路由表。不能直接测量的 OD 字节流数据，可以用以下模型来表示：

$$x_i\sim N(\lambda_i,\phi\lambda_i^c) \tag{7}$$

其中都服从正态分布，而且统计独立。其中 c 为一固定的能量常数。

$$Y\sim N(A\lambda,A\Sigma A^T) \tag{8}$$

式中

$$\lambda=(\lambda_1,\cdots,\lambda_n)^T$$

$$\Sigma=\phi diag(\lambda_1^c,\cdots,\lambda_n^c)$$

这里 $\lambda>0$ 是 OD 网络流平均速率的向量。$\phi>0$ 是一个尺度参数，它与平均速率的均值有关，因为更大的网络有更大的值。这均值的相互关系对模型参数可辨认性是很有必要的。在这限制条件下，直到 y 的期望决定尺度参数 ϕ，ys 协方差可以得到参数的可辨识性。

Cao 等人[27]使用一个局部似然模型来处理数据中的非平稳性。也就是说，对任何一个给定的时间 t，分析都是基于一个似然函数，该似然函数是从时间 t 对称的宽度为 $w=2h+1$ 的时间窗中衍生出来的。为了简化而不是为逼近窗内的平稳性考虑，假设在时间窗口内都是独立同分布的。通过联合使用 EM 算法和二阶全局优化估计方法的极大似然方法(MLE)来估计参数。成分方式的条件期望 OD 流、给定的链路流数据、待估计的参数、OD 网络流正值限制条件，都被用于 OD 网络流估计的初始化。对线性方程 $Y=AX$，通过迭代比例适合算法(the iterative proportional fitting algorithm)[30,31]的使用，可以获得 OD 网络流的最后估计。除了独立同分布模型中的正则化条件外，正值与线性条件限制对获得可靠的 OD 网络流估计是非常重要的。

为了平滑参数估计，文[27]把状态空间模型用于在时间窗口为 $w=2h+1$ 参数 λ'_s 和 ϕ 的对数的建模。$\theta_t=(\lambda_t,\phi_t)$ 是第 t 个时间窗的参数向量。我们假设参数的对数进化服从随机行走模型：

$$\log(\theta_t)=\log(\theta_{t-1})+V_t \tag{9}$$

式中：$V_t\sim N(0,D)$ 对不同的时间 t 是统计独立的。D 为用以前描述的 MLE 方法估计 θ_T 得到的对角矩阵。给定参数后，链路测量数据假定为独立同分布。

$$(\gamma_{t-h},\cdots,\gamma_t,\cdots,\gamma_{t+h})^T|\theta_t\sim\text{独立同分布 } N(A\lambda_t,A\sum_t,A^T)$$

时间 t 的推理可以用一系列的方法来获得。首先获得基于第 $t-1$ 个时窗的后验 PDF：$p(\theta_{t-1})$，然后用随机行走模型来更新先检验 PDF 函数 $\pi(\theta_t)$。通过使用第 t 个时间窗的观察和先验条件进行数值优化达到较晚估计 θ_t 最大化。

状态空间模型确实改进了参数估计，但是对 OD 流的 X_t 估计提高不大，因为它对 OD 流最后估计不是很敏感。参数估计的不敏感性与健壮性可能主要是由于在 MLE 方法中状态空间模型不能带来 OD 流估计的正值与线性的限制条件的改进。

4 网络层析成像技术的新发展

网络流的暂时平稳性、独立性以及网络传输模型具有很大的局限性，特别是在严重过载的网络中，由于网络层析成像的主要应用是检测严重过载的链路和子网。空间依赖性和暂时独立性已经出现在单播和多播网络层析成像中，然而需要有更具弹性、更容易处理的模型来对长时网络相关、动态随机路由和空间依赖性进行建模。由于无线链路和自主网变得越来越具有空间依赖性，路由的动态性变得越来越重要。

最近已经有一些初步的假设来处理网络时变和非平稳行为。除了时变 OD 网络流矩阵的估计，还有采用动态的系统方法去处理链路级的非平稳的网络层析成像问题。用连续的蒙特卡洛推理技术追踪非平稳网络的时变链路延迟分布。

由于主动发包探测技术的局限性，促使采用更多的被动网络检测技术，比如基于抽样的 TCP 网络流。然而，计算复杂度将会是一个很大的挑战。分散处理和数据融合技术可以在减少计算复杂度上发挥重要作用。

结论 本文主要介绍了网络层析成像技术作为通信网络、层析成像技术二项技术和统计学理论相结合的产物，它是一种全新的网络链路级参数推理、拓扑结构识别和 OD (Origin-Destination)流估计技术。在简要介绍网络层析成像的基本概念和数学模型的基础上，从网络链路级参数的推理、网络拓扑结构识别和 OD 流的估计 3 个方面介绍了网络层析成像的研究现状，分析和展望了一些有价值的新发展，并指出了下一步的研究方向。

参 考 文 献

1 黄志尧，金宁德，李海青. 层析成像技术在多相流检测中的应用. 化学反应工程与工艺，1996，12(4)：395～405

2 胥颐，刘福田，刘建华，等. 中国大陆西北造山带及其毗邻盆地的地震层析成像. 中国科学 D 辑，2000，30(2)：113～122

3 许有生，蒋伟荣，赵富金，等. 外伤性脾破裂的 CT 诊断(附 38 例分析). 临床放射学杂志，1998，17(3)：153～155

4 张宏莉，方滨兴，胡铭曾，等. Internet 测量与分析综述. 软件学报，14(1)：110～116

5 Claffy K, Monk TE, McRobb D. Internet tomography. Nature, 1999, January 7. http://www.nature.com/nature/webmatters/tomog/ tomog.html

6 Coates M, Hero A, Nowak R, et al. Internet tomography. IEEE SignalProcess Mag. 2002, 19(3): 47～65

7 Kay S M. 统计信号处理基础：估计与检测理论. 北京：电子工业出版社，2003

8 Vardi Y. Network tomography: Estimating ource-destination traffic intensitiesfrom link data. J Amer Stat Assoc., 1996, 91(433): 365～377

9 Coates M, Nowak R. Network tomography for internal delay estimation. In: Proc. IEEE Int. Conf. Acoust, Speech, and Signal

Proc. ,2001. 3409～3412
10 Cao J, Davis D, Wiel S V, et al. Time-varying network tomography: Router link data. J Amer Statist Assoc. ,2000,95:1063～1075
11 Coates M J, Nowak R D. Sequential Monte Carlo Inference of Internal Delays in Nonstationary Data Networks. IEEE Transactions on Signal Processing,2002,50(2):366～376
12 Multicast-based inference of network-internal characteristics (MINC). http://gaia. cs. umass. edu/minc
13 Cáceres R, Duffield N, Horowitz J, et al. Multicast-based inference of network-internal loss characteristics. IEEE Trans Inform Theory,1999,45:2462～2480
14 Coates M , Nowak R. Network loss inference using unicast end-to-end measurement. In : ITC Seminar on IP Traffic, Measurement and Modelling, Monterey, CA,2000, 28:1～9
15 Coates M ,Nowak R. Network tomography for internal delay estimation. In: Proc . IEEE Int Conf. Acoust. Speech and Signal Proc. , 2001. 3409～3412
16 Duffield N G,Presti F L,Paxson V,et al. Inferring link loss using striped unicast probes. In: Proc . IEEE INFOCOM 2001, Anchorage, Alaska,2001,(2) :915～923
17 Presti F L, Duffield N G, Horowitz J, et al. Multicast-based inference of network-internal delay distributions. Univ. Amherst, MA:[Tech Rep]. Massachusetts,1999. 99～55
18 Bestavros A,Harfoush K, Byers J. Robust identification of shared losses using end-to-end unicast probes. In :Proc . IEEE Int Conf. Network Protocols, Osaka, Japan, 2000. 22～33
19 Lai K, Baker M. Measuring link bandwidths using a deterministic model of packet delay. In: Proc. ACM SIGCOMM 2000, Stockholm, Sweden, Aug. 2000
20 Ratnasamy S, McCanne S. Inference of multicast routing trees and bottleneck bandwidths using end-to-end measurements. In: Proc. IEEE INFOCOM 1999, New York,1999(1):353～360
21 Duffield N G, Horowitz H, Presti F L,et al. Multicast topology inference from end-to-end measurements. In: ITC Seminar on IP Traffic, Measurement and Modelling, Monterey, CA, 2000,27:1～10
22 Duffield N G, Horowitz J, Lo Presti F, et al. Multicast topology inference from measured end-to-end loss. IEEE Trans Inform Theory,2002,48:26～45
23 Bestavros A, Byers J, Harfoush H. Inference and labeling of metric-induced network topologies: [Tech Rep]. Computer Boston, MA, BUCS-2001-010. Science Department, Boston Univ. June 2001
24 Castro R, Coates M J,Gadhiok M,et al. Maximum likelihood network topology identification from edge-based unicast measurements:[Tech Rep]. Houston, TX,Dept. Electrical and Computer Engineering, Rice Univ, TREE0107, Oct. 2001
25 Castro R,Coates M, Nowak R. Maximum likelihood identification of network topology from end-to-end measurement:[Tech Rep]. Rice Univ. TREE0109. Houston, TX,Feb. 2002
26 Tebaldi C , West M. Bayesian inference on network traffic using link count data (with discussion). J . Amer. Statist. Assoc. ,1998, 93(442): 557～576
27 Cao J, Davis D, Wiel S V, et al. Time-varying network tomography: Router link data. J. Amer. Statist. Assoc. , 2000, 95: 1063～1075
28 Vanderbei R J, Iannone J. An EM approach to OD matrix estimation:[Tech Rep]. Princeton, NJ. Princeton University . SOR 94-04, 1994
29 Feldmann A, Greenberg A, Lund C, et al. Deriving traffic demands for operational IP networks: Methodology and experience. In: Proc. ACM SIGCOMM 2000, Stockholm, Sweden, Aug. 2000. 257～270
30 Deming W E, Stephan F F. On a least squares adjustment of a sampled frequency table when the expected marginal totals are known. Ann. Math. Statist. ,1940,11: 427～444
31 Csiszáar I. Divergence geometry of probability distributions and minimization problems. Ann. Prob. ,1975,3(1): 146～158
32 Presti F L,Duffield N G,Horowitz J, et al. Multicast-based inference of network-internal delay distributions: [Tech Rep]. Amherst, MA,Univ. Massachusetts,1999. 99～55
33 Ratnasamy S, McCanne S. Inference of multicast routing trees and bottleneck bandwidths using end-to-end measurements. In: Proc. IEEE INFOCOM 1999, New York,1999, 1: 353～360
34 Shih M F, Hero A O. Unicast inference of network link delay distributions from edge measurements. In: Proc. IEEE Int Conf. Acoust. Speech and Signal Processing. Salt Lake City, UT, May. 2001. 3421～3424
35 Ziotopolous A G, Hero A O, Wasserman K. Estimation of network link loss rates via chaining in multicast trees. In: Proc. IEEE Int Conf Acoust. Speech and Signal Proc. Salt Lake City, UT, May 2001. 2517～2520
36 Coates M,Nowak R. Networks for networks: Internet analysis using Bayesian graphical models. In: Proc. 2000 IEEE Neural Network for Signal Processing Workshop, vol. 2. Sydney, Australia, Dec. 2000. 755～764
37 Duffield N, Presti F L. Multicast inference of packet delay variance at interior network links. In: Proc. IEEE INFOCOM 2000. vol 3. Tel Aviv, Israel, Mar. 2000. 1351～1360
38 Tsang Y, Coates M, Nowak R. Passive network tomography using EM algorithms. In: Proc. 2001 IEEE Int Conf. Acoust, Speech, and Signal Processing, vol. 3, May 2001. 1469～1472
39 Recommendations on queue management and congestion avoidance in the Internet. IETF Internet Request for Comments: RFC 2309, Apr. 1998
40 Paxson V. End-to-end Internet packet dynamics. IEEE/ACM Trans Networking,1999, 7:277～292

(上接第 7 页)

14 Ning Peng,Xu Dingbang . Learning Attack Strategies from Intrusion Alerts. In: Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03), Washington D. C. , October 2003. 200～209
15 Ning Peng,Xu Dingbang,Healey C G,et al. Building Attack Scenarios through Integration of Complementary Alert Correlation Methods. In : Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSS '04), February, 2004. 97～111
16 Ning Peng,Xu Dingbang. Hypothesizing and Reasoning about Attacks Missed by Intrusion Detection Systems. ACM Transactions on Information and System Security (TISSEC),2004,7(4):591～627
17 Morin B,Me L. M2D2: A formal data model for IDS alert correlation. In: Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection (RAID 2002),2002. 115～137
18 Michel C, Me L. Adele: an Attack Description Language for knowledge-based Intrusion Detection. In: Proc Of the 16th International Conference on Information Security,2001
19 Qin Xinzhou,Lee Wenke. Attack Plan Recognition and Prediction Using Causal Networks. In: Proceedings of The 20th Annual Computer Security Applications Conference (ACSAC 2004), Tucson, Arizona, December 2004
20 Zhai Yan,Ning Peng,Iyer P,et al. Reasoning about Complementary Intrusion Evidence. In: Proceedings of 20th Annual Computer Security Applications Conference, December 2004
21 Cabrera J B D, Gosar J,Lee Wenke ,et al. On the Statistical Distribution of Processing Times in Network Intrusion Detection. In: Proceedings of The 43rd IEEE Conference on Decision and Control (CDC 2004), Bahamas, Dec. 2004
22 Valdes A,Skinner K. Probabilistic alert correlation. In: Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection. 54～68