

# 针对网络编码的逆向工程技术合法性分析

杜行舟 徐 超 孟昭鹏

(天津大学国家示范性软件学院 天津 300072)

**摘 要** 网络编码是网络通信领域中的一项重大突破,它改变了传统网络的存储转发模式,将路由与编码的信息处理技术相结合,极大地提高了网络传输效率。在技术研究和应用实践的过程当中,随着网络逆向工程技术手段的介入,与之相关的技术合法性问题也再一次引起信息技术领域和法律领域的共同关注,尤其是“合理使用”原则的适用性颇具争议。网络编码的技术特征一定程度上可以反映对网络编码的逆向工程技术手段是否符合“合理使用”原则,进而触及针对网络编码的逆向工程技术合法性问题及相关可适用的原则。

**关键词** 网络编码,逆向工程,合理使用,知识产权保护

**中图分类号** TP393.0 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.11.003

## Legitimacy Analysis of Reverse Engineering Technique towards Network Coding

DU Xing-zhou XU Chao MENG Zhao-peng

(National Pilot School of Computer Software, Tianjin University, Tianjin 300072, China)

**Abstract** Network coding is a significant break-through in the field of network communications. It transforms the store-and-forward mode of traditional network and combines the information processing technologies of routing and coding, bringing in a great progress of network transmission efficiency. In the procedure of technology research and application, the intervene of network reverse engineering leads to a common attention and discussion of the intellectual property issue across the field of IT and law, especially for the topic of Fair Use. This article first studied the technical features of network coding, and then made an analysis of the legitimacy of network reverse engineering towards network coding upon the theory of Fair Use and network coding, coming up with proper principles.

**Keywords** Network coding, Reverse engineering, Fair use, Intellectual property protection

## 1 引言

网络编码理论最早由香港中文大学的 Rudolf Allseed 等人<sup>[1]</sup>在 2000 年 IEEE 信息论会刊上发表的一篇著名论文中提出。该文以蝴蝶网络模型为例,从理论上证明了在允许中继网络节点对所传输的数据进行线性或非线性的编码处理(如模 2 和、有限域上运算等)的情况下,多播网络总能够实现理论上的最大传输容量,即图论中的“最大流最小割”定理。网络编码的概念即为网络中继节点对所传输的数据进行操作和处理的过程<sup>[2]</sup>。在网络编码理论研究的不断深入的过程中,围绕网络编码安全性的问题也日益成为研究和关注的热点问题。蔡宁等人在 2002 年针对给出的搭线窃听网络模型从单信源有向无圈多播网络的安全问题入手,构造了信息论意义上的安全网络编码。在此基础上, Feldman 等人进一步证明了线性编码的安全性, Jain K 等人<sup>[3]</sup>得到了在单源网络中以单位速率安全单播的充要条件。

近年来,随着软件系统的规模和复杂度日益增长,软件的生命周期也在变长,维护和改造现有“遗产系统(Legacy System)”并从中提取业务需求、设计决策、规则流程以及经验数

据等分析与设计的成果对于软件开发和技术研究的助力不可小觑,尤其是对于软件技术移植以及兼容性软件开发都尤为重要。在这样的技术需求之下,逆向工程(Reverse Engineering)应运而生,成为了帮助开发者和研究者全面准确地理解软件系统的新方法和工具<sup>[4]</sup>。与此同时,与之相关的技术合法性问题也成为了跨领域的焦点话题。

本文主要从网络编码本身的特性出发,结合网络编码安全的相关理论以及相关法律研究成果,就逆向工程技术手段是否符合法律中“合理使用”原则的要求进行论述,并提出可适用的原则来解决对于网络编码逆向工程的研究活动在技术垄断和研究开放之间获得均衡这一问题。

## 2 网络编码及其逆向工程研究综述

网络编码理论的核心思想是基于中继节点的计算能力提升整个网络的数据传输能力,构造典型多播传输模型,将编码技术和路由功能相整合,旨在通过编码算法的不断优化使得多播网络传输总能达到理论最大容量。在针对网络编码的研究活动中,逆向工程技术手段可用于对网络拓扑结构、网络层协议、编解码算法及路由算法等客体的研究过程。

到稿日期:2013-06-25 返修日期:2013-08-16

杜行舟(1990-),硕士生,主要研究领域为复杂网络与智能交通系统, E-mail: xzdu@tju.edu.cn; 徐超(1982-),男,博士,讲师,主要研究领域为人工智能和模式识别; 孟昭鹏(1962-),男,博士,教授,博士生导师,主要研究领域为物联网软件与系统、智能交通系统与应用。

## 2.1 网络编码的概念

网络编码允许网络链路传输信道的中继节点对所传输的数据进行字节级的编码组合操作,用节点的计算成本换取网络传输效率的提升。

图1所示为简单“蝴蝶网络”模型中通过网络编码实现理论最大流多播传输的示例。设各网络链路容量为1,信源A和B通过网络将数据传输至信宿E和F,所传输数据为 $x_1$ 和 $x_2$ ,C、D为数据链路中继节点。图1(a)为传统路由网络方式传输,信源在向信宿通信的同时将数据 $x_1$ 、 $x_2$ 从A、B节点传输至C节点,由于链路容量所限,C节点1个单位时间只能将1个单位数据传输至D节点进而转发至E、F信宿节点,因此C、D节点链路不得不重复使用才能完成信息的完整传输,对于信宿E和F,在2个单位时间内均获得3个单位数据,平均速率为1.5单位数据/时间;图1(b)为应用网络编码方式传输,信源在向信宿通信的同时将数据传输至C节点,由C节点将两个信道上的数据 $x_1$ 、 $x_2$ 加以整合,将结果 $x_1+x_2$ 传输至D节点,进而转发至E、F信宿节点,信宿E获得数据 $x_1$ 与 $x_1+x_2$ ,信宿F获得数据 $x_2$ 与 $x_1+x_2$ ,通过进一步译码操作即可获得原始数据 $x_1$ 与 $x_2$ ,在该传输模式下,信宿E和F在1个单位时间内获得2个单位数据,平均速率升至2单位数据/时间,恰为依据图论中“最大流最小割”理论所求得解<sup>[5]</sup>。

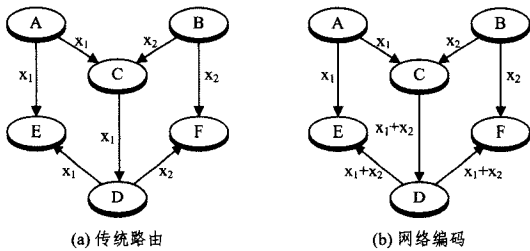


图1 蝴蝶网络<sup>[5]</sup>

从图1例子中可以进一步归纳网络编码理论的特征:信源节点入度为0(如A、B),信宿节点出度为0(如C、D);入度至少为2且出度大于0的节点可具备编码条件(如C节点);编码节点在对接收到的数据进行一定的处理之后继续传输,直到将经过处理后的所有信源数据都传输至信宿;信宿节点通过译码操作获得信源原始数据。

上文的分析展示了网络编码对提升多播网络数据吞吐量以及缩减数据传输周期起到的重要作用。在传输过程中可间接提升网络链路与节点连接成功率,提升网络健壮性,减小网络带宽开销与传输能耗。但是,新技术的诞生总是一把双刃剑,网络编码也存在诸多暂时难以量化的缺点,如网络编码对中继编码节点的运算能力有较高的要求,包括预处理信息的缓存以及I/O和CPU的消耗情况,中继编码节点编码和译码的时间是否会增加网络延迟、造成拥塞甚至影响系统实时性以及传输数据编码译码稳定性。上述问题在目前还难以考量。

## 2.2 网络编码技术构造逆向工程研究

逆向工程(Reverse Engineering),又称反向工程、反求工程,是20世纪80年代末发展起来并最初应用于制造业的先进技术。它以产品及设备的实物等资料为研究对象,逆向推导出其设计理念供研究或开发使用,有着广泛的应用领域和应用前景。其核心思想被学者定义为“对一个复杂的硬件系统实施有条理的检查,以开发出关于这个系统的一组规范说

明的过程”<sup>[6]</sup>。逆向工程在计算机软件领域的应用按照逆向工程研究对象可划分为软件逆向工程和网络系统的逆向工程等类型,主要的技术方法有词法语法分析、图形化方法、程序(数据流)切片和动态分析等。软件逆向工程和网络逆向工程在实际研究过程中具有协作性,但二者在研究来源、分析方式、描述表达、验证与假设等方面都具有不同的内容<sup>[7]</sup>。网络逆向工程更关注于网络节点的作用、网络链接与传输信道、网络拓扑结构设计及优化和网络带宽使用效率等要素。因此对于网络编码的研究常采用网络逆向工程方法进行。目前,实现网络逆向工程的主要技术手段有以下几类。

表1 网络逆向工程方法概述

逆向工程方法	核心思想	研究对象
基于数据流的网络通信协议解析	自动协议逆向工程,动态监控应用程序流程及算法 <sup>[8]</sup> ;动态二进制分析,记录污点数据地址依赖 <sup>[9]</sup>	数据编码协议;范式数据格式
基于网络跟踪的网络通信协议解析	跟踪网络数据报,总结并推理高频信息格式以评估协议 <sup>[10]</sup> ;建立网络协议状态机模型,获得高精度的网络数据及指令流的交互情况 <sup>[11]</sup>	应用层网络协议及其运作模式
网络通信协议的再工程	针对传感器网络协议的定制、检验、分析、修改提出的规范化流程推演 <sup>[12]</sup>	网络拓扑结构;底层网络协议模型

在网络通信技术的研究与开发中,使用逆向工程手段最主要的目的就是获得网络系统的物理组织结构(即网络拓扑结构等)以及逻辑组织结构(即网络通信协议、标准等),进而实现对网络系统的安全设计进一步深入、对网络运行状况进行模拟监控、对现有网络体系进行性能分析和优化以及对网络通信应用进行深度开发的最终目的。

## 3 网络逆向工程与“合理使用”原则

逆向工程作为一项实用技术,不仅极大地有助于技术研究,也是面向应用开发的重要手段。随着近年来知识产权相关法律对智力成果保护力度的加强,这种分析、研究、借鉴已有科技成果的技术手段屡有争议且日趋激烈。由于在实践中不可避免地造成原有成果技术细节的流露,因此如何将逆向工程这一新兴技术纳入法律意义上的“合理使用”原则轨道这一问题备受学界瞩目。

### 3.1 所涉智力成果及“合理使用”问题

综合以上对于网络编码特征及其安全的论述,网络编码系统理论中的智力成果如表2所列。

表2 网络编码系统相关智力成果

智力成果类别	智力成果具体内容
传统网络模式下的智力成果	网络拓扑结构;应用层、传输层、网络层、数据链路层、物理层网络协议;路由转发选路算法等
网络编码体系的构造算法	网络编码优化所涉及的最小花费组播算法、最大吞吐量算法、最小编码节点与编码边算法、编码网络拓扑结构组织算法等 <sup>[13]</sup>
网络编码及译码的实现算法	给予特定拓扑结构的编码解决方案;基于信息流分解及最小代价函数的编码解决方案;无线网络、传感器网络、P2P网络中的编码应用部署;基于复杂网络环境下的编码解决方案等
网络编码的安全算法	分层网络(物理层及应用层)防御算法 <sup>[14]</sup> ;数据加密签名算法;防窃听网络通讯模型;安全网络编码 <sup>[15]</sup> 等

对于逆向工程的“合理使用”问题,Pamela S等人在其《逆向工程的法律与经济》一文开篇指出,“逆向工程是一种从人

造物品中提取技巧和知识的过程,这种做法被接受和实践已经有很长时间。律师和经济学家认可逆向工程是获取这些信息的恰当手段,即使其意图是制造一种产品并从被反向工程的厂商手里夺取客户。既然有这一共识,过去几十年里逆向工程所遭受的非议是令人吃惊的”<sup>[16]</sup>,在这部被认为是逆向工程里程碑式的研究著作中,无疑表明逆向工程已被学术界默许。不过也有学者认为,在未经授权的情况下对于计算机软件作品进行逆向工程构成了对原作品知识产权的侵犯,如低成本的复制、分享,对原有技术细节的重新演绎而引起技术推广过程中潜在的不正当竞争等。

作为知识产权中的一种均衡型的保护机制,“合理使用”原则允许合法用户无须经授权即可善意、合理地在一程度和范围内使用知识产权人的智力成果<sup>[17]</sup>。在计算机软件知识产权保护体系中,“合理使用”原则的存在不仅一定程度上限制了专利权人的独占性权利,同时也对因著作权保护而形成的潜在技术垄断的风险进行了缓解。对于功能性作品而言,对其设计思想进行妥善折衷的保护有益于技术的进步和相关利益的良性配置与流转。因此,对于“合理使用”原则的解读也成了界定逆向工程行为合法性的关键因素。

### 3.2 相关技术手段合法性分析

基于上文对网络编码特征及其安全性问题、网络逆向工程技术目的和手段以及逆向工程在“合理使用”原则下合法性的论述,网络编码的逆向工程技术主要存在互联网络安全范畴的风险以及知识产权保护等法律范畴的风险。

#### 3.2.1 逆向工程技术的风险性分析

如图2所示,目前逆向工程研究主要针对遗产系统(Legacy System)进行。在数据流和网络跟踪方法的介入下,逆向工程对整个网络系统内部的组织结构、逻辑关系以及构造算法、业务流程进行全面的分析把握。文献<sup>[18]</sup>给出了以模型驱动(Model-driven)为指导思想,将遗产系统的数据流以数据点序列的方式进行形式化描述,以数据流时间为单位将其中的数据报元组化后进行分类,依据所属类别调用不同的处理函数,最终获得该系统的功能运行性能分析数据,并根据其进行重构调优。

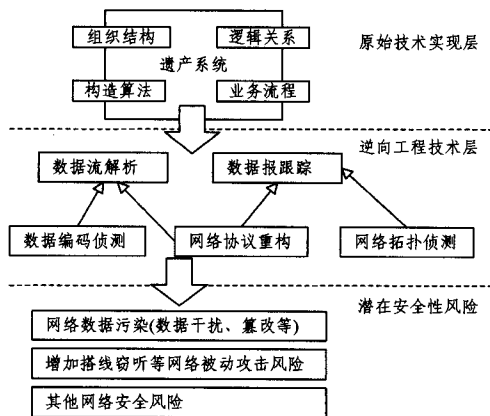


图2 网络逆向工程技术的风险性分析

在网络编码系统中,编码体系构造算法起着关键性的作用。通过逆向工程手段,整个编码网络的构造算法、数据传输信道中继节点的数据组合处理所采用的编码向量、甚至整个网络的逻辑拓扑组织结构均可直接接触,这增加了整个网络系统受到主动攻击的风险,干扰数据和篡改数据的流入将使得原始数据被污染并且难以恢复,整个网络趋于瘫痪,因信源

原始数据的丢失,其损失较传统网络传输模式下的主动攻击更为严重。而对于节点编码译码算法的纰漏,其不仅使主动攻击可以更具目的性和针对性,而且在网络系统受到被动攻击时,网络编码失去其自身优势,通过搭线窃听方式获得的信息更容易被破解。

因此,网络编码系统逆向工程技术应当在学术上保持开放包容的态度,以技术研究学习和设计思想改善为目的,同时应对逆向工程的目的进行严格的限制,否则即违背了“合理使用”原则中“善意”的要求。这一点也符合我国著作权立法中“因科学研究”的要求及《计算机软件保护条例》中“为学习和研究软件内含设计思想与原理”的相关规定。

#### 3.2.2 逆向工程技术的法律风险分析

前文已经论述了逆向工程技术对网络编码系统造成的安全性风险,在信息网络安全的相关立法中,网络传输的安全受法律保护,因此这种安全性风险一旦引起实际的损害或损害威胁,就需要承担相应的法律责任。

由知识产权保护引起的法律风险主要产生于网络编码逆向工程所获得的结果。参照欧美的对于“合理使用”的细节性限制的一些要求,该逆向工程研究过程应当在区分是否商业利益目的的情况下,遵从以下要件审查流程。

如图3所示,逆向工程技术法律风险审查主要分为普遍的通用审查标准及针对涉及商业利益条件下的商业审查标准。

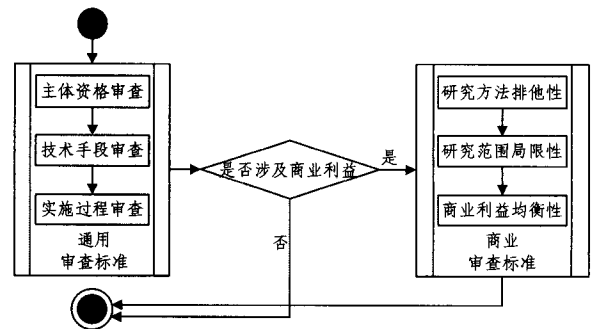


图3 逆向工程技术法律风险审查流程

在通用审查标准中,主体资格审查要求逆向工程技术实施主体需对所涉网络编码技术智力成果具备享有资格;技术手段审查要求逆向工程技术的实施不应有对原有成果造成损害、损害威胁或影响其正常运营,同时不得对原网络编码技术的应用实现进行篡改或注入;实施过程审查要求逆向工程技术在实施过程中不得造成原网络编码技术细节的大范围复制或公开,如原网络拓扑结构、编码加密算法的公开等。

当逆向工程技术手段涉及商业利益时,在上述审查的基础上还应符合商业审查标准的要求。在商业审查标准中,研究方法的排他性要求逆向工程技术当且仅当作为技术演进的唯一手段或最佳手段时方能采用,即无其他研究途径或该研究途径的综合成本消耗最低;研究范围局限性要求逆向工程技术只能对原网络编码技术域特定需求或关键技术进行,如仅对安全网络编码的加密算法进行研究;商业利益均衡性要求除非经逆向工程技术产生独创性智力成果,否则基于逆向工程技术所获得的应用实现不得与原网络编码技术的应用实现进行不正当竞争或技术授权转让。

在近几年的计算机软件研发过程中发现,“净室软件工程(Cleanroom software engineering)<sup>[19]</sup>”方法能够将分析设计

工作与开发活动相独立,因而可以使负责开发过程的人员对逆向工程的原始对象毫不知情,在实践中很好地规避了这一法律风险。

### 3.3 网络编码逆向工程的合法性原则

综上对网络编码逆向工程技术安全性风险和法律风险的论述,可以对网络编码逆向工程技术的合法性原则做如下归纳:

1) 网络安全维护原则:网络编码逆向工程研究应当以充分维护网络系统安全为前提条件,在学术科研活动中以促进技术进步为善意目的,学术界也应对基于该目的之下的逆向工程研究行为持开放包容的态度;

2) 主体及过程审查原则:网络编码逆向工程研究的主体应当具有合法享有,并且在具体的技术方案实施过程中尊重原技术成果的完整性、一致性,不得对原有成果造成不必要的分享和扩散或损害及影响原有实现的稳定运行;

3) 面向商业目的的限制性原则:网络编码逆向工程研究若以商业利益为目的,还需符合方法排他性的要求,即逆向工程须作为唯一或最佳的研究方法而介入研究活动,在研究中要有针对性的研究所必需的需求功能范围内的部分;

4) 技术成果合理管制原则:应当对网络编码逆向工程研究所获得的成果进行合理的管制,以免对原技术成果所享有的知识产权造成侵害。

如图4所示,以3.2.1节中基于模型驱动的遗产系统网络逆向工程研究活动为例,以上述4个合法性原则进行约束。在研究活动的不同环节,上述原则贯穿始终。网络安全维护原则主要针对逆向工程技术层对网络数据流的解析和跟踪可能导致的潜在风险而进行约束;主体及过程审查原则植根于原遗产系统实现层的相关成果在研究活动中的封闭和稳定;商业目的限制原则及技术成果管制原则是在逆向工程研究成果产出和应用的过程中分别从商业利益和知识产权的角度对研究成果进行约束。整个研究活动最终得到网络编码安全、研究活动合理、利益分配均衡、知识产权受保护的技术研究成果。

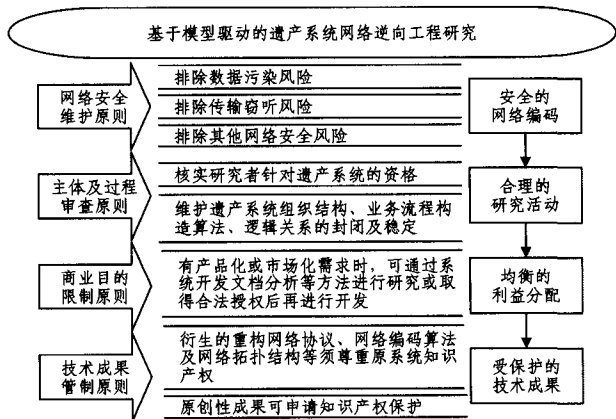


图4 网络编码逆向工程合法性原则应用分析

因此,在以上4项原则的规范之下,基于网络编码的逆向工程研究活动能够在保障技术安全稳定的同时促进技术发展,并保护相关智力成果知识产权的价值实现。

**结束语** 随着网络编码等新兴科学技术研究的进一步深入,运用知识产权等相关法律对研发活动智力成果保护的保驾护航作用也日益凸显。网络编码逆向工程作为网络编码技术研发的重要手段,不仅能够促进相关技术的进步,对于技术的产品化转型也有不可取代的作用。但是,逆向工程技术合

法性规范的缺失,使得逆向工程技术手段所获得的技术成果在法律界备受争议,因而产生的法律纠纷也不胜枚举。本文从维护网络安全以及“合理使用”法律思想的角度全面分析了网络编码逆向工程技术的合法性,并对其合法性审查原则做了详细的阐述,从技术合法性的角度提出4项网络编码逆向工程研究中的行为准则及规范——网络安全维护原则、主体及过程审查原则、面向商业目的的限制性原则以及技术成果合理管制原则,从而解决了网络编码逆向工程的研究活动在技术垄断和研究开放之间获得均衡这一问题。

### 参考文献

- [1] Ahlswede R, Cai Ning, Li Shuo-yen, et al. Network information flow[J]. IEEE Transactions on Information Theory, 2000, 46(4):1204-1216
- [2] 陶少国,黄佳庆,杨宗凯,等. 网络编码研究综述[J]. 小型微型计算机系统, 2008, 29(4):583-592
- [3] 张盛勇,陈世康. 网络编码的安全问题初探[J]. 通信技术, 2012, 45(1):105-107
- [4] Kienle H M, Müller H A. Rigi—An environment for software reverse engineering, exploration, visualization, and redocumentation[J]. Science of Computer Programming, 2010, 75(4):247-263
- [5] 熊志强,黄佳庆,刘威,等. 无线网络编码综述[J]. 计算机科学, 2007, 34(3):6-9
- [6] 严秀,李龙澍. 软件逆向工程技术研究[J]. 计算机技术与发展, 2009, 19(4):20-24
- [7] Zhou Hui, Du Wen-cai. How Network Reverse Engineering Differs from Software Reverse Engineering[J]. Wireless Communications and Applications, 2012, 72(1):33-43
- [8] Wondracek G, Comporetti M P, Kruegel C, et al. Automatic network protocol analysis[C]// Proceedings of the Network and Distributed System Security Symposium, 2008. San Diego, California, USA, 2008
- [9] 何永君,舒辉,熊小兵. 基于动态二进制分析的网络协议逆向解析[J]. 计算机工程, 2010, 36(9):268-270
- [10] Cui Wei-dong, Kannan J, Wang H J. Discoverer: automatic protocol reverse engineering from network traces[C]// SS'07 Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, 2007. CA, USA, 2007
- [11] Antunes J, Neves N, Verissimo P. Reverse Engineering of Protocols from Network Traces[C]// 2011 18th Working Conference on Reverse Engineering (WCRE). Limerick, Ireland; IEEE, 2011:169-178
- [12] 彭磊,袁海,曾家智. 无线传感器网络的协议再工程与方法研究[J]. 计算机集成制造系统, 2008, 14(6):1236-1243
- [13] 黄政,王新. 网络编码中的优化问题研究[J]. 软件学报, 2009, 20(5):1349-1361
- [14] 刘外喜,余顺争,蔡君. 安全的网络编码所面临的挑战和对策[J]. 计算机科学, 2011, 38(6):20-27
- [15] 曹张华,唐元生. 安全网络编码综述[J]. 计算机应用, 2010, 30(2):499-504
- [16] Pamela S, Suzanne S. Law and Economics of Reverse Engineering[J]. Yale Law Journal, 2002, 111(7):1575-1664
- [17] Madison M J. Some Optimism About Fair Use and Copyright Law[J]. Journal of the Copyright Society of the USA, 2010, 57(3):351-370
- [18] 张志斌,高峰,唐朝京. 净室软件工程中的关键技术研究[J]. 计算机应用研究, 2003, 20(2):17-20