摘要

网络编码是一种新颖的网络传输技术，它从网络总体或系统性的角度出发，能有效解决最大流量、路由策略等问题。网络编码可以利用其在网络节点上对所要求传送的消息作适当的线性或非线性处理来改善网络的传输效率、可靠性、鲁棒性、安全性、节点能耗等性能，是有别于传统方法的一种新的思路，因而受到高度重视，成为当前网络信息论中一个重要的研究方向。与多数技术一样，网络编码在充分利用网络理论组播速率的同时，也伴随着对应的开销。如何在应用网络编码技术充分利用网络传输能力的同时，尽可能地减少付出的各种开销，是网络编码在实际应用中所要解决的重要问题。

本文首先对网络编码进行了综述，介绍了它的理论背景、研究概况和发展趋势，重点讨论了当前它在无线网络中的一些应用及优势，并针对其中一种基于稀疏网络编码的 P2P 内容分发算法进行了详细研究和仿真验证。仿真实验表明，与一般网络编码相比，稀疏网络编码能够减小分发系统中编码分块的线性相关性，降低编码计算复杂度，并且解码成功率较高。与无编码的分发系统相比，基于稀疏网络编码的分发系统在吞吐量、平均下载时间和总分发时间等方面的性能都要优于前者。

虽然在多数需要承载广播业务的网络中，网络编码技术的引入可以提高和改善多项网络性能指标，但由于网络编码是在各个节点处对接收的信息进行组合后发送出去，因此数据包在传递的过程中很容易被篡改或遭受其他类型的攻击，信息的安全性遇到了严重的考验。为此，本文还重点研究了网络编码在安全性方面的应用，讨论了抵御不同安全攻击的网络编码方案，其中以窃听攻击为研究重点。同时，本文还针对网络的外部窃听攻击提出了一种改进的安全网络编码方案，从理论上证明了其安全性和可达性，并证明该方案的计算复杂度较已有方案更低。

最后，论文就今后工作的发展方向提出了一些个人的观点和看法。

关键词：网络编码，网络安全，安全网络编码，内容分发

Abstract

Network Coding is a brand new information transmission technology, which solves problems such as max flow and routing strategies in perspective of the whole network or system. Network coding allows the intermediate nodes to send out packets that are linear or non-linear combinations of its received information, and thus to improve the performance of transmission efficiency, reliability, robustness, security and energy efficiency. Currently, the research of network coding has received great interests and has become one of the most important fields in network information theory. However, like most other technologies, the advantage of network coding gets along with some overhead. How to reduce these overhead becomes a big challenge.

In this thesis, we first review the technology of network coding by introducing its theoretical background and current developments. Then, we focus on its applications and advantage in wireless networks. Addressing the problem of P2P content distribution, we carefully study a content distribution system based on sparse network coding, and carry out simulations to verify its performance compared to systems using general network coding and without network coding. Simulation results show that compared with general network coding, sparse network coding can reduce the linear dependence between coded blocks and the computational complexity of encoding operations, as well as ensuring a high successfully decoding rate. Simulation results also demonstrate that sparse network coding systems can achieve better performance than non-coding systems in terms of throughput, average downloading time and total distribution time.

Although network coding can bring performance gain for networks from several perspectives, it will also make the information exposed to different attacks during transmission due to its property of mixing data. Therefore, this thesis also focuses on security issues of network coding. We study network coding schemes used to counter different attacks, with emphasis on wiretapping problems. We then propose an improved network coding scheme against wiretapping attack based on existing works, and prove it to be secure and admissible with lower computational complexity compared to existing schemes.

Finally, some aspects needed to be studied for further research are pointed out.

Keywords: network coding, network security, secure network coding, content distribution

缩略词表
List of Abbreviations

NC	Network Coding	网络编码
RLNC	Random Linear Network Coding	随机线性网络编码
WMA	Wireless Multicast Advantage	无线组播特性
PNC	Practical Network Coding	实际网络编码
P2P	Peer-to-Peer	对等网络
SLNC	Sparse Linear Network Coding	稀疏线性网络编码
CSWN	Communication System on a Wiretap Network	窃听网络上的通信系统
WMN	Wireless Mesh Networks	无线网状网
WSN	Wireless Sensor Networks	无线传感器网络
LCM	Linear-code Multicast	线性码组播
IP	Internet Protocal	因特网协议
FEC	Forward Error Correction	前向纠错编码
MIMO	Multiple-Input Multiple-Output	多输入多输出
DAS	Distributed Antenna System	分布式天线系统
DOS	Denial of Service	拒绝服务攻击
PKI	Public Key Infrastructure	公钥基础设施
AES	Advanced Encryption Standard	高级加密标准

南京邮电大学学位论文原创性声明

本人声明所呈交的学位论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得南京邮电大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

研究生签名：张岩 日期：2009.4.13

南京邮电大学学位论文使用授权声明

南京邮电大学、中国科学技术信息研究所、国家图书馆有权保留本人所送交学位论文的复印件和电子文档，可以采用影印、缩印或其它复制手段保存论文。本文电子文档的内容和纸质论文的内容相一致。除在保密期内的保密论文外，允许论文被查阅和借阅，可以公布（包括刊登）论文的全部或部分内容。论文的公布（包括刊登）授权南京邮电大学研究生部办理。

研究生签名：张岩 导师签名：张俊所 日期：2009.4.13

第一章 绪论

网络编码（*Network Coding*）是一种融合了编码和路由的信息传输技术，在传统的存储—转发路由方式的基础上，通过允许对接收的多个数据包进行编码信息融合来增加单次传输的信息量，从而提高网络的整体性能。Ahlswede等人[1]于2000年提出了网络编码的概念，指出对组播网络中的某些节点附加额外的编码操作，能使源与组播成员间达到最大流最小割定理所定义的组播速率。

网络编码一经提出便引起了国际学术界的广泛关注，其理论和应用已成为通信领域研究的新热点。网络编码在提高网络吞吐量、改善负载均衡、减小传输延迟、节省节点能耗、增强网络鲁棒性等方面均显示出其优越性，可广泛应用于Adhoc网络[97]、传感器网络[94]、P2P 内容分发[82]、分布式文件存储[10]和网络安全[4]等领域。经过几年的发展，网络编码的理论研究已取得重要进展，而其在应用基础和工程实践方面的研究正在全方位展开。网络编码已成为一项融合信息论、代数学、图论、网络流理论和优化理论等多学科的交叉技术，且日益引起更多研究者的关注。可以说，网络编码对现有的网络体系结构、协议设计方法、信息交换方式和网络管理模式带来了革命性的变化。国外多所著名大学如麻省理工学院、多伦多大学、瑞士EPFL学院等和多家知名IT研究机构包括微软研究院、贝尔实验室等都在积极开展网络编码的理论和应用研究。而国内针对网络编码的研究尚处于起步阶段。

1.1 网络编码的概念

网络通信的目的是在源点和目的节点之间传递信息。因此，网络设计中最基本的问题就是怎样增加传输的信息量。计算机通信网络的飞速发展以及边缘学科的兴起，使人们的目光越来越多地投入到网络信息论上面。2000年，香港中文大学的R. W. Yeung和N. Cai等人首次将网络和编码进行结合，提出了网络编码的概念，其核心思想是在网络中参与传输的节点不单纯地执行存储-转发功能，而可对来自多条链路的数据信息进行一定的线性或非线性处理（即编码），然后发送出去，并保证接收节点可正确恢复出源节点所发送的信息，从而达到通信网络的最大容量，最大限度的利用网络的现有资源。

下面通过一个简单的例子对网络编码的基本思想进行解释，图1-1所示的通信网络是一个组播网络。图中箭头代表有向链路，假设每条链路容量为1bit/单位时间，信源节点s向接

收节点r1和r2同时发送两个比特信息a和b。图(a)中采用传统的多播技术，节点s分别向节点1和2发送a和b，节点1和节点2再分别将接收到的数据转发给其他节点。这样节点1可以直接获得a，节点2可以直接获得b。但是当a和b准备通过节点3进行转发时，由于节点3和节点4之间的链路容量为1，a或b必须在此排队等候一个单位时间。这样每个接收节点在单位时间内收到的比特数为1.5。图(b)则采用网络编码技术，中间节点3将两条输入链路上收到的信息a和b进行线性编码1，得到$a \oplus b$（异或加），然后送出。在接收节点r1处，根据接收到的a和$a \oplus b$，即可恢复出来b；同样，在接收节点r2处也可以恢复处a。由于解决了节点3处的传输瓶颈，每个接收节点在单位时间都可以收到2个比特，并达到了多播的最大流量。

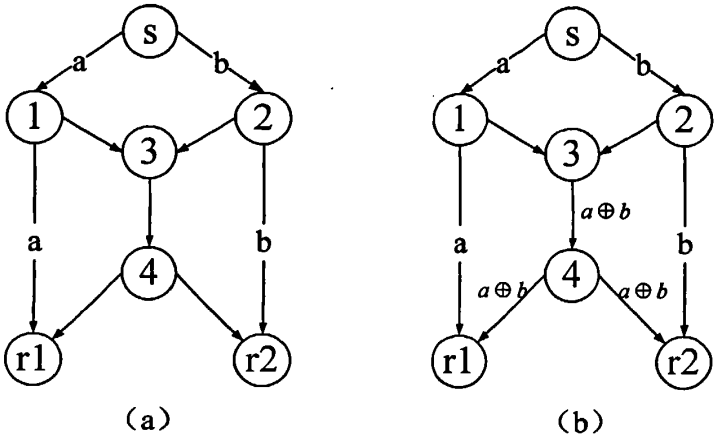


图 1-1 网络编码原理图

网络编码本质上是一种编码算法，支持者们声称它可以将现有的网络吞吐量提高许多，同时还能改善网络的可靠性和防范攻击的能力。网络编码技术最热心的支持者们说，该技术将会引发网络的下一代革命；其他人则认为，网络编码技术更有可能会潜移默化地改变目前基于路由的网络架构。

1.2 网络编码的研究现状

自从网络编码的思想提出以来，这个新兴的领域受到了众多研究学者的关注，下面简单介绍一下网络编码的发展概况。

首先按网络编码的构造方式分，主要又两种。一种是由 R. W. Yeung 和 N. Cai 提出的从向量空间构造网络编码的方式，而另一种则是由 R. Koetter 和 M. Medard 给出的代数构造方式。Yeung 和 Cai 等在文献[46]中提出了向量空间构造线性网络编码的方法，并指出线性编码是最简单的编码方法。他们将链路上输出的信息分组看成一定有限域下的向量，允许节点通过线性方式对信息进行编码处理然后再传输，并证明线性编码可以达到多播的最

大流。P. Sanders 等人提出了一种实现网络编码的多项式时间算法[13][57]，将[46]中提出的网络编码的构造进一步简化，不但把网络编码构造的复杂度从指数级降到了多项式级，而且大大降低了网络编码中所采用的字母表的下限。R. Koetter 和 M. Medard 提出的代数构造方式[47][48]，用一个系统转移矩阵来描述信源输入信息和信宿上接收到的信息之间的关系，并通过构造符合要求的系统转移矩阵来实现网络编码。这是一种指数时间算法，算法复杂度比较大。

上述方法都是基于已知整个网络的拓扑信息，几乎同时有人又提出了不需网络拓扑信息的分布式网络编码和随机网络编码。分布式网络编码[6]的实现是在网络中传输的每个数据包上留出一些比特用来记载此数据包在前面各个节点上所经历的操作，那么接收节点就可以从接收到的数据包中直接译出信源所发送的信息。这种方法可以在不知道网络拓扑信息的情况下实现网络编码，但是增加了网络负载。但是仿真表明，在这个信息组播的过程中，这种处理方式带来的负载代价并不大。另一种不需网络拓扑的方法是随机网络编码[3][60]，即在网络的中间节点上对接收到的信息在一个有限域内随机选择一个元素作为组合的系数。研究已经表明，只要有限域取得足够大，这种方法的失败率就可以很低。这种方法带来的缺点一个是以一定的概率实现正确无误的传输，另一个是需增大通信网络中所需字母表的大小。

文献[32]提出了基于网络编码的网络纠错码的概念。网络纠错码不同于传统的基于逐个链路的错误纠正的经典纠错码，它是采用分布式的方式来对整个网络中的差错进行纠正。只要链路上发生传输错误的符号数不超过纠错范围，不用经过重传，接收节点通过一定的译码就可恢复信息。文献[111][112]将网络编码与卷积码相结合，探讨了单位延迟网络模型下的网络编码问题；文献[113]分析了简单的具有两接收端的多元网络编码；文献[114]探讨了相关信源下的网络信息理论。文献[115]指出基于差错控制的网络编码和传统差错控制码的设计有很强的联系，这为基于差错控制的网络编码设计提供了方向。

Popovski等人[105]研究了现有各类物理层编码方案在两路中继信道下如何最大化通信速率的问题，并给出了各方案中对系统性能影响最大的关键要素。文献[106]对基于网络编码的协作通信进行了系统的理论分析，相对于传统的协作方案，基于网络编码的方案在同等的频谱效率下可达到更高的分集增益。

在提高无线网络的吞吐量方面，Leong[100]等提出了一种随机网络编码算法，并将该算法与基于在线Steiner树生成算法、Dijkstra最短路径算法和最近节点优先算法的路由算法进行比较。结果表明，分布式随机网络编码方法在组播吞吐量和鲁棒性方面要明显优于基于路由的算法。为了提高能量的利用效率，MIT的Petrovic等人提出了一种结合网络编码的、

对无线信号不进行调制的策略[101]。该策略由于节省了模拟器件进行调制所消耗的能量，降低了节点成本，因此可以节省大量能量。

Katti 等人[99]针对无线网状网（*Wireless Mesh Networks*）提出了基于机会的网络编码协议COPE，并在20个节点的网络测试床上完成了协议实现。这是网络编码首次在无线环境中的协议层面上的具体实现。文献[16]对基于COPE的无线网络进行了更深入的理论分析，并给出了相应的性能改进。其他涉及节能和跨层设计的研究可参阅文献[75] [107]。

文献[102]针对无线传感器网络提出了一种结合分布式源编码和网络编码的优化算法，目的是用来提高传感器网络的容错性和可靠性，同时对分布式源编码的压缩效率和网络鲁棒性进行了折衷考虑。Dimakis等提出了一种传感器网络中基于网络编码的数据聚合算法[88]，使得数据聚合的效率得到极大的提高。

基于网络编码的P2P内容分发协议一直是网络编码的研究热点之一，它在节省带宽资源、提高系统的抗毁性和可扩展性等方面都比无编码协议优势明显，但也面临着解码计算复杂、延时过大导致系统性能下降的新问题。文献[82]指出，在P2P系统中采用随机线性码，仅在编码块数目较少且块大小合适的情形下，其性能才可接受。 Ma等人[84]实现了一个基于稀疏线性编码策略的P2P内容分发系统，通过邻居选取、环路检测和编码区间划分3种策略，降低了各编码块间的线性相关性，提升了系统的整体性能。文献[109]提出了一种基于网络编码的P2P流媒体直播方案。仿真实验表明，采用网络编码后，节点的播放质量得到了普遍增强。LAVA[110]是首个集成网络编码技术的P2P流媒体协议实际系统。通过与已实现的标准流媒体协议Vanilla比较，网络编码协议在可用上传带宽略大于流媒体所需带宽时优势较明显。

Acedanski等人[12]研究了在多个存储资源受限的节点间进行分布式文件存储的问题，比较了无编码存储、基于纠删码存储和采用随机线性码存储3种策略。仿真结果表明，基于随机线性码的分布式存储策略在无需全局文件服务器的参与时，其性能接近集中式全局调度算法。文献[93]关注基于纠删码的文件存储在保持冗余度不变时，如何最小化网络带宽的问题。

网络编码在通信网络安全性方面的应用是网络编码研究中逐渐兴起的一个领域，也是本文的研究重点。2002年，Yeung和Cai就网络窃听问题首先进行了研究[18]，设计了一种安全的网络编码，在通信链路已经被窃听的情况下，在信源处将原始数据和随机信息结合起来进行网络编码设计。该文献从理论上证明了此方案使得只有接收方才能正确解码，窃听者得到的信息包和原始数据包之间没有任何相关性，互信息为零（就信息论而言，是安全的）。Feldman等人则在[18]的基础上，改进了构造方法，并将其提出的定理细化，将组

播容量和构造线性码所需的字母表大小进行了折衷[19]。

K. Bhattad等人[23]针对无环网络的组播问题，提出了窃听者不能得到任何有意义信息的弱安全网络编码模型。他们通过理论证明，在该模型下，对于计算能力有限的窃听者来说，只要它们窃取的独立信源信息数小于组播容量，就可以用安全网络编码来进行保密通信，并且不会降低传输速率。同样是针对窃听攻击，K. Jain等在[103]中得到了单源网络中（可以有环）以单位速率安全单播的充要条件，利用哈希函数和网络编码相结合的方法，使得网络以更高的速率安全传输数据，而搭线窃听者得不到信源的任何有用信息。Chan等人在文献[104]中讨论了多源网络的安全通信问题。他们在一定窃听范围的限制下，利用随机网络编码的方法，给出了多源安全网络编码容量的内界、外界和线性规划界。这些界是Yeung得到的界的推广。

中继节点对编码数据的恶意修改可能会导致网络编码使用受限，甚至不可用，因此消除拜占庭攻击的影响一直是网络编码安全应用研究中备受关注的问题。文献[4]提出了一种用散列函数检测拜占庭敌手的方法，首先对原始数据进行简单多项式函数哈希变换，然后把得到的结果添加到每一个原始数据包内。接收节点经过比较解码后的数据和哈希值就可以判断数据包是否被修改过，可以防止拜占庭攻击。Jaggi等人[33][108]进一步给出了一种多项式复杂度的分布式算法，在纠正敌手错误的前提下，同时达到最优组播速率。该方法无需对编码节点添加新的功能，对无线和有线网络均适用。Krohn等人[36]提出了一种基于同态散列函数的方法，用于检测被修改的编码分组，但该方法需要将计算好的散列值预先通过其他通道分发给所有节点，因此该方法具有一定的局限性。文献[35]利用椭圆曲线算法给出了一种适用于网络编码的签名方案，除了可检测被修改的分组，还加入了对数据的身份认证功能。

Gkantsidis等人[37]研究的是使用了网络编码技术的P2P内容分发网络的安全问题。他们集中研究了如何抵抗针对系统熵或试图完全阻塞系统的安全攻击，提出了一种能够提高验证效率的方案。他们还提出一种基于安全随机校验和的、能够防止伪造警报造成的DoS攻击的有效机制。Oliveira等人[43]通过研究证明，利用网络编码的优势，可以为传感器网络设计出一种密钥分配方案，它只需要用到少量预先存储的密钥，但仍然可以确保以概率1建立共享密钥连接，并且移动节点并不知道所分配的密钥。

总而言之，现在关于网络编码的研究是百家争鸣，各种方法和应用层出不穷，但是没有一个统一的标准，而且多数是基于理论分析，试验仿真很少。到目前为止，网络编码应用到实际网络中去还比较少，所以关于网络编码的研究还有很多东西去做。

1.3 论文主要工作及章节安排

本文在对网络编码的基本理论进行深入学习和研究的基础上，着重讨论其在无线网络和网络安全中应用时的性能增益。首先，重点研究一种基于稀疏网络编码的 P2P 内容分发算法，并对其进行详细研究和仿真验证。仿真实验表明，与一般网络编码相比，稀疏网络编码能够减小分发系统中编码分块的线性相关性，降低编码计算复杂度，并且解码成功率较高。与无编码的分发系统相比，基于稀疏网络编码的分发系统在吞吐量、平均下载时间和总分发时间等方面的性能都要优于前者。此外，本文还将对网络编码的安全性进行重点研究，讨论抵御不同安全攻击的网络编码方案；同时针对网络的外部窃听攻击提出一种改进的安全网络编码方案，从理论上证明其安全性和可达性，且具有较低的计算复杂度。

本文共分六章，其余几章安排如下：

第二章对网络编码的基本理论进行讨论，先对网络编码的数学模型和原理进行研究；然后依次介绍线性网络编码、随机网络编码和实际网络编码的概念；最后总结网络编码的性能优点。

第三章首先介绍网络编码在无线网络中的一些典型应用；接着就P2P内容分发问题，着重研究一种基于稀疏网络编码的内容分发系统，并通过性能仿真，验证稀疏网络编码的优越性；最后，通过从安全性角度将网络编码方案分类以及将各种安全攻击归类，引出网络编码在安全性方面的研究。

第四章研究如何利用网络编码的特性来抵抗各种不同的安全攻击，其中重点研究抵抗窃听攻击的网络编码方案，并对方案性能进行了详细分析。

第五章针对窃听问题，在前人工作的基础上，提出一种改进的网络编码方案，并对其性能进行验证。

第六章总结全文的工作，并指出今后有待进一步深入研究的一些问题。

第二章 网络编码基础

本章首先从通信网络的角度出发，介绍了图论的相关知识，在此基础上引出了网络编码的基本原理及数学模型，并从信息论角度出发证明了其可以实现网络中的最大流，而这是传统路由方式无法达到的。接着，本章重点描述了网络编码最主要的实现方式—线性网络编码的原理以及两种从不同角度出发的构造方法，同时分析了线性网络编码的局限性。之后，本章研究了线性网络编码中最重要，也是最为实用的两种方案—随机网络编码和实际网络编码。最后，本章从增加网络容量以及节省网络带宽两个角度分析了网络编码技术的优点。

2.1 网络编码的数学模型

2.1.1 网络编码的预备知识—图论和网络流图

2.1.1.1 图论基础

一个图是由一些节点和连接两个节点之间的连线所组成，至于连线的长度及节点的位置是无关紧要的。

定义 2-1：一个图是一个三元组$\langle V(G),E(G),\Phi_c\rangle$，其中$V(G)$是一个非空的节点集合，$E(G)$是边集合，$\Phi_c$是从边集合$E(G)$到节点无序偶（有序偶）集合上的函数。

若把图中的边 e_l 看作总是与两个节点关联，那么一个图亦可简记为$G=\langle V,E\rangle$，即该图由端集$V=(v_1,v_2,...,v_n)$和边集$E=(e_1,e_2,...,e_m)$组成。边集 E 是端集 V 中二个元的关系 $R:V\times V\xrightarrow{R}E$。每一个$e_r\in E$所对应的 v_i和 v_j称为与 e_r有关联的端；存在 e_r的两个端称为邻接端。当 v_i对 v_j有某种关系等价于 v_j对 v_i有某种关系，就称该图为无向图；反之，则称为有向图。当集合 V和 E 都是有限集时，所构成的图称为有限图；否则就称为无限图。实际中所遇到的都是有限图。对端和边赋予某些数值的图称为有权图，端或边上所赋的值称为权值或权。

最直观地表达图的含义还是几何图形，因此有图、端（或顶点）、边等术语。端集V中的n个元素可用n个点来代表，而边集E中的m个元素就是m条连线。在无向图中，边是一

般的连线；而在有向图中，由于端间关系的不可逆性，可用带箭头的连线。

若图 A 的端集和边集分别为图 G 的端集和边集的子集，则图 A 是 G 的子图。若 $A \subset G$，但 $A \neq G$，则称 A 是 G 的真子图。

在有向图中，与某端 v_i 相关联的边数称为该端的次数，记为 $d(v_i)$。射入节点 v_i 的边数，称为该节点的入向次数，记为 $d^-(v_i)$；由节点 v_i 射出的边数称为该节点的出向次数，记为 $d^+(v_i)$。因此，节点 v_i 的次数就是其出向次数与入向次数之和，即 $d(v_i)=d^+(v_i)+d^-(v_i)$。

有限条边的一种串序排列称为边序列。若相邻两边有公共端，在边序列中，某一条边可以在序列中重复出现，一端也可以重复出现，如图2-1中的 $(e_1,e_3,e_5,e_4,e_3,e_6)$ 就是一个边序列。

链是没有重复边的边序列，也就是说在链中每条边只能出现一次。通常链是指开链，即起点和终点不是同一个端，如图2-1中的 (e_1,e_3,e_5,e_4,e_2) 是一条 v_1 到 v_3 的链，端 v_2 在序列中经过两次。

径是既无重复边、又无重复端的边序列。在径中，每条边和每个端只能出现一次，因此径又是无环的链，如图2-1中的 (e_1,e_3,e_5) 是 v_1 与 v_4 之间的一条径。

环是起点和终点为同一端的链，即闭链，当然闭径也是环，如图 2-1 中的 (e_1,e_3,e_4) 是一个环。

图内任何两个端之间至少有一条径，该图称为联结图；否则称为非联结图。

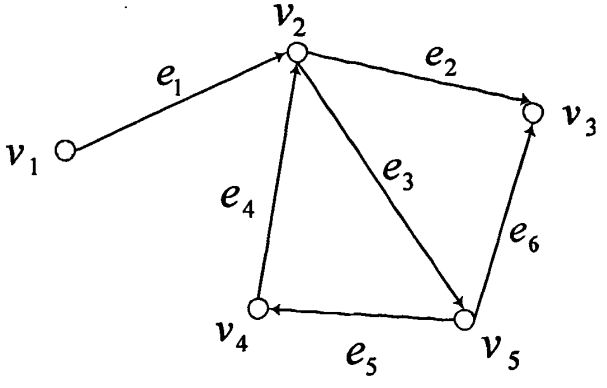


图 2-1 简单有向图

定义 2-2：若有向图$G=(V,E)$满足下列条件者，则称其为网络流图：

(1) 有且仅有一个顶点 Z，它的入向次数为零，这个顶点 Z 便称为源节点，或称为发点；

(2) 有且仅有一个顶点$\bar{Z}$，它的出向次数为零，这个顶点$\bar{Z}$便称为目的节点，或叫作收点；

(3) 每一条边都有一个与之相关的非负数，叫做该边的容量。边(v_i,v_j)的容量用 c_{ij} 表示。

例如图 2-2 就是一个网络流图。我们定义的网络常常称为运输网络。可用运输网络来表示的物理模型是多种多样的。网络的有向边可以用来表示城市之间的公路、电讯局之间的通信线路；边的容量则可以是允许通过的物资、速度，公路上的汽车数量或信号流量等等。

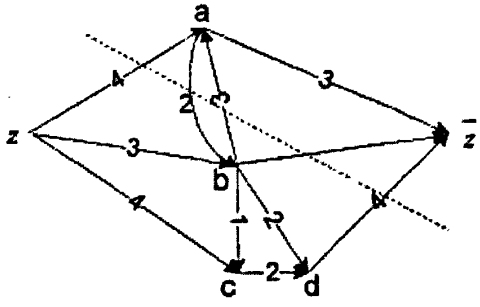


图 2-2 网络流图

定义 2-3：对于网络流图 G，每一条边(v_i,v_j)都给定一个非负数 f_{ij}，这一组数满足下列两条件时称为这网络的容许流，用f表示它。

(1) 每一条边(v_i,v_j)有 $f_{ij}\le c_{ij}$；

(2) 除了发点 Z 和收点$\bar{Z}$以外的所有的点v_i，恒有：

$$\sum_j f_{ij}=\sum_k f_{kl} \tag{2.1}$$

这个等式说明中间节点v_i的流量守恒，输入与输出的量相等。

(3) 对于源 Z 和目的节点$\bar{Z}$有：

$$\sum_i f_{Zi} = \sum_j f_{j\bar{Z}} = w \tag{2.2}$$

这个数 w 叫做这个网络流图的流量，而且从 Z 点发出的量等于流入目的节点 $\bar{Z}$ 的量。

定义 2-4：当 $f_{ij} = c_{ij}$ 时便称边 (v_i, v_j) 为饱和，表示流 f 对该边已饱和。所谓最大流问题是求使得从发点 Z 送往目的节点 $\bar{Z}$ 的流量 w 达到最大的流 f。

为了解决求运输网络的最大流问题，下面给出切割的概念。割是指图的某些子集，去掉这种子集就使图的部分数增加。根据这种子集的元素不同，可分为割端集和割边集：令 v 是图 G 的一个端，去掉 v 和与之相关联的边后，若使 G 的部分数增加，则称 v 是 G 的割端；去掉几个端后，部分数增加，则这些端的集称为割端集。在众多的割端集中，至少存在一个端数最小的最小割端集。

令S是联结图G的边子集，如果在G中去掉S能使G成为非联结图，则称S是G的割边集；若S的任何真子集都不是割边集，则S称为割集，即最小割边集。

定义2-5：$G=(V,E)$ 是已知的网络流图，假定S是V的一个子集，而且S满足下面两个条件：

(a) $Z \in S$，

(b) $\bar{Z} \notin S$。

令 $\bar{S} = V - S$，即 $\bar{S}$ 为S的补集。这样把顶点V便分成S和 $\bar{S}$ 两个部分，其中 $Z \in S$，$\bar{Z} \in \bar{S}$，对于一个端点在S而另一个端点在 $\bar{S}$ 的所有的边的集合叫做割切，用 $(S,\bar{S})$ 表示。

定义 2-6：在这集合 $(S,\bar{S})$ 中，把从 S 到 $\bar{S}$ 的边的容量的和叫做这个割切的容量，用 $C(S,\bar{S})$ 表示，即

$$C(S,\bar{S}) = \sum_{i\in S, j\in \bar{S}} c_{ij} \tag{2.3}$$

如图 2-2 中虚线表示一个割切，其中：

$$S = \{Z,b,c,d\},\ \bar{S} = \{a,\bar{Z}\},$$

$$C(S,\bar{S}) = c_{Za} + c_{ba} + c_{b\bar{Z}} + c_{dZ} = 4+3+2+4 = 13。 \tag{2.4}$$

显然不同的割切有不同的割切容量。

定理 2-1（最大流－最小割定理）[49]：对于已知的网络流，从发点 Z 到收点 $\bar{Z}$ 的流量

w 的最大值小于或等于任何一个割切的容量，即

$$\max w \le \min C(S,\bar{S}) \tag{2.5}$$

2.1.1.2 通信网络中的网络流图

前面介绍了图论中的一些基本概念，这一部分将上述概念应用到通信网络中的组播问题中去。并给出一个关于单源问题可达编码速率域的重要猜测[1]。假定考虑一个通信网络，用有向图 $G=(V,E)$ 来表示。设 $a:\{1,...,m\}\to V$ 和 $b:\{1,...,m\}\to 2^V$ 是两个任意的映射。信源 X_i 在节点 $a(i)$ 上产生，它将被组播到节点 j，对所有的 $j\in b(i)$。对于这里的单源问题，我们假定 $a(1)=s$，$b(1)=\{t_1,...,t_L\}$，也就是说，信源 X_i 由节点 s 产生，网络将其产生的信息组播到节点 $t_1,...,t_L$。我们称节点 s 为信源，节点 $t_1,...,t_L$ 为信宿。对于某个特定的值 L，我们称这种问题为单信源 L 信宿问题。

我们首先定义一些下面将会用到的符号：设图 $G=(V,E)$ 中的信源为 s，信宿为 $t_1,...,t_L$。边 $(i,j)\in E$ 上的容量为 $R_{i,j}$，且有 $\vec{R}=\left[R_{i,j},(i,j)\in E\right]$。从信源 s 到信宿 $t_l, l=1,...,L$ 的子图用 $G_l(V,E_l)$ 表示，其中

$$E_l=\{(i,j)\in E: \text{边}(i,j)\text{在信源}s\text{到信宿}t_l\text{的有向路径上}\} \tag{2.6}$$

$\vec{F}=\left[F_{i,j},(i,j)\in E\right]$ 是图 G 中从信源 s 到信宿 t_l 的流，如果下式对于所有的 $(i,j)\in E$ 都有

$$0\le F_{i,j}\le R_{i,j} \tag{2.7}$$

且对于除信源 s 和信宿 t_l 之外的所有其他节点 $i\in V$ 有

$$\sum_{i':(i',i)\in E} F_{i',i}=\sum_{j:(i,j)\in E} F_{i,j} \tag{2.8}$$

也就是流入节点 i 的总流量等于流出节点 i 的总流量。$F_{i,j}$ 是指向量 $\vec{F}$ 在边 (i,j) 上的取值。向量 $\vec{F}$ 的定义如下：

$$\sum_{j:(s,j)\in E} F_{s,j}-\sum_{i:(i,s)\in E} F_{i,s}=\sum_{i:(i,t_l)\in E} F_{i,t_l}-\sum_{j:(t_l,j)\in E} F_{t_l,j} \tag{2.9}$$

如果从信源 s 到信宿 t_l 的流量 F 的值大于等于任何其他从信源 s 到信宿 t_l 的流量值的话，我们就称 F 为图 G 中从信源 s 到信宿 t_l 的最大流。

根据图论中的最小割最大流定理，得到通信网络中的如下猜想[1]：

设在有向图$G=(V,E)$中存在信源 s 和信宿$t_1,...,t_L$，边(i,j)的容量可以表示为$R_{i,j}$。那么$(\vec{R},h,G)$是可达的，当且仅当从信源 s 到信宿$t_l,l=1,...,L$的最大流大于等于信源的输出信息速率 h。

2.1.2 网络编码原理

2.1.2.1 关于通信网络的基本假设

首先对通信网络进行如下理想化的假设：

(1) 有向图 G 中每条边的容量均为常数，如 1 比特/单位时间；若某条边其容量为 r(r为整数)，则用 r 条单位容量（1 比特/单位时间）的并行边来表示。这样即使边上的容量为分数时，也可以通过选择足够大的时间单位来精确的表示边容量。

(2) 每条链路有相同的时延。如果时延为零，则称该网络无时延；无时延网络只适用于非循环网络。此处假定网络中没有时延，没有环路存在。

(3) 假设网络中的链路均无差错传输。在网络的七层模型中，差错控制可以由底层完成，而提供给网络层的是一个没有差错的系统，而网络编码是在网络层的操作。

(4) 信源产生的随机过程是相互独立的，并且有相同的整数熵，如 1 比特/单位时间，且不同节点产生的随机过程也是彼此独立的。

一个通信网络可以用有向图$G=(V,E)$来表示，其中 V 代表节点集，$E\subseteq V\times V$ 代表边集。考虑组播情况，用$S\subset V$来表示通信网络中的信源，集合$T\subset V$表示目的节点的集合。网络中的节点可以分为源节点、中间节点、目的节点（有时一个节点会充当多种角色，比如说既是中间节点又是源节点）。我们用(v,v')来表示节点 v 到节点v'的边，即$(v,v')\in E$；边$e=(v,v')$的头为$v'=head(e)$，其尾为$v=tail(e)$。$\Gamma_I(v)=\{e\in E:head(e)=v\}$表示节点$v\in V$的输入边的集合；$\Gamma_O(v)=\{e\in E:tail(e)=v\}$表示节点$v\in V$的输出边的集合。

某个信源节点 v 产生的信息空间为$\Omega(v)=\{X(v,1),X(v,2),...,X(v,u(v))\}$，它是由 $u(v)$个离散独立的随机过程组成，其中每个离散随机过程均取自有限域F_{2^m}，所以节点 v 的熵为

$$H=\sum_{i=1}^{u(v)}H(X(V,i))=mu(v) \tag{2.10}$$

目的节点 v 所收到的信息空间 $\Psi(v)=\{Z(v,1),Z(v,2),...,Z(v,\eta(v))\}$，它是由 $\eta(v)$ 个离散随机过程组成。在一个通信网络中，可以用 $(v,v',\Omega(v,v'))$ 来表示节点 v 和节点 v' 之间的通信，它们之间所需传输的信息是 $\Omega(v,v')$。节点 v 可以通过从其出发的边 $e=(v,v')$ 来传输信息，用随机过程 $I(e)$ 来表示。边上所传输的随机过程的取值范围是有限域 F_{2^m}。

2.1.2.2 网络编码的数学描述

下面给出网络编码的抽象数学描述[50]。网络编码不同于传统路由之处就在于在各个中间节点上的信息处理方式，下面定义各边上的函数映射。对边集 E 中的每条边 $e=(v,v')$，存在一种映射：

$$f_e:\prod_{e\in\Gamma_I(v)}F_{2^m}\to F_{2^m} \tag{2.11}$$

这是对应于每条边的编码函数，它把某个节点所有输入边上的信息映射成其某个输出边上将传输的信息。目的节点 v 为了得到所需信息，对 $\forall Z(v,i)\in\Psi(v)$，$g_{v,i}:\prod_{e\in\Gamma_I(v)}F_{2^m}\to F_{2^m}$。映射 $g_{v,i}$ 是对应于目的节点 v 的第 i 个所需信息的译码函数，它从此目的节点输入边上所传输的信息中恢复出所需信息。如果存在编码函数 f_e 和译码函数 $g_{v,i}$，使 $\Omega(v,v')\subset\Psi(v)$，则称通信网络 $(v,v',\Omega(v,v'))$ 是可解的，同时称编码函数 f_e 和译码函数 $g_{v,i}$ 是此网络的一组解。

2.1.2.3 多源组播网络的转化

对于多源组播网络通过下面定理[51]进行转化。

定理 2-2[51]：任何多源组播网络的网络编码可以等效为单源组播网络加以研究。

其中，单源组播网络如图 2-3 所示，证明从略。

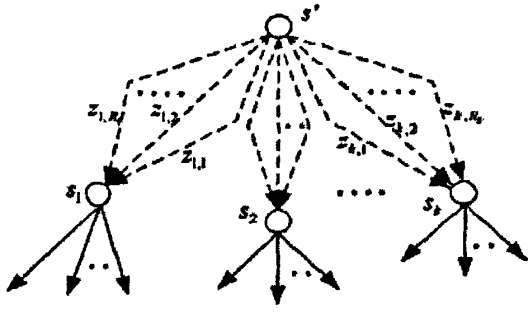


图 2-3 单源组播网络

从前面在对通信网络的流的介绍可以看出，对于网络中的中间节点来说网络的流量是守恒的，即非源节点的输出实物流的总量不能超过该节点的输入实物流 的总量。但是这

是适用于实际的商品流的特性，与商品流不同的是，信息可以进行复制和压缩。信息流也遵循一定的法则，虽然物质商品和信息本质上是不一样的，但是它们都遵循一定的流的法则的约束。对应于信息流有以下法则：流出非信源节点集的信息源于流入这些节点的信息的累积（信息流法则）。

总之，网络中的节点对信息的复制或是编码并没有增加信息的总量。信息流法则更加准确地反映了信息网络的实质，避免了在通信网络的研究中，信息"被当作货物一样进行运输"，使得通信网在本质上区别于交通网络、供应链网络等实物传输网络[52]。

2.1.2.4 网络编码可以实现网络最大流的可行性证明

在这一部分，给出一个重要结论：使用网络编码后，可以实现网络的最大容量。设有向图$G=(V,E)$中，信源为s，信宿为$t_1,...,t_L$，边$(i,j)\in E$上的容量为$R_{i,j}$。因为我们所关心的是信源到信宿的最大流，所以为了不失一般性，我们假定图中没有从其他节点流入信源s的边 ，也不存在$(i,i)\in E$。

考虑一个码长为n的分组码。X的取值x取自于均匀分布的集合Ω中，集合Ω中的元素称为信息。对于边$(i,j)\in E$，节点i发送给节点j的信息仅仅依赖于节点i之前所收到的信息。下面定义一类分组码：α-码。

图G上的一个$\{n,(\eta_{ij},(i,j)\in E),h\}$ α-码的定义包含下面5个要素：

(1) 一个正整数K;

(2) $u:\{1,...,K\}\to V$， $v:\{1,...,K\}\to V$，使得$(u(k),v(k))\in E$;

(3) $A_k=\{1,...,|A_k|\},(|A_k|\geq 1,\ 1\leq k\leq K)$，

使得$\prod_{k\in T_{ij}}|A_k|=\eta_{ij}$，其中$T_{ij}=\{1\leq k\leq K:(u(k),\ v(k))=(i,j)\}$;

(4) 如果$u(k)=s$，那么$f_k:\Omega\to A_k$，

否则：$f_k:\prod_{k'\in Q_k}A_{k'}\to A_k$，其中$\Omega=\{1,...,\lfloor 2^{nh}\rfloor\}$，$Q_k=\{1\leq k'<k:v(k')=u(k)\}$;

(5) $g_l:\prod_{k'\in W_l}A_{k'}\to\Omega,1\leq l\leq L$，其中$W_l=\{1\leq k\leq K:v(k)=t_l\}$，使得对于所有的$1\leq l\leq L$和所有的$x\in\Omega$，有$\bar{g}_l(x)=x$成立，且$x$为$\Omega$中的任意值。

根据上述描述，$\{n,(\eta_{ij},(i,j)\in E),h\}$ α-码的构造如下：在编码起始阶段，节点s获得信息源的一个值。在编码阶段，按照时间顺序依次进行K次处理，每次处理意味着一个节

点向另一个节点传输信息。在第 k 次处理中，节点$u(k)$根据函数f_k进行编码，得到A_k中的一个符号，并将其发送到节点$v(k)$。函数f_k所处理的符号域（定义域）是节点$u(k)$当前收到的所有信息：如果$u(k)=s$，则函数f_k的定义域为Ω；如果$u(k)\neq s$，则Q_k给出目前节点$u(k)$所接收到的信息，因此函数f_k的定义域为$\prod_{k'\in Q_k} A_{k'}$。集合T_{ij}给出了从节点i到节点j所传输信息的处理次数，所以η_{ij}代表编码过程中所有从节点i到节点j所传输的所有可能的符号集。最后，W_l给出了将信息发送到t_l上接收到的信息的处理次数。g_l是信宿节点t_l处的译码函数，它可无错的将x恢复出来。

定义 2-7：设边容量限为$\vec{R}=[R_{ij},(i,j)\in E]$的有向图$G=(V,E)$中，三维向量$(\vec{R},h,G)$如果满足下列条件，则称其为$\alpha-$可达的：

如果对于任意$\varepsilon>0$，存在一个足够大的n，使图G上的$\{n,(\eta_{ij},(i,j)\in E),h-\varepsilon\}$ $\alpha-$码对于所有的边$(i,j)\in E$均满足：

$$n^{-1}\log_2\eta_{ij}\le R_{ij}+\varepsilon \tag{2.12}$$

这里$n^{-1}\log_2\eta_{ij}$是编码后链路(i,j)上的平均比特速率。

定义 2-8：$R_{h,G}=\{\vec{R}:(\vec{R},h,G)$是$\alpha-$可达的$\}$。

定义 2-9：有向图$G=(V,E)$中，信源为s，信宿$t_1,...,t_L$，边(i,j)上的容量为R_{ij}，则

$$R^*_{h,G}=\{\vec{R}:s到t_l(l=1,...,L)的最大流\ge h\}。$$

定理 2-3[1]：$R_{h,G}=R^*_{h,G}$。

文献[1]给出了上述定理的详细证明，此处从略。通过有关熵的理论，该定理证明了通过网络编码，可以使网络的传输容量达到最大流最小割给出的理论限。

2.2 线性网络编码

网络编码方案可分为线性和非线性两种。所谓线性网络编码[46]也就是在实现网络编码过程中所用到的编码函数和译码函数均采用线性函数来实现。线性网络编码是中间节点将接收数据在某有限域内进行线性组合，节点接收足够数量的独立数据包就可以通过正确译码解得全部信息内容，能充分利用网络带宽。假设每个信息数据包为 L 比特，当它与要

组合的数据包长度不同时，较短的信息附加额外一串“0”，将包中的 s 个连续比特组成域上的一个符号，则一个包中包含 L/s 个符号。在线性编码下，运用乘法和加法运算，使从节点发送出去的数据为

该节点接收到信息的线性组合[56]。文献[13][46][48][53][54][55]等都讨论了线性网络编码的原理及实现问题。

2.2.1 线性网络编码的基本原理

下面介绍线性网络编码的基本原理，即如何进行编码和解码操作。

2.2.1.1 编码过程

假设一个源或多个源产生的原始数据包信息为 $M_1,...,M_n$，则在线性网络编码中传输的数据可表示为：

$$X=\sum_{i=1}^{n} g_i M_i \tag{2.13}$$

其中 $g_1,...,g_n$ 表示相应的编码系数，对每个符号有：

$$X^k=\sum_{i=1}^{n} g_i M_i^k \tag{2.14}$$

其中，M_i^k 和 X^k 分别表示 M_i 和 X 的第 k 个符号。

传输的数据包中既包括编码向量，又包括信息向量，编码向量用于接收端的解码。编码过程采用迭代的方法，若一个节点已经接收和存储的包信息集合为 $(g_1,X_1),...,(g_m,X_m)$，则该节点可以通过选定编码系数 $h_1,...,h_m$ 和运用算式（2.15）得到新的信息包 X'：

$$X'=\sum_{j=1}^{m} h_j X_j \tag{2.15}$$

编码向量 g' 可以通过，直接的代数计算得到，该过程可以在若干个节点中重复操作：

$$g^{i}{}'=\sum_{j=1}^{m} h_j g_j^i \tag{2.16}$$

2.2.1.2 解码过程

假设节点接收集合为 $(g_1,X_1),...,(g_m,X_m)$，为了恢复原始信息，需要求解（2-20）中的

m 个等式中的 n 个未知数 M_i，因此恢复所有数据要求 $m \geq n$，也就是说接收包的个数至少要为原信息的个数。而有些线性组合可能是线性相关的，所以 $m \geq n$ 并不是充分条件，但却是网络编码的重要条件。

$$X_j = \sum_{i=1}^{n} g_j^i M_i \tag{2.17}$$

解码需要求解一组线性方程。实际中，可以应用高斯消去的方法：节点存储编码向量以及编码之后的结果，以行向量的形式，存储在所谓解码矩阵中。最初解码矩阵中只包含未经该节点编码的包以及与之相对应的编码向量(如果有的话)，否则为空。当接收到一个已编码包后，会从中抽取它的编码向量以及编码结果，放入到解码矩阵中。解码矩阵会经过等价变换变成行阶梯型，最终变成行最简型。如果所收到的某一个包可以增加矩阵的秩，则称之为更新包；如果所收到的包是非更新的，它可以通过等价变换变为全零，从而可以忽略。当解码矩阵变换成最简型后，方程组得解。这种情况发生在当接收到 n 个线性独立的编码向量之后。

2.2.2 线性网络编码的实现方案

编码向量的选取可以采用确定性编码策略和随机编码策略。

确定性的方案是根据网络拓扑为节点选取确定的编码向量。Yeung 等人[46]提出了线性网络编码的向量实现方法：通过分析网络结构，根据节点的输入输出个数设计相应的局部编码向量，用迭代的方式得到全局编码向量，从而实现网络编码；Koetter 等人[47]则提出了较为完备的线性网络编码的代数实现方法，但他们的方法运算量太高。于是 Jaggi 等人[13][57]又提出了一种确定的多项式时间编码设计算法，可以为特定的广播网络找到可行的网络编码，目前已有对此算法的各种改进。

确定性的编码方案由于每个节点应用的都是固定的编码向量，因此网络中传递的数据中只需要包含信息向量，节省带宽，并且所需的符号域比较小；但确定性的网络编码需要了解全网的情况（拓扑结构等），复杂度比较高，难于分布式地实现。一旦网络拓扑结构发生了变化，就必须对整个编码方案进行修改，对无线环境变化的鲁棒性比较差。

由于确定性网络编码的以上缺点，Ho 和 Medard 等人[2][58]提出了随机网络编码的概念。随机网络编码是让网络中的节点以完全独立的分布式方式，随机选取编码系数，对输入信息编码，并把这组随机向量作为报头的一部分发送给收点，以便于解码。已经证明，

随机方式选取的编码向量成功的概率为$1-1/|F|$，其中 F 为编码的符号域。当符号域为无穷大时，采用随机编码，系统传输矩阵满秩的概率为“1”。

随机编码可以分布式地实现，并可增加保密性。文献[47]提出的代数实现框架指出，线性网络编码可以通过随机编码有效地构建。Chou[6]应用随机编码，提出了第一个实用的网络编码方案。为了保证随机编码成功概率，编码向量的符号域必须足够大，这可能会增加数据包头部的负担，因此符号域的大小必须仔细选择。

确定性编码和随机编码分别用于不同的网络应用与构架上，这些方案主要是基于理论上的分析和实现，因此在实际网络上需要针对不同的应用设计相应的编码方式：如对于结构较小的网络，可以选择比较简单的确定性算法，编码过程中甚至可以通过转换为对数，将乘法运算转换成加法运算，降低总的编码复杂度；而对于无线网络，则应用随机编码机制是主要的研究趋势，即令中间节点随机生成编码系数，对节点所有的可用信息应用线性编码，并随时更新编码系数。还有一种半随机的编码方案，整个网络被化分成若干区域，各区域都采用随机编码，但为了保证传输矩阵满秩，区域间要相互传递信息，以使每个区域在选择编码向量时尽量不选可能导致解码失败的那些向量。

2.2.2.1 从向量空间角度构造线性网络编码

继 R. Ahlswede 等人[1]指出网络的最大流可由网络编码实现以后，[46]首先给出了网络编码的具体实现方法，之后，[13][57]又从信息流的角度对以上方法进行了简化，把算法的时间复杂度从指数级降到了多项式时间级。

设 d 表示信源 S 和任一非信源节点 T 的最大流 $maxflow(T)$ 的最大值；Ω 表示一足够大基域 F 上的 d 维向量空间。这里采用的信息速率单位为每单位时间信道上可以传输一个基域上的符号。

定义 2-10[46]：通信网络(G, S)上的一个线性码组播(*Linear-code Multicast*，LCM)v 是对每一节点 X 分配一个向量空间 $v(X)$，每一信道 $(X,Y)\in E$ 分配一个全局编码向量 $v(X,Y)$，使得它们满足以下条件：

(1) $v(S)=\Omega$；

(2) 对每一信道 XY 有，$v(X,Y)\in v(X)$；

(3) 对于网络中的任何非信源节点集合 Φ，有

$$\langle\{v(T):T\in\wp\}\rangle=\langle\{v(XY):X\notin\wp,Y\in\wp\rangle \tag{2.18}$$

(4) 给节点 T 的输出边分配的编码向量是其输入边所分配的编码向量的线性组合。

符号$\langle\bullet\rangle$表示线性张成，LCM v刻画了一种信息数据在网络中传播的结构。开始将源节点 S 中要传输的信息分成 d 维的向量组，称作信息向量；在传输过程中，每条信道上承载的数据符号是信息向量和该信道所分配的编码向量的向量积。

图 2-4(b)就是一个线性编码组播的例子。在该例中，网络编码的的基域为F_2，每一条链路分配的编码列向量为：

$$\begin{cases} v(S,U)=v(U,T_1)=v(U,W)=\begin{pmatrix}1\\0\end{pmatrix} \\ v(S,V)=v(V,T_2)=v(V,W)=\begin{pmatrix}0\\1\end{pmatrix} \\ v(W,X)=v(X,T_1)=v(X,T_2)=\begin{pmatrix}1\\1\end{pmatrix} \end{cases} \tag{2.19}$$

信源 S 的信息向量为(a,b)，每一条链路上传输的信息符号为信息向量(a,b)和该链路编码列向量的向量积。对于一个线性网络编码组播，如果所有接收节点能够恢复出信源发送的信息向量，则称其为有效的线性编码组播。当网络中的任何 $m(1\le m\le d)$ 条链路 $X_1Y_1,X_2Y_2,...,X_mY_m$ 对应的编码向量线性无关时，就可以保证任何接收点能够恢复出信源的信息向量。当编码符号域足够大时，就可以保证这一点成立。

可以验证，上述线性码组播可以实现图 2-4(b)中网络的通信。但是对于任意复杂的通信网络，如何找到其所有的全局编码向量呢？P. Sanders 等人[13][57]针对组播网络给出了一种多项式时间算法，现把其主要思想介绍如下。

这种多项式时间算法是对从向量空间角度构造线性网络编码的方法进行的简化[46]。首先，对于任意给定的通信网络，我们利用最小割最大流算法确定网络中所能传输的最大信息量 h。如果这个通信网络是可解的，那么对每一个目的节点，我们都可以找到 h 条边不相互重合的路径，这 h 条路径组成了此目的节点的一个流。此网络的最大信息传输量是 h 个符号，所以我们沿着每个目的节点的流上的 h 条路径，在每条路径上分别传输一个符号，则可实现所要的通信。也就是说，对每个目的节点的 h 条路径，它们传输了目的节点所要的全部信息，所以这 h 条路径上的全局编码向量必须张成整个信息空间。这种确定全局编码向量的方法可以在多项式时间内完成。

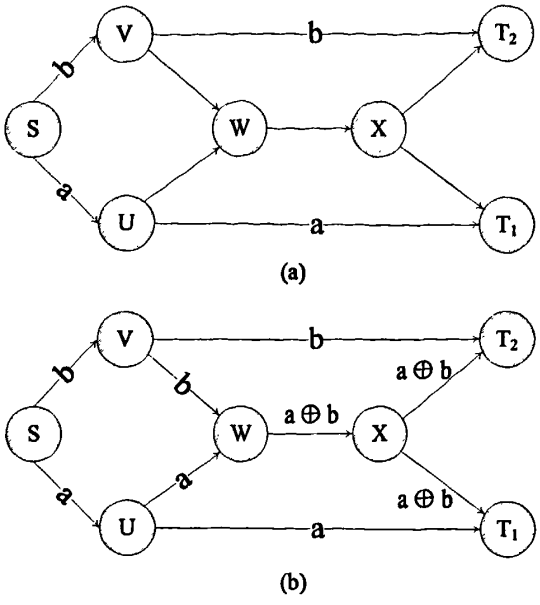


图 2-4 线性码组播

2.2.2.2 代数方法构造线性网络编码

R. Koetter 和 M. Medard[47][48]从另一个角度出发，提出了用抽象代数理论描述网络编码的方法。该算法需要知道整个网络的拓扑信息情况，通过构造符合要求的系统转移矩阵来实现网络编码。该算法虽然是一种指数时间算法，但为网络编码的实际实施提供了方向。

一. 数学模型

定义 2-11：$G(V,E)$是无延迟的通信网络，如果对于网络中的每一条边$e=(v,u)\in E$上的随机过程$Y(e)$均满足：

$$Y(e)=\sum_{l=1}^{u(v)}\alpha_{e,l}X(v,l)+\sum_{e':head(e')=tail(e)}\beta_{e',e}Y(e') \tag{2.20}$$

在目的节点v处有：

$$Z(v,j)=\sum_{e':head(e')=v}\varepsilon_{e',j}Y(e') \tag{2.21}$$

则称这样的G为域F_{2^m}上的线性网络。其中，系数$\alpha_{e,l}$，$\beta_{e',e}$，$\varepsilon_{e',j}$被称为局部编码向量，是有限域F_{2^m}中的元素，如图 2-5 所示。

定义 2-12：组播通信网络$G(V,E)$中，信源$s\in V$的输入可以看作是有限域F_{2^m}上的向量

$(\sigma_1,\sigma_2,...,\sigma_h)$。采用线性网络编码后，边$e=(v,u)\in E$上传送的信息$Y(e)$是信源输入符号向量的线性组合，用一个向量$Ve(e)$来表示组合的系数向量，称其为全局编码向量。则有

$$Y(e)=Ve(e)\begin{bmatrix}\sigma_1\\ \sigma_2\\ \vdots\\ \sigma_h\end{bmatrix} \tag{2.22}$$

可以看出，全局编码向量和局部编码向量之间的关系是:

$$Ve(e)=\sum_{e':head(e')=tail(e)}\beta_{e',e}Ve(e') \tag{2.23}$$

在一个组播通信网络中实现网络编码，可以通过对网络中的各个节点上的全局编码向量和局部编码向量进行必要的操作。所以如果一个通信网络是可解的，那么网络编码的求解可以通过两个途径实现：确定全局编码向量或者确定局部编码向量，它们具有同等的作用。从向量角度出发实现网络编码，是求解全局编码向量；求解局部编码向量，是从代数构造角度出发的实现。

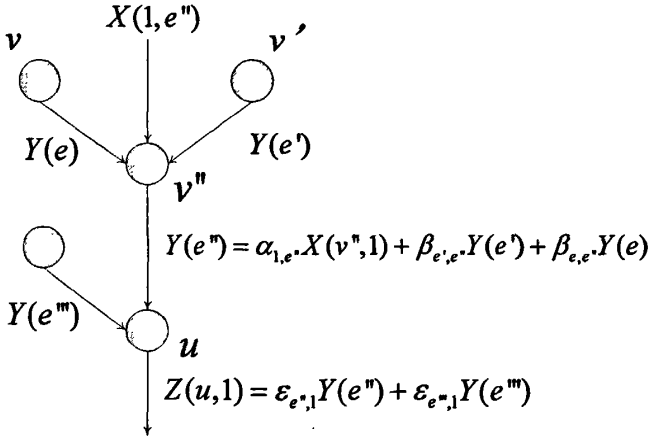


图 2-5 用代数方法构造网络编码的示例

二．编码的可译条件

首先定义任意通信网络的邻接矩阵 F，其中的元素为：

$$F_{i,j}=\begin{cases}\beta_{e_i,e_j} & head(e_i)=tail(e_j)\\ 0 & \text{其他}\end{cases} \tag{2.24}$$

则邻接矩阵 F 是一个$|E|\times|E|$的矩阵，它直接反映了通信网络的拓扑结构。

定义通信网络的信源输出矩阵 A 为：

$$A_{l,j}=\begin{cases}\alpha_{e_j,j} & \text{对一些}l\text{,有}x_i=X(tail(e_j),l)\\ 0 & \text{其他}\end{cases} \tag{2.25}$$

它是一个$\mu\times|E|$阶矩阵，反映了信源输出的情况。

通信网络的目的节点输入矩阵 B 定义为：

$$B_{l,j}=\begin{cases}\varepsilon_{e_j,j} & \text{对一些}l\text{,有}z_i=Z(head(e_j),l)\\ 0 & \text{其他}\end{cases} \tag{2.26}$$

它是一个$\eta\times|E|$阶矩阵，反映了某个目的节点的收到信息的情况。

综上可得，矩阵 A、B 和 F 均用局部编码向量表示，它们反映了整个通信网络的信息输入输出和整个拓扑结构的情况。

由此可得输入输出的几个相关方程：

(1) 输入与转移方程：描述某个信道上传输的信息与其尾节点的输入之间的编码关系；

$$y=xA+yF \tag{2.27}$$

(2) 输出方程：描述某个信宿节点的输出及其输入边之间的编码关系；

$$z=yB^{\mathrm{T}} \tag{2.28}$$

(3) 传递方程：描述网络的输入和输出之间的编码关系。

$$z=xM \tag{2.29}$$

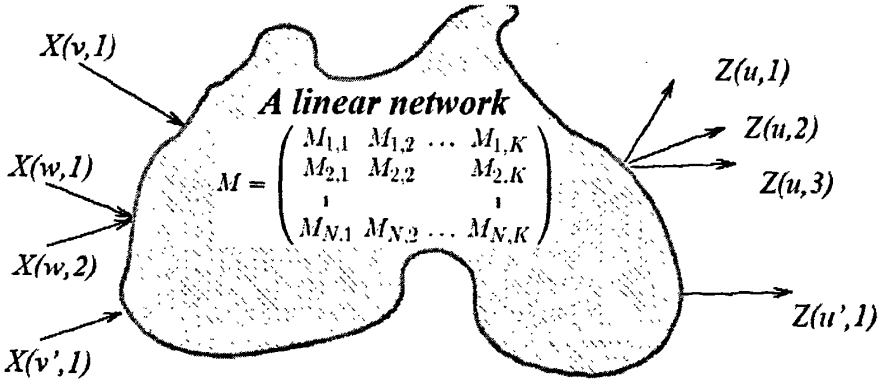


图 2-6 系数矩阵关系图

由此可得下面的定理：

定理 2-4[47]：在给定的通信网络中，定义反映网络拓扑结构的矩阵 A、B 和 F 后，可以得到这个网络的系统转移矩阵 M 为：

$$M = A(I-F)^{-1}B^T \tag{2.30}$$

其中 I 是一个 $|E|\times|E|$ 的单位阵。

综上所述，构造可译的网络编码的关键是系数转移矩阵 M 为可逆矩阵 $\det(M)\neq 0$，即构造可译的网络编码的关键是合适的选取系数。如果已经得到 N 个子矩阵的行列式之积 F，设其包含参数 $\xi_1\xi_2,...,\xi_n$，且把向量 $(\xi_1\xi_2,...,\xi_n)$ 的一个特定值称为一个点，把所有使 F=0 的点称为被函数 F 分割出来的代数族。下列算法用来得到一个不位于被函数 F 分割出来的代数族的一个点。

算法 2-1：输入：以 $\xi_1\xi_2,...,\xi_n$ 为变量的多项式 F，初始化 $i=1,t=1$。

迭代：1) 找出多项式 F 所有变量 ξ_j 中的最大度 δ，令 i 为满足 $2^i>\delta$ 的最小值；

2) 在 F_{2^i} 中找到一个 a_t 使得 $F(\xi_1\xi_2,...,\xi_n)|_{\xi_t=a_t}\neq 0$ 且令 $F\leftarrow F(\xi_1\xi_2,...,\xi_n)|_{\xi_t=a_t}$；

3) 如果 $t=n$ 则停止，否则 $t\leftarrow t+1$，返回到 2)。

输出：$(a_1,a_2,...,a_n)$。

有了此算法，就可以找出一个点 $(...,\alpha_{e_j,j},...,\beta_{e_i,e_j},...,\varepsilon_{e_j,j},...)$ 使 $F(...,\alpha_{e_j,j},...,\beta_{e_i,e_j},...,\varepsilon_{e_j,j},...)\neq 0$。算法中给出了网络编码可解时有限域大小的一个上界，即当域大小大于等于 2^i 时该网络的网络编码是一定有解的。

定理2-5：对于一个单源多播网络G，有N个接收节点。用F表示N个子矩阵 $M_{t_1},M_{t_2},...,M_{t_N}$ 行列式之积且假设 δ 是F中关于任意变量 ξ_j 的最高次幂，则在域 F_{2^i} 中存在该网络的网络编码有解，这儿的i取满足 $2^i>\delta$ 的最小值。算法2-1给出了求解的方法。

推论2-1：在一个无延迟可解多播传输网络G中，有一个源节点和N个接收节点，令其传输速率为R，则在有限域 $F_{2^m}(m\leq\lceil\log_2(NR+1)\rceil)$ 中网络编码有解。

给出了网络的上述代数描述后，可以得到下面的重要定理：

定理 2-6[47][48]：给定一个线性网络，下面的三个命题是等价的：

(1) 一个组播传输是可解的。

(2) 可以达到图 G 上由最小割最大流定理得到的容量限。

(3) 系统转移矩阵 M 的行列式在环 $F_2[\ldots,\alpha_{e_j,l},\ldots,\beta_{e_i,e_j},\ldots,\varepsilon_{e_j,l},\ldots]$ 上非零。

只要根据约束条件：系统转移矩阵的行列式不为 0，确定出上式中的满足条件的变量，也就是得到了局部编码向量，就完成了这个通信网络的线性网络编码。

三. 简单的编码示例

考虑图 2-7 这样一个点到点的通信网络，信息从源节点 v_1 传送到终端节点 v_4 [48]。

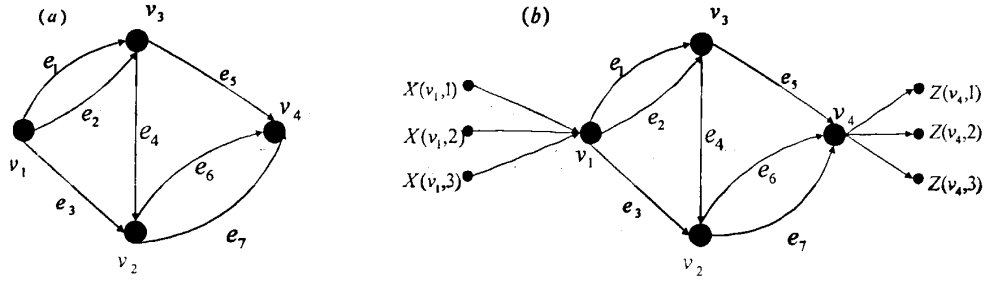


图2-7 单信源单信宿通信网流图

根据上图，可得到下列等式：

$$\left.\begin{aligned} Y(e_1)&=\alpha_{e_1,1}X(v_1,1)+\alpha_{e_1,2}X(v_1,2)+\alpha_{e_1,3}X(v_1,3)\\ Y(e_2)&=\alpha_{e_2,1}X(v_1,1)+\alpha_{e_2,2}X(v_1,2)+\alpha_{e_2,3}X(v_1,3)\\ Y(e_3)&=\alpha_{e_3,1}X(v_1,1)+\alpha_{e_3,2}X(v_1,2)+\alpha_{e_3,3}X(v_1,3)\end{aligned}\right\} \tag{2.31a}$$

$$\left.\begin{aligned} Y(e_4)&=\beta_{e_1,e_4}Y(e_1)+\beta_{e_2,e_4}Y(e_2)\\ Y(e_5)&=\beta_{e_1,e_5}Y(e_1)+\beta_{e_2,e_5}Y(e_2)\\ Y(e_6)&=\beta_{e_3,e_6}Y(e_3)+\beta_{e_4,e_6}Y(e_4)\\ Y(e_7)&=\beta_{e_3,e_7}Y(e_3)+\beta_{e_4,e_7}Y(e_4)\end{aligned}\right\} \tag{2.31b}$$

$$\left.\begin{aligned} Z(v_4,1)&=\varepsilon_{e_5,1}Y(e_5)+\varepsilon_{e_6,1}Y(e_6)+\varepsilon_{e_7,1}Y(e_7)\\ Z(v_4,2)&=\varepsilon_{e_5,2}Y(e_5)+\varepsilon_{e_6,2}Y(e_6)+\varepsilon_{e_7,2}Y(e_7)\\ Z(v_4,3)&=\varepsilon_{e_5,3}Y(e_5)+\varepsilon_{e_6,3}Y(e_6)+\varepsilon_{e_7,3}Y(e_7)\end{aligned}\right\} \tag{2.31c}$$

令矩阵 A 和 B 表示如下：

$$A=\begin{pmatrix}\alpha_{e_1,1} & \alpha_{e_2,1} & \alpha_{e_3,1}\\ \alpha_{e_1,2} & \alpha_{e_2,2} & \alpha_{e_3,2}\\ \alpha_{e_1,3} & \alpha_{e_2,3} & \alpha_{e_3,3}\end{pmatrix} \tag{2.32}$$

$$\mathrm{B}=\begin{pmatrix}\varepsilon_{e_5,1} & \varepsilon_{e_5,2} & \varepsilon_{e_5,3}\\ \varepsilon_{e_6,1} & \varepsilon_{e_6,2} & \varepsilon_{e_6,3}\\ \varepsilon_{e7,1} & \varepsilon_{e_7,2} & \varepsilon_{e_7,3}\end{pmatrix} \tag{2.33}$$

则可以得到一个系统矩阵：

$$M = A\begin{pmatrix} \beta_{e_1,e_5} & \beta_{e_1,e_4}\beta_{e_4,e_6} & \beta_{e_1,e_4}\beta_{e_4,e_7} \\ \beta_{e_1,e_5} & \beta_{e_2,e_4}\beta_{e_4,e_6} & \beta_{e_2,e_4}\beta_{e_4,e_7} \\ 0 & \beta_{e_3,e_6} & \beta_{e_3,e_6} \end{pmatrix} B^T \tag{2.34}$$

其行列式 $\det(M) = \det(A)(\beta_{e_1,e_5}\beta_{e_2,e_4} - \beta_{e_2,e_5}\beta_{e_1,e_5})(\beta_{e_4,e_6}\beta_{e_3,e_7} - \beta_{e_4,e_7}\beta_{e_3,e_6})\det(B)$。可以在域 F_{2^m} 的扩展域内选择参数，使得系统矩阵 M 的行列式在 F_{2^m} 中为非零矩阵。因此，令矩阵 A 与矩阵 B 为单位阵，使得系统矩阵 M 也为单位阵。等效于 *Ford-Fulkerson* 算法[48]解决问题的方法，令 $\beta_{e_1,e_5} = \beta_{e_2,e_4} = \beta_{e_4,e_6} = \beta_{e_3,e_7} = 1$，所有 $\beta_{e',e}$ 类型的其它系数均等于零。由此可以清楚地看到，一个在 v_1 与 v_4 之间的点对点通信在 3 比特每单位时间下是可行的。对于令人困惑的网络问题存在很多种解决办法，那就是对于系数 $\beta_{e',e}$ 的所有值，可令已知的转移矩阵的行列式的值不为零。

观察这个例子，可看到网络极其重要的地方是方程式 $(\beta_{e_1,e_5}\beta_{e_2,e_4} - \beta_{e_2,e_5}\beta_{e_1,e_5})$，$(\beta_{e_4,e_6}\beta_{e_3,e_7} - \beta_{e_4,e_7}\beta_{e_3,e_6})$ 被认为是可变的选择。因此该多项式的值并不为零。

2.2.3 线性网络编码的局限性

现已证明，可解的组播网络均有线性解。但是，对于非组播网络，线性就失去了其优越性。S. Riis 等人[54]给出了线性不可解的非组播网络。但[59]中用向量线性网络编码解决了那个问题。向量线性网络编码是一种更为广泛的线性运算，它不同于前面讲到的线性网络编码：它一次处理的每个信源的信息不为 1，这相当于在一次处理中重复使用通信网络。紧接着，Randall Dougherty 等人[55]又构造出了一个向量线性网络编码也不能解的非组播网络，但它却存在非线性解。

2.3 随机网络编码

2.3.1 随机网络编码的提出

无论是线性的向量编码还是代数编码，都要求对所选择的系数或是向量进行验证，只有当选择的系数满足一定的条件的时候才能够成功的编码。这实际上要求每一个节点已知

整个网络的拓扑结构，同时也知道整个网络每个节点的编码过程。只有这样才能保证边上选择的向量能够相互线性无关，同时选择的编码系数能够使整个网络有解。但这只是理想的情况。实际上，由于网络拓扑的变化和网络规模的扩大，每一个节点了解整个网络结构和每一个节点的编码系数不容易实现。

针对以上的问题，Ho 和 Medard 等人[60]提出了一种不用知道网络结构也不需要验证的编码方式，称为随机网络编码。同时，[60]还给出了随机网络编码的成功概率和鲁棒性分析，指出当网络编码的符号域足够大时，可以以接近 1 的概率获得网络组播的最大容量。

2.3.2 随机网络编码方案

Ho 提出，对于线性向量编码，可以让节点携带一个全局编码向量，在经过每一个节点的时候都根据该节点的编码方式在改变信息的同时改变编码向量。这样，当接收节点接到信息的时候，不需要知道整个网络的拓扑和网络的编码情况。只要接收信息的全局编码向量组成的矩阵维数为 d(一次发送信息的数量)，就可以解码出全部 d 个信息。这样一来接收节点就不需要知道网络的拓扑。

随机编码同时规定，中间节点在为边分配局部编码向量的时候只需要在有限域凡中随机选择数字，不需要验证是否相关。当然，这样也可能会导致在信宿节点出现线性相关的向量而使编码失败。

2.3.3 随机网络编码性能评价

定理 2-7[58]：对于一个信源相互独立或线性相关的可行的组播链接问题，如果一个网络码的部分或所有的编码系数都独立并且在一个有限域上均匀选取（一些节点的编码系数可以是固定的，只要这些取值是可行的），则接收者可以以最小概率 $((1-d/q)^v)$ 恢复出信息序列，这里 d 是接收节点的个数，$q>d$ 为编码符号域的大小。边上传递的信息来自所有源节点，同时将信息传到任何一个接收节点去。满足这样要求的边的最大数量是 v，即 v 是随机选取编码系数的链路的个数。

由此可见，网络传输的失败率与网络的规模成反比，传输失败率与编码之后的码字长度呈指数关系减少。这样只要根据网络的大小和信息多少，估算出传播需要的中间边的数量，就可以选择合适的字母表大小，在网络的稳定性与网络传播冗余量之间进行折中。对于线性相关的网络，这种算法也不需要源节点知道其他源的信息。与传统路由方法相比，

对于源节点的增加或减少和网络拓扑变化等问题，随机网络编码更加灵活。

随机网络编码是一种分布式的网络编码方案。在进行网络编码时，其不需知道整个网络的拓扑结构，就可以进行编码。编码符号域足够大时，可保证接收节点以很大的概率恢复出信源的信息。当符号域$|F|=2^{16}$时，理论上任一接收节点可至少以概率 0.996 成功获取信源发送的信息[13]。在采用随机网络编码进行网络组播时，多个信源可以是线性无关的，也可以是线性相关的。对于线性相关的信源，随机网络编码可以起到压缩信源信息的作用。此外，随机网络编码可适用于随机的网络结构。对于网络节点和链路时变的网络，随机网络编码可以利用整个网络的剩余容量来获得网络的最佳容量，提高网络多播的鲁棒性。

2.4 实际网络编码

2.4.1 实际网络编码的提出

上面提到的无论是线性向量、代数方法实现的网络编码还是随机网络编码，都是在一定的假设前提下提出的，比如非循环网络，无延迟网络等。这些理论上的假设限制了网络编码的使用范围。Chou 和 Wu 等人[6]提出了模拟实际网络中一切性质的实际网络编码(*Practical Network Coding*, PNC)。该网络编码方案应用的环境包括信息传送是不同步的、有延迟和丢失、边的容量随时间变化、网络的组播容量和网络拓扑结构均未知、每个节点的最大流相差很大、网络存在的错误类型未知、网络包含循环，以及各个接收节点性质不同等等。这种方法经过仿真证实可以在实际网络中应用。

实际网络编码的基本思想是：将分组数据编码成多份相互无关的数据，接收端只要能够收到其中的一部分，就可以恢复出原始数据，具体产生的编码数据数量与应用的需求相关。

2.4.2 实际网络编码的编码策略

假定一组含有 h 份报文，当节点要发送这些报文时，首先产生 h 个随机数，并组成 h 维向量$(r_1,...,r_h)$，随后，按向量$(r_1,...,r_h)$以及数据块$B_1,...,B_h$的内容生成一个新的数据块 E，并且也按向量$(r_1,...,r_h)$及该组中的系数向量$\vec{e_1},\vec{e_2},...,\vec{e_h}$生成一个新的系数向量$\vec{\alpha}$，$E$和$\vec{\alpha}$的定义分别如下：

$$E=r_1B_1+r_2B_2+...+r_hB_h \tag{2.35}$$

$$\vec{\alpha} = r_1\vec{e_1} + r_2\vec{e_2} + ... + r_h\vec{e_h} \tag{2.36}$$

每次传输都需产生一组新的随机数，除了数据源以外，中间节点如果收到多份数据，还可以再次编码。这种编码方法的好处在于，把不同的数据糅合在一起，减少了对单份数据的依赖，增加了数据传输的可靠性，非常适用于传感器网络报文易丢失的特点。只要信宿节点接收到 h（或大于 h）份数据，就可以恢复出原始数据。假定信宿节点收到的 h 份数据分别是 $E_1, E_2, ..., E_h$，则信宿进一步判断相应的 h 个系数向量 $\alpha_1, \alpha_2, ..., \alpha_h$ 是否线性无关，即 $\alpha_1, \alpha_2, ..., \alpha_h$ 所组成的 $h \times h$ 维矩阵是否为满秩的。如果满秩，则原始数据可按公式 2-37 恢复：

$$\begin{bmatrix} E_1 \\ E_2 \\ \vdots \\ E_h \end{bmatrix} = \begin{pmatrix} r_1^1 & \cdots & r_h^1 \\ \vdots & \ddots & \vdots \\ r_1^h & \cdots & r_h^h \end{pmatrix} \begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_h \end{bmatrix} \Rightarrow \begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_h \end{bmatrix} = \begin{pmatrix} r_1^1 & \cdots & r_h^1 \\ \vdots & \ddots & \vdots \\ r_1^h & \cdots & r_h^h \end{pmatrix}^{-1} \begin{bmatrix} E_1 \\ E_2 \\ \vdots \\ E_h \end{bmatrix} \tag{2.37}$$

这种方法与传统的前向纠错编码（*Forward Error Correction*，FEC）在思想上有些相似，但比 FEC 更为灵活、更具鲁棒性。这一点可以在下一章讨论的网络编码与多径传输结合的方法中明显地体现出来。

值得说明的是，对于普通的网络编码，如果接收到的信息组成的矩阵的秩小于信息发送时网络的最大流（假设为 d）的值，信宿节点将无法解码出任何信息。同时由于网络传输的延时和链路衰落的原因，节点必须使用大量空间存储没有解码的信息，从而占用了宝贵的存储空间，并且编码抵抗网络错误的能力也不足。而在[6]中，引入了按照优先级进行分类编码的方法—优先级编码传输，信宿节点即使没有接收到全部信息，而是接到了 n ($n<d$) 个数据包，仍可以完全解码出前 n 层信息，从而保证重要信息优先传送。

该文还引入了节点缓存丢包机制，证明了使用最简单的丢包机制就可以满足实际需要。这种机制就是当接收到新一代的信息的同时节点丢弃所保存的前一代信息，同时拒绝接收任何前一代的信息。这种方法可以在使网络传输的速度逼近网络容量的同时，实现较低的延时。

2.5 网络编码的性能优点

目前，网络编码是国际信息论和网络理论领域所关注的热点。作为一种新型的网络传输技术，网络编码的优点不言而喻。

2.5.1 增加网络容量

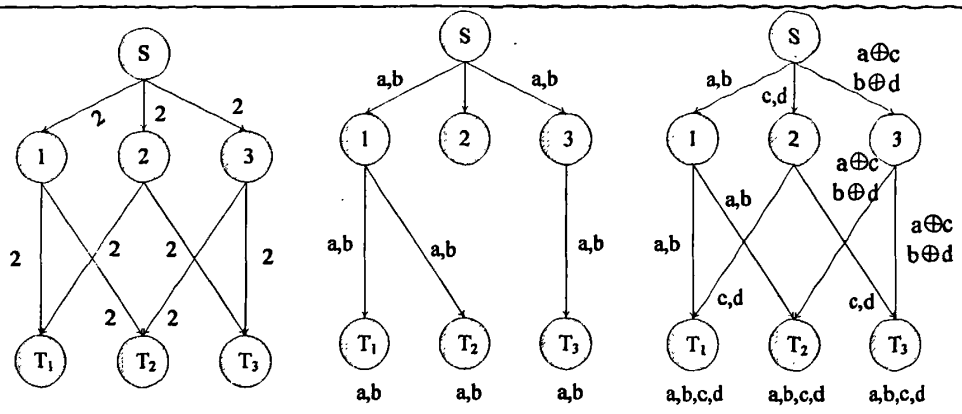
文献[1]指出，允许中间节点对信息流进行编码组合可以达到最大流最小割定理的上界。图 2-8 是基于网络编码的组播和 IP（*Internet Protocol*）组播在网络容量性能方面的比较。假设各条链路无差错和无时延。图 2-8(a)显示每条链路的容量为 2。由最大流最小割定理有 $\max flow(S,T_i)=4$，其中 $i=1,2,3$，因此信源 S 到信宿 T_1、T_2 和 T_3 的最大传播速率不可能超过 4。图 2-8(b)是一个单会话 IP 组播，在这种情况下，每个接收者所得到的最大传播速率均为 2。图 2-8(c)允许节点采用网络编码，这里采用模 2 加的编码方案。信息 a、b、c 和 d 在节点 S 被编码为 $a\oplus c$ 和 $b\oplus d$。在接收节点 T_2 中，c 和 d 可以从 a、b 和 $a\oplus c$、$b\oplus d$ 中恢复出来。同样，在接收节点 T_3 中，a 和 b 可以从 c、d 和 $a\oplus c$、$b\oplus d$ 中恢复出来。这样接收节点 T_1、T_2 和 T_3 均可接收到 a、b、c 和 d，从而达到网络的最大流限 4。

2.5.2 节省网络带宽

为了说明网络编码可以节省网络带宽资源，仍将基于网络编码的组播和 IP 组播进行比较说明。如图 2-9 所示，每条链路的容量为 2，在图 2-9(a)和图 2-9(b)中，接收者都能得到 a、b，但是在图 2-9(a)中整个网络传输了 10 比特，即占有的网络带宽为 10，而在图 2-9(b)中传输了 9 比特，即占有的网络带宽为 9，也就是说，使用网络编码技术后网络带宽消耗节省了 10%。

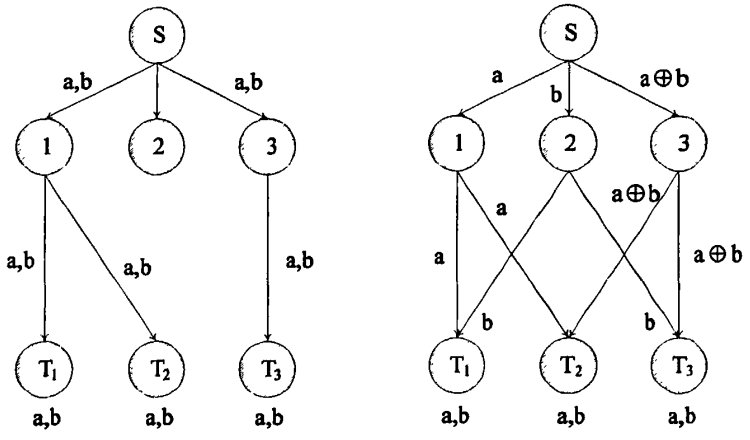
2.5.3 其他的好处

网络编码机制使信息更加分散，等同于将信息进行了隐藏，提高了信息安全性。接收信息的节点需要具有译码功能，同时要求得到足够的数据才能正确解码，信息很难被窃听，此外网络编码还可以防止拥塞方面的侵害，因此，将网络编码技术应用于军事等领域，其保密性和鲁棒性方面的潜力很大。P2P 网络中，网络编码机制可以降低下载时间。在大规模的 P2P 网络中，全局的调度非常复杂，而应用网络编码后，可以采用很简单的机制来构造随机的网络架构，提高系统性能，同时由于已编码文件块的密集性，基于网络编码的解决方案健壮性更强，例如当某种子节点过早离开时，编码机制的应用使网络信息块均匀分配，从而可以降低信息丢失的情况。



(a) 链路容量 (b) 单会话IP组播 (c) 基于网络编码的组播

图 2-8 网络容量性能的比较



(a) 单会话IP组播 (b) 基于网络编码的组播

图 2-9 网络带宽消耗的比较

2.6 本章小结

本章介绍的几种网络编码构造方式，其本质上都是线性网络编码，即某节点输出链路上的信息是输入链路信息的线性组合。我们下一章即将介绍的无线网络中的网络编码算法也是基于这一核心思想。但随着研究的不断深入，人们发现线性网络编码已经不能满足一些网络的需要，所以一些学者开始转向非线性网络编码的研究，这里因为篇幅的限制，不再详细介绍。此外，本章还分析了网络编码性能上的一些优点。

第三章 无线网络中的网络编码研究

网络编码最初是针对有线网络提出的。随着研究的不断深入，人们基于无线网络存在广播传送的优势，开始研究将网络编码应用于一些无线网络。本章首先对网络编码在无线网络中的应用进行简单介绍。之后，重点研究基于两种不同网络编码算法的 P2P2 内容分发系统。最后，本章还引入网络编码在安全性方面的研究，作为下一章的铺垫。

3.1 无线网络编码应用介绍

3.1.1 无线组播特性 WMA 及基于网络编码的信息交换

为了研究基于网络编码的信息交换，我们首先介绍一下无线网络的组播特性（*Wireless Multicast Advantage*，WMA）。我们考虑一个无线组播网络，网络的连通性取决于各个节点的发射能量。我们假定每个节点可以自由选择它的发射能力值，但其值不可超过 $p_{\max}$，接收能量值随 $r^{-\alpha}$ 变化，其中 r 是接收节点与发射节点之间的距离，α 为取值在 2 和 4 之间的参数，具体取值取决于网络的通信介质的特性。所以，相距为 r 的两个节点之间建立链路所需的发射能量正比于 $r^{-\alpha}$。为了不失一般性，我们将能量归一化。由此可得：

$$p_{i,j} = \text{节点}i\text{和节点}j\text{之间建立链路所需的能量}=r^{-\alpha} \tag{3.1}$$

如果一个无线通信网络的最大允许发射能量 $p_{\max}$ 足够大，那么节点就可以以充分大的能力值发射，以使整个通信网络是全连通的。

我们假设用的是全向天线，因此在一个发射节点通信范围内的所有节点均可以收到其发射的信息。下面就举例说明无线通信中的广播特性在组播中应用的重要性。如图 3-1 所示，无线通信网络中节点 i 要同时向其邻居节点 j 和 k 传输相同的信息，设到达节点 j 和 k 分别所需的能量为 $p_{i,j}$ 和 $p_{i,k}$，而节点 i 只要以 $p_{i,(j,k)} = \max\{p_{i,j}, p_{i,k}\}$ 的能量发射，则节点 j 和 k 都可以接收到所要的信息。于是可以节省的能量为：$p_{i,j} + p_{i,k} - p_{i,(j,k)}$。这就是无线网络中的无线组播特性[63][64][65]。

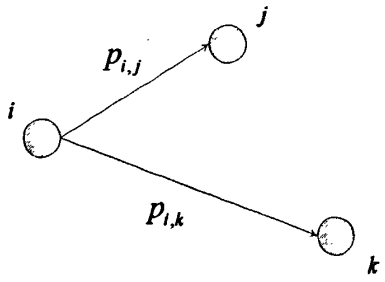


图 3-1 无线组播特性：$p_{i,(j,k)}=\max\left\{p_{i,j},p_{i,k}\right\}$

网络编码技术的引入给无线网络信息交换带来了新的契机。相互独立的信源之间的信息交换[69][79]是无线通信网络中的一种特殊情况。在这种应用下，结合无线网络的无线组播特性，应用网络编码的信息处理方式，可以在节省网络的能量消耗方面带来巨大好处。

定义 3-1 信息交换[79]：假定在一个基于分组的无线通信网络中，有两个相互独立的信源节点 a 和 b，其中，节点 a 想把它自己产生的数据包串$\{X_1(n)\}$发送给节点 b，而节点 b 想把它自己产生的数据包串$\{X_2(n)\}$发送给节点 a，如图所示。

信息交换一般是由两个单播过程完成，一个是从节点 a 到 b 的传输，另一个是从节点 b 到 a 的传输。因为这两个单播过程中传输的是不同的信息，所以它们分别处理，各自独立建立传输链路，完成传输任务。

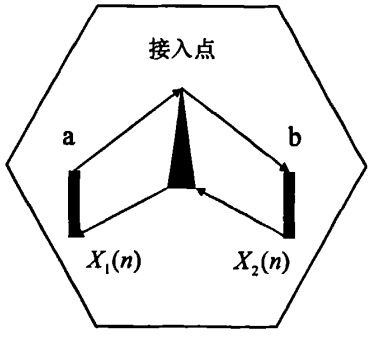


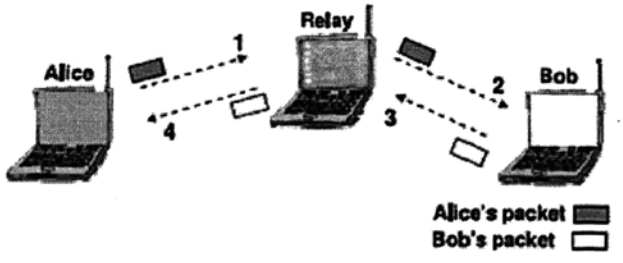
图 3-2 三个节点之间的信息交换

但是，我们可以运用网络编码来改变传统的信息处理方式。下面我们用一个简单的例子来说明网络编码在此处的基本应用思想。假定图 3-2 中的 WLAN 工作在有基础设施的模式下，即网络中存在一个接入点将网络连接到有线网络。与接入点有关的通信都分为上行链路和下行链路。在这种结构下，假定 a 和 b 需要交换信息。那么传统上，每包数据$\{X_1(n)\}$（或$\{X_2(n)\}$）需要先沿着上行链路发射到接入点，然后再由接入点通过下行链路发射到 b（或 a）。然而加入网络编码的思想之后，我们可以按如下方法进行 a 与 b 的信息交换：首

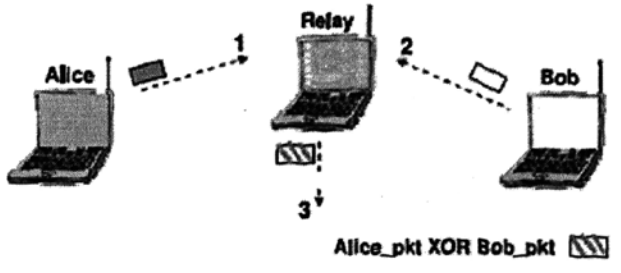
先，与传统处理方式一样，在上行链路阶段，a（或b）发射$\{X_1(n)\}$（或$\{X_2(n)\}$）给接入点；接着，由于无线媒质是一种广播媒质，所以在接入点处，我们可以将$\{X_1(n)\}$和$\{X_2(n)\}$进行处理过后再发送至a和b。而在这里，我们只需将$\{X_1(n)\}$和$\{X_2(n)\}$进行异或之后，将$\{X_1(n)\oplus X_2(n)\}$沿下行链路传送至 a 和 b 即可。最后，a 和 b 可以根据接收到的$\{X_1(n)\oplus X_2(n)\}$和自己原有的信息$\{X_1(n)\}$（或$\{X_2(n)\}$）解出自己想要接收的信息$\{X_2(n)\}$（或$\{X_1(n)\}$），这样就完成了信息的交换。

图 3-3 给出了一个采用网络编码技术后的无线网络信息交换的一个具体实例。网络编码技术的引入使 Alice 和 Bob 两个用户通过三次传输完成信息交换，而不是传统的四次传输。第三次传输充分利用了无线媒质的广播特性，减少了发射次数，提高了系统的吞吐量。

信息交换可以用在语音通信，两方参加的可视会议，以及即时消息的传输等场合。更甚者，信息交换不但可以应用在一般地端到端通信上，还可以应用在更广泛的情况下，比如说，节点a和b并非两个需要进行通信的终端，而是网络中间的两个路由器，但是它们之间需要交换互有的信息。



(a) 未编码



(b) 编码后

图 3-3 无线网络信息交换举例

3.1.2 网络编码与网络节能

由于无线网络特殊的传播方式，使得人们一直以来总是考虑如何使网络进行最小化能量传播，从而解决电池受限的问题。网络编码技术的提出为最小化能量组播问题打开了一个窗口。最小能量组播问题涉及到了网络层的网络编码或路由算法、媒质接入MAC层的调度算法以及物理层的功率控制。所以，它需要综合考虑各个层的因素，也就是，为了达到最佳性能，需要进行跨层设计。而在无线网络组播中，可以将网络编码和物理层的无线广播特性相结合，从而减小信息传输时能量的消耗[69]。本文在这一小节研究网络编码实现最小能量组播的原理。

假设合成容量图 G 消耗的总能量为 $P(G)$（瓦特）。如果图 G 中可以实现的组播速率为 r 比特每秒，则组播中每比特消耗的能量为：

$$\frac{P(G)}{r}\text{(焦耳/比特)} \tag{3.2}$$

最小能量组播问题就是找到合适的容量图 G，以及此图上的信息流量分布，使得在组播中传输每个比特所消耗的能量最小化。首先，在网络层我们采用网络编码，其描述是基于网络信息流在有向图上的分配的，这里不再赘述。下面我们给出基于网络信息流的、利用线性最优化得到最小能量组播的定理：

定理 3-1（最小能量组播定理）[69]：在一个固定无线通信网络中，设 $B=\{G_k\}$ 代表与最小能量组播有关的 ECG 的集合，那么由 B 张成的容量图集合如下：

$$\xi(B)=\left\{G \mid G=\sum\nolimits_k \lambda_k G_k, \sum\nolimits_k \lambda_k \le 1, \lambda_k \ge 0\ \forall k, G_k \in B\right\} \tag{3.3}$$

从信源 s 向信宿集合组播的过程中，每比特的最小能量 $\beta^*=\min\sum_k \lambda_k P(G_k)$，约束条件为：

$$g(vw) \le \sum_k \lambda_k c_k(vw), \quad \forall vw \in E \tag{3.4}$$

$$\lambda_k \ge 0, \quad \forall k \tag{3.5}$$

$$0 \le f_t(vw) \le g(vw), \forall vw \in E, \forall t \in T \tag{3.6}$$

$$\sum_{w \in V: vw \in E} f_t(vw) - \sum_{w \in V: wv \in E} f_t(wv) = 0, \quad \forall v \in V \setminus \{s,t\}, \forall t \in T \tag{3.7}$$

$$\sum_{w \in V: sw \in E} f_t(sw) - \sum_{w \in V: ws \in E} f_t(ws) = 1, \quad \forall t \in T \tag{3.8}$$

上述每比特的最小能量可以由在子图上设计网络编码实现，

$$G^* = (V, E, g^*) \prec G = (V, E, c) \tag{3.9}$$

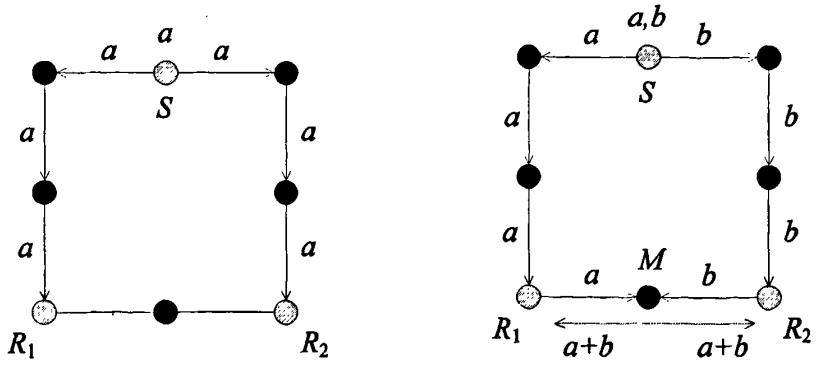
其中
$$g^*(vw)=\frac{1}{\sum_k \lambda_k} g(vw), \quad \forall vw \in E \tag{3.10}$$

上式中，$\{g(vw), \forall vw \in E\}$ 和 $\{\lambda_k\}$ 是由上面的线性表达式解得的。

上述定理从网络信息流的角度出发，说明了在无线网络中，将无线组播特性和网络编码相结合，可以在多项式时间内实现最小能量组播。

如图 3-4 所示。设每一节点在发射一个信息比特时，消耗的能量为 1。在图 3-4(a)中，信源节点 S 将信息比特 a 传输到接收节点 R_1 和 R_2，总共需要 5 次节点广播过程，消耗的总能量为 5。而在图 3-4(b)中，信源节点将两比特 a 和 b 分别传输到接收节点 R_1 和 R_2，节点 R_1 和 R_2 再将其传输到中间节点 M，节点 M 对其做模 2 运算后，再将其广播到节点 R_1 和 R_2。这样，两个接收节点就可以同时恢复出比特 a 和 b，总共用到了 9 次物理层广播，所以每比特消耗的能量为 4.5。通过这个简单例子可以看出采用网络编码技术可以提高无线网络的性能。

无线网络的节能问题一向受到研究人员的关注。尤其是移动Ad Hoc网络，其节点一般采用电池供电，为了延长网络的生存时间，节点采取各种方式节能。网络编码技术可以在一定程度上使其能量受限问题得到改善。



(a) 最佳组播，每比特消耗能量为 5

(b) 基于网络编码的组播，每比特消耗能量为 4.5

图 3-4 无线网络能量消耗比较

3.1.3 基于网络编码的 P2P 内容分发

P2P是一种分布式网络，网络的参与者共享他们所拥有的一部分硬件资源（处理能力、存储能力、网络连接能力、打印机等），这些共享资源能被其它对等节点（Peer）直接访问而无需经过中间实体。在此网络中的参与者既是资源（服务和内容）提供者（Server），

又是资源获取者（Client）。P2P结构与传统的C/S（Client/Server）结构的一个本质区别是：在网络中的每个节点的地位都是对等的。

短短几年的发展已经使P2P技术进入内容分发、即时通讯、网络流媒体传输、分布式计算、协同工作等各个领域，并促使这些领域出现了新的发展和应用。内容分发一直是网络技术发展的重要推动力，也是P2P技术最典型的应用。内容分发是指允许一定数量的用户合作从而共享特定的文件内容。目前更多地研究均是基于有线架构下的。然而，随着科技的发展，各种形式的无线通信（最后一公里连接，传感器，社团网络等）将在未来通信中占主导地位。目前的无线网络仍然主要受到带宽的限制，网络编码潜在的优势恰恰可以弥补这个不足。

由于网络节点和链路经常会出现失效，因此会影响网络的鲁棒性及分发效率。引入网络编码技术，可以在一定程度上提高网络的鲁棒性[80]。如下图所示，在网络的传输过程中，图3-5(a)每个节点若都要收到a、b、c三个比特，只能容忍节点2或4中的一个失效；而图3-5(b)中可以容忍任何一个节点失效，其它节点均可以根据剩余的三个节点完整地恢复出数据a、b、c。

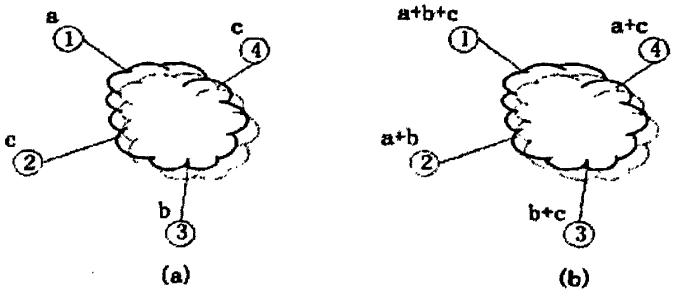


图 3-5 网络编码鲁棒性示例

本文将在 3.2 小节对采用网络编码的 P2P 内容分发算法进行具体研究。

3.1.4 网络编码在无线自组织网络中的应用

3.1.4.1 无线 Adhoc 网络中网络编码的应用优势

网络编码在改善网络吞吐量、降低节点能量消耗、减少网络延迟方面有着很好的应用前景。本文在这里将网络编码改善 Adhoc 网络性能参数的原理与方式进行了总结。

(1) 改善网络吞吐量

网络编码提出的最初目的便是提高组播网络的网络容量，使单信源多信宿网络的吞吐量能够达到或者接近该网络的最大流。在 Adhoc 网络中，Jun Yuan 和 Zongpeng Li 等人[66]

将优化网络吞吐量的问题分解为优化网络层多跳路由以及优化物理层能量分配两个子问题，并提出了一种跨层优化的策略。该策略分别在网络层和物理层平衡链路带宽的供需，在这种平衡状态上，提供了利用网络编码优化吞吐量的流路由方法。与此类似，Yunnan Wu等[67]提出了一种中心化的算法。该算法主要是进行递归的跨层优化，在获知物理层状态的同时，对MAC层分时调度和网络层最大流指派进行联合优化。

运用网络编码可以在很大程度上提高网络吞吐量，但是不可避免地会增加网络的复杂性。因此，不少学者在致力于提高Adhoc网络组播吞吐量的同时，寻找性能更好的编码方式来降低复杂度。Yunnan Wu和Kung等人[68]从网络编码的角度把网络链路划分为两类：进入中继节点的链路和进入目的节点的链路。他们证明，在达到同样组播容量的前提下，只需要在进入中继节点的链路进行网络编码即可。而对进入目的节点的链路，可以只采用路由策略，降低了编码的复杂性。Tracey等人主要考虑的是时变的、链路容量受噪声干扰影响的无线网络模型。他们在时变无线网络模型的基础上，使用了动态的压力反馈算法来分别优化网络编码和路由。研究表明，在网络状况较好的情况下，网络编码相对于路由方式，能够较大程度地提高组播通信方式时的网络吞吐量；在网络状况较差的情况下，网络编码和路由方式在组播通信时的网络吞吐量差别不大。此时，网络编码的优势则体现在降低网络的复杂度上。因此，可以根据不同的网络状况，动态地调整网络编码算法以获得合适的网络性能参数。

(2) 降低能量消耗

在Adhoc网络，尤其是无线传感器网络中，节点通过携带能量有限的电池供电。因此，在这些网络中，各种协议设计（如MAC协议，路由协议）首要目标便是能源的高效使用。

在组播通信网络中，Yunnan Wu等[69]提出了Adhoc网络中，基于网络编码的最小能量消耗算法。在采用网络编码的情况下，能量消耗最小化问题可以转化为网络的线性规划问题。Lun 等人[70]在动态变化和不可靠的网络环境下，实现了最小化能量消耗的组播算法。Lun和Medard等人还提出了非中心化和随机方式的网络编码解决方案[71][72]。

广播通信是 Adhoc网络中一种很普遍的通信方式。在很多路由协议中，网络大部分节点都需要对全网广播自身的某些信息。用路由方法实现最小化能量广播是非常困难的。已经证明，解决最小化能量广播问题的最小权生成树算法是NP完全问题[73][74]。另外，也有人提出采用启发式算法来解决这个问题，但是这种方法的计算开销和时间消耗都比较大。现在 ，研究者开始转而利用网络编码来解决广播通信中的能量有效性问题。Widmer和 Fragouli 等人[75]首先提出了一种针对简单圆形拓扑和矩形拓扑的网络编码算法。该算法相对于路由方法的精妙之处在于，充分利用了无线通信的广播特性，一次通信就让邻居

节点都获得消息，邻居节点同时也获得自身邻居的数据包并进行编码。这样，经过少数几次广播之后，每个节点都会获得全网节点的信息。这种在简单网络拓扑结构下的广播算法推广到节点随机分布的一般网络中，仍然取得了很好的效果。为了提高无线网络中的单播通信效率，传统的解决办法有重传、端到端编码、链路编码、路径编码等。现在，有研究者提出了网络编码和分布式流优化结合的方法[76]。这种方法能够在很大程度上提高传输效率，有效地减少重传次数，增大传送成功概率，从而降低能量消耗。该研究针对的网络节点数目较少，因此在网络规模较大的情形下，寻找减少网络数据包重传次数的网络编码方式有待进一步地研究。

(3) 提高网络的健壮性

Adhoc 网络中，节点间采用无线通信方式，信道衰减严重。在无线网络中，空间差异性的利用已经被广泛认为是克服无线信道衰减的最有效方法之一。Chen 等人[77]研究了在分布式天线系统和多入多出系统（DAS-MIMO）中线性网络编码如何提高网络鲁棒性的问题。在 DAS 模型中，Chen 等人引入了网络编码的概念，经过理论推导和实验仿真，证明了在分布式天线系统中，不论有无辅助天线，网络编码都能提高网络的性能，尤其是在减小系统丢包损耗方面。在大规模的无线网络中，可以在网络编码的基础上结合应用分布式信道编码，进一步提高网络性能。文献[78]从纠删码的思想出发，提出了一种利用网络编码进行网络多播链路失败恢复的方案，该方案可有效抵抗网络链路失败对网络连接可靠性的影响。

3.1.4.2 网络编码在 WSN 中的应用

无线传感器网络（WSN）就是由部署在监测区域内的大量的廉价微型传感器节点组成，通过无线通信方式形成的一个多跳的自组织的网络系统，其目的是协作地感知、采集和处理网络覆盖区域中感知对象的信息，并发送给观察者。随着研究者们将网络编码的领域拓展到无线网络中，用途广泛的无线传感器网络（WSN）自然成为了研究重点。许多人针对WSN中的各种关键问题提出了基于网络编码的解决方案，例如WSN中数据分发、传输、存储以及数据采集问题[88][93][94]。然而，由于网络编码的编解码复杂度较高，在WSN中对网络编码技术的使用目前仍然非常有限。我们在这里主要介绍一下WSN中网络编码当前的2种主要应用：多径传输和信息交换。

一．WSN 中基于网络编码的多径传输

在 WSN 中，保障可靠的数据传输是一个关键而棘手的问题。当前的研究大都采用冗余传输的方式来保证数据传输的可靠性，如多径或者重传。其中，多径方式就是在源和目

的之间构建多条路径，通过将同一份数据报文同时沿着多条路径传输，来增加数据传输的可靠性；而重传方式主要是计算为达到一定的传输可靠性，路径上每跳至少需要的传输次数。多径相对于重传，其最大的优势是延时小。然而，这些方法会造成能效降低，缩短网络生命周期。

由于网络编码可以在网络中提高网络吞吐率、降低能耗、减少传播延迟，一些研究者提出将网络编码与多径数据传输相结合，以使传感器网络获得更高的能效。由于传感器网络中主要的能耗用于节点间通信，因此减少传输量是节约能耗的主要方法。与传统多径方法相比，采用网络编码能够在保证同等数据传输可靠性的同时，显著地减少通信量，为解决可靠数据传输问题提供了一种高效的方法。

Dimakis等人[88]将网络编码应用在传感器网络的数据存储中，提高了数据备份的鲁棒性。Toledo和Wang等人[15]将网络编码和Directed Diffusion[89]相结合，选择性地加强有利数据的路径。Sengupta等人[16]也将路由和网络编码结合起来进行了研究。

当使用网络编码进行多径传输时，源节点不像传统多径方法那样对每份数据沿多条路径传输，而是首先将数据进行分组，每个分组包含 h 个等长的数据段 B。每组按其产生的先后顺序赋予一个组标识，第 1 组标识为 0，第 2 组标识为 1，以此类推。当组标识增长到某个上限值时，再让其重新回归为 0。每个数据段都分配一个 h 位的单位系数向量 e，对于数据段 $B_i(1 \le i \le h)$，其相应的 e_i 值定义为：除第 i 个分量的值为 1 外，其余分量的值均为 0。这样，一个组内的所有向量就构成了一个 $h \times h$ 单位矩阵。对每个数据段而言，其报文格式如图 3-6 所示；源节点处进行编码的方法如图 3-7 所示；整个编码数据传输的过程如图 3-8 所示。

图 3-6 使用网络编码的报文格式

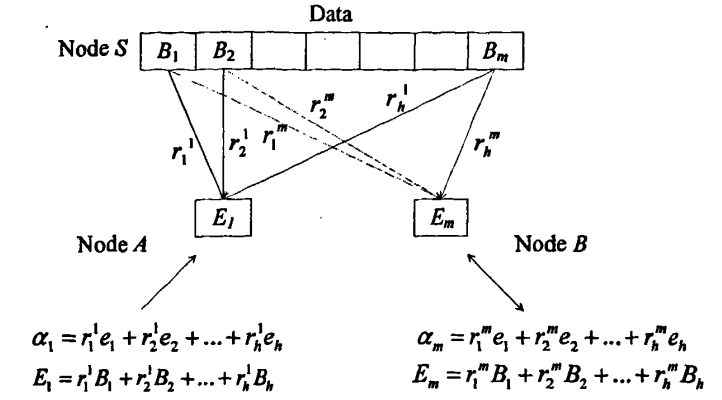


图 3-7 源节点将组内数据编码成 m 份新数据

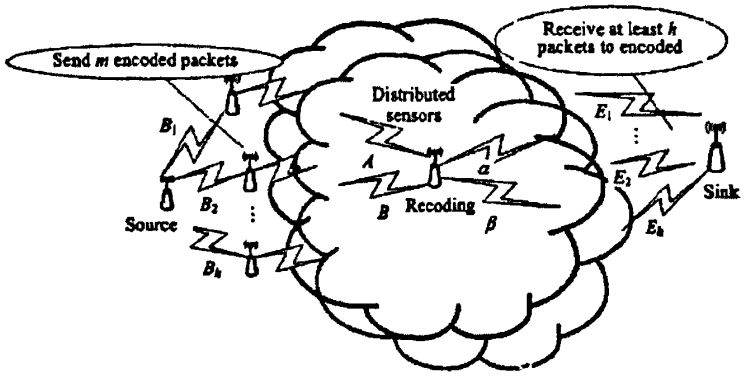


图 3-8 基于网络编码的多径传输

二．WSN 中基于网络编码的信息交换

我们在3.1.1里已经介绍过采用网络编码进行无线网络信息交换的基本原理。信息交换过程存在于多种网络应用中，比如在分布式计算环境中的路由发现和更新阶段,需要在网络节点之间交换同步信息和阻塞控制信息，而这种信息交换的方式常常被称作Gossiping或All-to-All广播[90]。在以数据为中心的无线传感器网络中，节点间的信息交换问题也越来越受到研究者的关注。信息交换的效率反映了网络的服务质量，甚至直接影响到网络的生命周期。

Wang等[91]针对高密度传感器网络中的格型拓扑网络和随机拓扑网络，提出了基于网络编码的信息交换算法，以解决网络中的2跳（2-hop）信息交换问题。他们在理论分析和仿真实验的基础上，证明了网络编码在这类问题中，相较于传统转发算法的高效性。而Xiong等[92]立足于分簇的无线传感器网络，提出了基于网络编码的簇内信息交换算法。他们经过理论分析和仿真实验，将网络编码算法与传统信息交换算法进行了比较和总结，并得出结论：网络编码算法在能量消耗和时间成本上要优于传统的洪泛、路由和中继算法。

3.2 采用网络编码的 P2P 内容分发研究

近年来国内外众多学者在研究网络编码理论的过程中，积极探索了这一技术在P2P网络内容分发方面的应用。例如，Gkantsidis等[11]基于网络编码技术，设计了一个P2P内容分发系统Avalanche。他们的实验结果表明，网络编码技术可以提高整个系统2-3倍的吞吐量。本小节主要研究一种采用稀疏线性网络编码的P2P内容分发系统（以下简称为SLNC分发系统）[84]。

3.2.1 SLNC 分发系统的体系结构

Ma和Xu等人[84]基于Cooper关于稀疏矩阵的理论成果[83]，提出了一种稀疏随机线性编码技术，并使用该技术在局域网内实现了一个由50个节点组成的P2P内容分发系统，通过限定每个节点的连接数以及每条通讯链的带宽来模拟因特网的实际环境。与完全网络编码相比，稀疏线性网络编码降低了编码操作的计算复杂度，并保持了较高的成功解码的概率。其基本体系结构如图3-9所示，包括7个模块，分别是：Chord服务模块、对等更新模块、传输控制模块、种子产生模块、稀疏编码模块以及相关检测和解码模块。

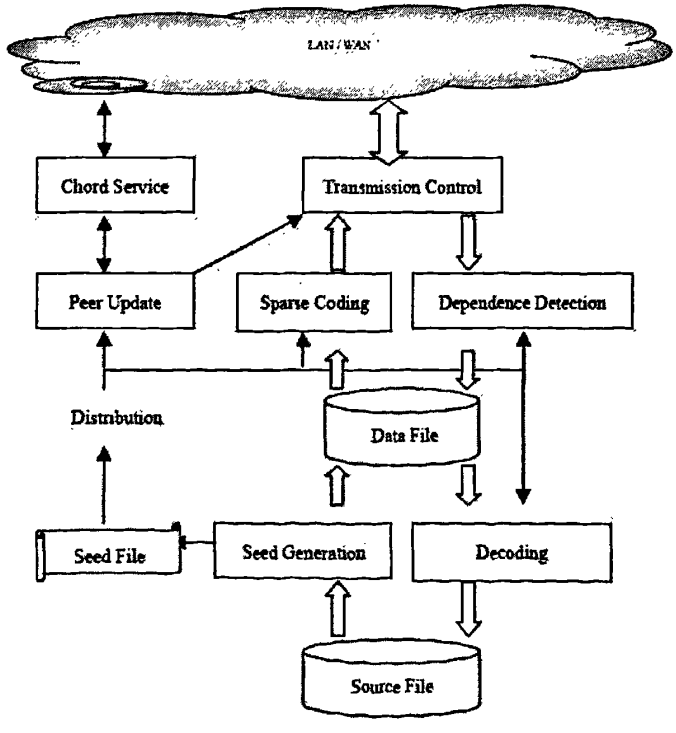


图3-9 基于稀疏网络编码的P2P内容分发系统

3.2.2 SLNC 分发系统的链路建立

该系统首先用Chord协议[85]建立拓扑结构，使得每一个参与节点知道有哪些节点参与内容分发（通过建立一张包含所有参与内容分发节点的IP列表）。同时，将每个对等节点的最大连接数设为10，每个节点在连接数小于5时，会周期性地发起连接请求；在连接数小于10时，可以接收其他节点的连接请求。当连接双方中至少有一方对对方的数据“感兴趣”时（如对方拥有20块以上可能与己方线性无关的数据块），建立连接；如果双方都对对方的数据“不感兴趣”（如对方传给己方过多线性相关块），连接将被断开。同时，每条连接的上传和下载速度都被限制在100kB/s以下。

3.2.3 稀疏编码、相关性检测和解码

为保证传输的正确性，我们使用随机线性网络编码（RLNC）[2]作为构造稀疏网络编码的基础。RLNC是以2.2.2小节中叙述的向量角度构造的线性网络编码为基础的，不同的是，RLNC系统矩阵中的系数是随机选取的，而不是普通线性网络编码那样预先规定好的，也就是说，网络中的每个节点随机独立地选择一组系数，然后将它所接收到的数据符号（或分组）的线性组合发送出去。

为了使系统达到低编码计算复杂度和较高的解码成功率，必须选择一个合适的编码密度。这里，我们使用一种基于Galois域上随机矩阵的稀疏编码策略。为了保证该随机矩阵为非奇异的概率尽可能高，我们根据定理3-2来选取稀疏矩阵，并将其与原RLNC的系统矩阵相乘，即可得到稀疏网络编码的系统矩阵。定理3-2可以由[83]推导得出，由上可知，它也是本系统使用的稀疏编码方法的理论基础。

定理3-2[84]：假设 $M=(m_{ij})$ 是一个 $n\times n$ 的Galois域上的随机矩阵，矩阵中的每个元素 m_{ij} 都以下列概率独立同分布：

$$P_r(m_{ij}=r)=\begin{cases}1-p & r=0\\ p/(t-1) & r\in[1,2,...,t-1],\end{cases} \tag{3.11}$$

则如果 $p\geq(\log n+d)/n$（d为非负常数），那么：

$$\lim_{n\to\infty}P_r(M\ is\ non-singular)=e^{-2e^{-d}}\prod_{j=1}^{\infty}1-t^{-j} \tag{3.12}$$

根据定理3-2，我们可以保证由同一个对等节点产生的所有编码分块都以较高的概率线

性独立。如果 $p=(\log n+d)/n$，一个 $n\times n$ 矩阵是非奇异的概率就很高，例如当 n 足够大，t=28，d=6或10时，矩阵分别以大于99.5%和99.991%的概率非奇异。在这里，我们把要分发的原始内容分成相同大小的 n 块，在源节点处将编码密度设定为 $p=(\log n+d)/n$，以使源节点能够以较高概率产生 n 个独立的分块。

设非源节点 A 有 k 个分块 $B_1,B_2,...,B_k$，并由此产生 l 个分块 $B_1',B_2',...,B_l'(l\le k)$。将 $B_1,B_2,...,B_k$ 的 $k\times n$ 系数矩阵表示为 M，而 $B_1',B_2',...,B_l'$ 在节点 A 处的 $l\times k$ 局部系数矩阵则表示为 N，因此，$B_1',B_2',...,B_l'$ 的系数矩阵就是 $N\times M$ 阶。由于此系统中所有的对等节点只接受独立分块，因此 $rank(M)=k$。如果 $rank(N)=l$，那么 $B_1',B_2',...,B_l'$ 就是线性独立的。同时，根据定理3-2还可以得出，如果 $p=(\log k+d)/k$，$rank(N)=l$ 的概率上限将为 $e^{-2e^{-d}}\prod_{j=1}^{\infty}1-t^{-j}$（$k$ 足够大），并且 $B_1',B_2',...,B_l'$ 将以较高概率线性独立。这里需要注意的是，在实际情况下，k 可能并不一定足够大到满足定理3-2的先决条件。因此在系统中非源节点处，我们设定 $p=(\log n+d)/k$，以确保以较高概率产生独立的分块。后面的仿真实验可以表明，在源节点处 $p=(\log n+d)/n$，而在非源节点处 $p=(\log n+d)/k$ 在实际环境中就足够了。如果 p 过大，反而会导致分块独立的概率降低，而且编码计算复杂度也会过高。

由于所有对等节点处的编码过程都是独立同分布的，因此很难保证不同节点处的编码分块都线性无关。另外有一些影响线性相关性的因素，例如网络拓扑中如果有环存在，也会为分发系统引入线性相关性。这里必须指出，由这些因素引起的线性相关性是无法通过增加编码密度来解决的。

当一个分块到达接收节点时，该分块的系数就被取出，并作为一个新的行向量添加到内存的系数矩阵中。之后，接收节点就可以在检验该系数矩阵的线性相关性（通过高斯消去法）之后，判断是接受这个分块，还是丢弃它。为了便于评价该内容分发系统的性能，这里将节点的丢包率定义为被丢弃的分块数与所有接收到的分块数的比值。通过衡量丢包率，我们可以研究在使用稀疏编码后，传输中出现相关分块的概率。对于那些被接受的分块，我们可以将他们作为行向量添加到节点辅助存储器的分块矩阵中。这样一来，内存中仅需存储分块的系数以用于相关检测，而不需存储整个分块，大大加速了接收过程。另外，我们还可以将存储在内存中的系数矩阵变换成三角矩阵（因为有些对角线上的元素在使用了高斯消去法后可能会变为0，我们通过列交换得到三角矩阵），这样可以在有新分块到

达时加快执行高斯消去的速度。当一个节点接收到n个独立分块时，就能将原始内容成功解码出来。

综上所述，在此内容分发系统中，中间节点为自己接收到的每一块数据在$GF(t)$中随机选择一个系数，该系数以不小于$p=(\log n+d)/k$（k是该节点当前拥有的块数）的概率大于0，以$1-p$的概率为0。发送出去的编码块是这些系数与数据块的线性组合，系数也同时被发送出去。在实验中，我们取$t=256$，$d=10$，系数矩阵非奇异的概率不小于0.99991（若系数矩阵非奇异，接收节点即可解码源内容）。节点接收到编码块后，使用高斯消元法对其进行线性相关性检测：若与已有数据块线性无关，将被存入硬盘，否则将被丢弃。传送线性相关的数据块会大大降低网络性能，因此需要研究减少线性相关块出现的策略。

3.2.4 SLNC 分发系统的传输控制

在系统中传输和接收相关分块都会大大降低基于网络编码的内容分发的性能。为此，可以采用下面3种方法来减少分块相关的概率。

3.2.4.1 邻居选择

连接建立后，该连接两端的节点会互相询问对方拥有的块数。如果节点拥有的分块很少，它就会以较高概率传送相关的分块。所以在一个内容分发阶段，除了开始和结束时刻，节点都不会向拥有少于$s=\log n+d$个分块的邻居请求数据（避免接收到相关分块）。但是对于在开始时刻拥有较少分块，在分发结束时刻只需增加少量新分块来完成接收过程的节点，不管邻居节点拥有多少分块，它们都会持续向邻居请求新的分块。虽然这样有可能产生更多的相关分块，但接下来的仿真实验表明，这种策略能够大大加快分发过程。综上所述，一般情况下，如果对方拥有多于$s=\log n+d$块数据，己方对其“感兴趣”，可以建立连接；在节点拥有少于s块或多于$n-s$块时，总是对其他节点的数据“感兴趣”。

3.2.4.2 编码区间

在基于完全随机线性网络编码的系统中，某个节点的所有分块都要参与编码，这会对相应的接收者造成快速信息扩散。但是如果使用稀疏网络编码，节点处的所有分块都以相同概率参与编码，因此新到达该节点的分块可能不会被选择参与编码，则在某些情况下，这些分块在网络中的扩散速度就相对变慢了。

在拥有n个数据块前，节点的数据块会动态增加，这样，在编码时会使得随后收到的

数据块被选中的几率大大小于先收到的数据块，由此可能增加收到线性相关块的概率。我们采用编码区间来缓解该问题。当一个节点第一次向邻居发送数据块请求时，会记录该邻居当前拥有的数据块数q，而该邻居也只会发送$[1,q]$区间中数据块的编码块。在接收到邻居q块线性无关数据或连续收到两个线性相关数据块后，节点会再次询问该邻居，若此时邻居的数据块数为q'，并且区间$[q+1,q']$长度大于s，或节点拥有少于s块或多于$n-s$块数据，则请求$[q+1,q']$间的数据块。

3.2.4.3 环消除（自动断开连接）

网络中的环或过多的共同邻居都可能大大增加某条连接传送线性相关数据块的可能性。所以在传输过程中，可以采用分块相关性检测（后验方式）来避免这些不利影响。如果一个节点从某邻居节点处连续收到两个线性相关块，上述编码区间会滑向下一个区间；如果收到线性相关的数据块数超过从邻居处收到的总块数的3%，暂停向该邻居请求数据30秒，如果30秒后相关比率还是大于3%，则继续暂停请求数据30秒，依此类推；如果超过5%，该连接（逻辑链路）会被断开。

3.2.5 性能分析与仿真

本小节从编解码速率、编码密度、编码区间和系统吞吐率等方面验证稀疏网络编码对P2P内容分发系统性能的影响。我们使用上述稀疏随机线性编码技术（SLNC）在局域网内实现一个拥有50个节点的P2P内容分发系统，并用3.2.2小节的链路建立方法来限定每个节点的连接数以及每条通讯链的带宽，以此来模拟因特网的实际环境。

3.2.5.1 编解码速率

编解码速率会极大影响系统的性能，如果编码速度跟不上网络传输速度，网络编码反而会使系统性能降低。因此使用稀疏线性编码时，我们可能更关心与一般的完全线性网络编码相比，它的编解码速率如何。本文以100M大小的文件作为原始分发内容，对稀疏编码的编解码速率进行了测试（实验环境为处理器Intel Celeron Northwood Processor 2.0GHz，内存512M的PC机）。在仿真实验中，设定稀疏编码的编码密度为$p=(\log n+10)/k$（n是分块总数，k是某个节点拥有的分块数），分块大小从64KB到2048KB不等。图3-10是不同分块大小下，稀疏编码和完全线性编码的编码速率对比的仿真结果。结果表明，稀疏网络编码大大提高了编码速率，在某些情形下，可使其达到4MB/s。另外在编码过程中，如果不

把整个100MB文件都下载到内存中，同样可以达到一个较高的编码速率。从图3-10可以清楚地看出，稀疏网络编码的编码速率即使在没有进行码字优化的情况下，已经可以达到内容分发所需的一般传输带宽要求。从另一方面来看，分块大小为256KB时，完全线性网络编码仅能使编码速率达到300KB/s，只有稀疏编码的10%不到。在内容分发阶段，由于节点接收到的分块可能被多次编码，系数矩阵的密度很有可能会增加。在测试解码速率的仿真实验中，对原始分块进行1、4、8次稀疏编码后再执行解码。图3-11显示了不同分块大小下，多重稀疏编码与完全线性编码的解码速率的比较。相较于图3-10中的编码速率，解码速率就非常低。从图3-11中可以看出，稀疏编码和完全编码对于不同分块大小，达到的解码速率几乎相同。虽然在多次编码后，系数矩阵密度可能会增加，但解码速率对于不同次数的编码来说几乎是一样的，这是因为如果一个矩阵是稀疏的，它的逆矩阵通常就不再是稀疏矩阵了。还有一点要提出的是，稀疏编码在使用高斯消去法的解码过程中起的作用很小。结合图3-10和图3-11来看 ，编解码速率随着分块大小的增加而增大。对于大小固定的文件，分块数目和系数矩阵的阶数随着分块大小的增加而减小，因此解码的计算复杂度随着分块大小的增加而降低。然而，在分块大小为256KB到512KB不等时，稀疏编码和完全编码的解码速率都降低了。这种情况可能是由于内存读取的开销和缓存大小引起的。

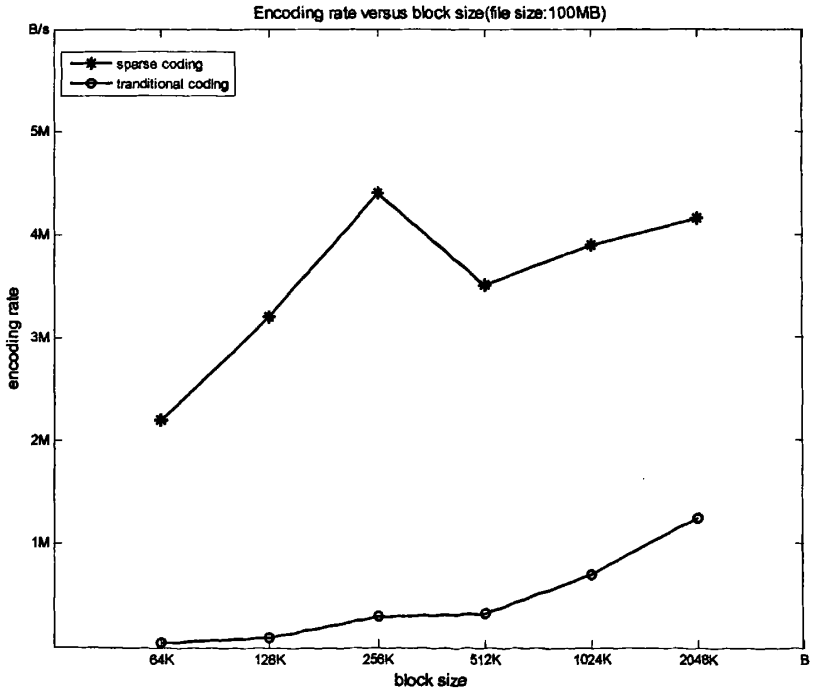


图 3-10 不同分块大小下稀疏编码与完全线性随机编码的编码速率比较（B/s）

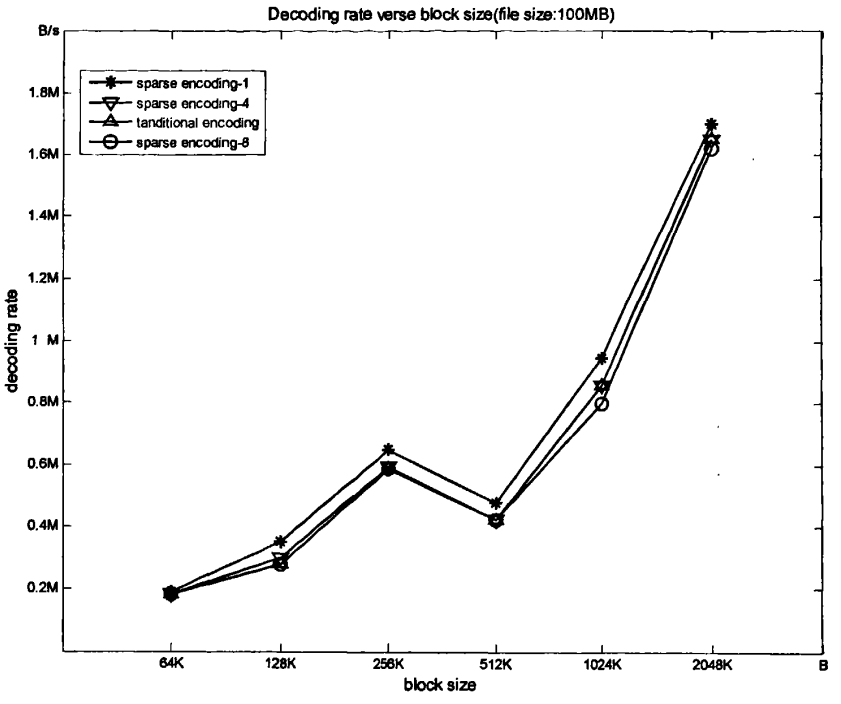


图 3-11 不同分块大小下 3 种稀疏编码与完全线性随机编码的解码速率对比（B/s）

3.2.5.2 编码密度

本文通过对一个128M大小的文件进行分发实验来研究不同编码密度对系统性能的影响，分块大小设定为256KB。源节点处编码密度设为 $p=(\log n+d)/n$，非源节点处则设定为 $p=(\log n+d)/k$，其中n=512，k是编码区间长度。实验从非源节点的平均下载时间和平均丢块率（丢弃的块数/接收的块数）两方面来衡量系统性能。当一个节点拥有n个独立分组时，就会停止接收其他节点的数据。图3-12显示了编码密度参数d由0变化到10的实验结果。可以看出，与 $d\geq 4$ 相比，d=0时系统性能最差（平均下载时间最长），丢块率也最高。直到d=4，系统性能随着d的增大而逐渐提高。当 $d\geq 4$ 时，不同d值下的平均下载时间和平均丢块率几乎相等。因此可以得出结论：d越大，分块之间线性相关的可能性就越低（根据Cooper的理论）。但是d=10时的稀疏线性编码系统和完全编码的系统（可以看作是d值很大的一种稀疏编码系统）所达到的性能几乎等同，而此时由于存在一些特定拓扑诸如环之类，丢块率仍然只有2%。

另外我们还通过一个32M大小文件的分发实验，比较了稀疏编码与完全编码的性能，具体结果见表3-1，结果表明稀疏编码与完全编码的丢块率相差不多。

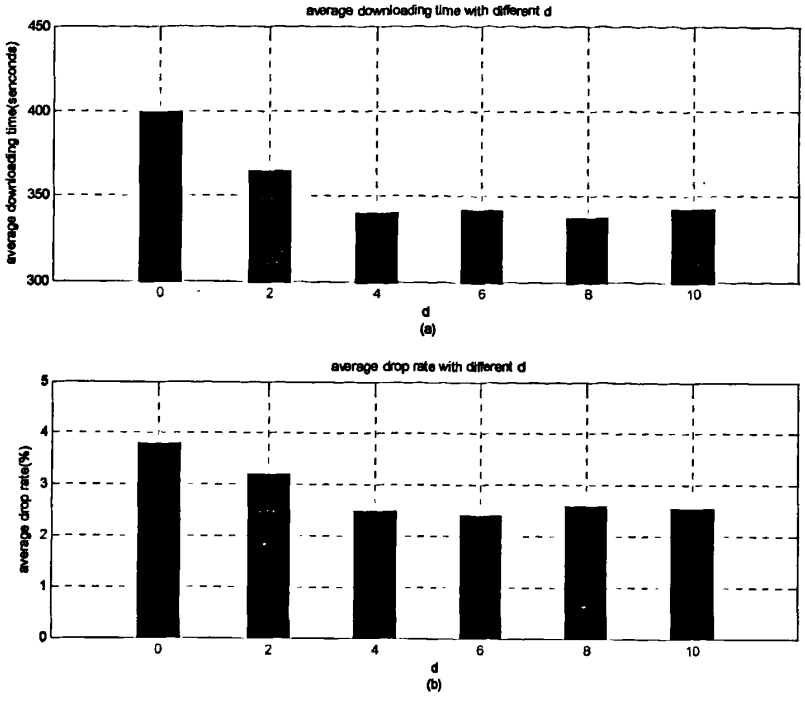


图 3-12 不同编码密度参数 d 下的系统性能比较

(a) 平均下载时间；(b) 平均丢块率

表 3-1 使用稀疏编码（d=10）与完全编码分发 32M 文件时的性能对比

方法	平均下载时间	总分发时间	丢块率
稀疏编码	302.6s	367.8s	2.087%
完全编码	293.8s	369.4s	1.802%

3.2.5.3 编码区间

针对大小为128M的文件，设定分块大小为256KB，$d=10$，仿真实验还对参与分发节点数从8到40不等、使用与不使用编码区间的系统的平均下载时间和丢块率进行了对比，结果如图3-13所示。结果表明，编码区间在节点较多时，确实有效地提高了网络的性能，当参与分发的节点数多于24时，使用了编码区间的系统，其性能（主要看平均下载时间和丢块率两项指标）远优于不使用编码区间的系统。但是在节点较少时，效果不明显，在只有8个节点参与分发时，使用与不使用编码区间的系统性能几乎等同。尤其是当参与分发的节点数为16时，使用编码区间反而使得性能变差。可能的原因是：当节点数较少时，节

点之间有更多的公共邻居，可能会收到较多的线性相关数据块。使用编码区间，编码块被限定在一定的区间内，选中线性相关块的概率更大；而不用编码区间，在拥有的所有数据块中选择，可能会降低线性相关出现的概率。实际应用中，通常都会有比较多的用户同时下载，因此使用编码区间将有助于提高性能。

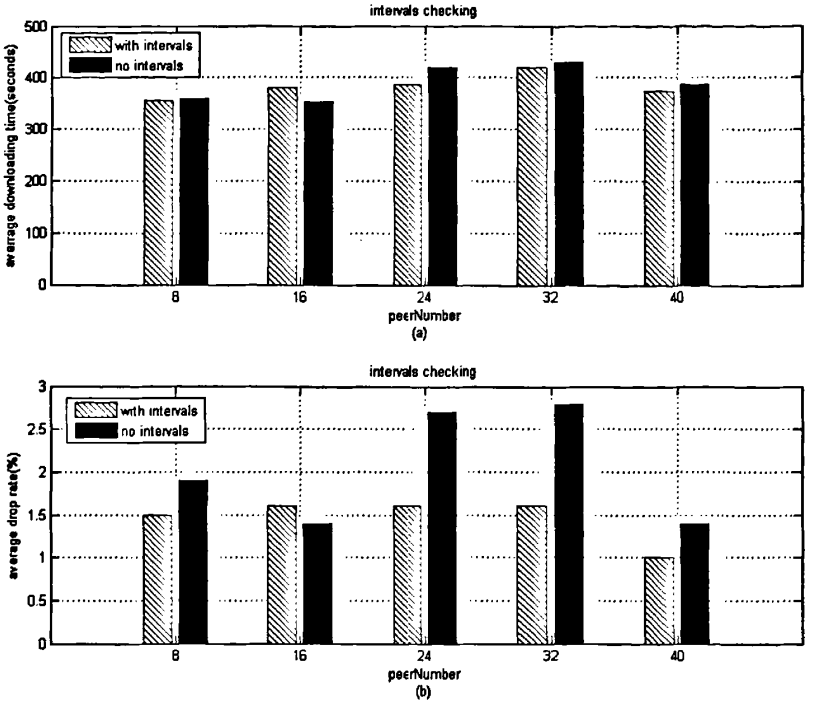


图3-13 不同对等用户数下使用与不使用编码区间的系统性能对比

(a) 平均下载时间；(b) 平均丢块率

3.2.5.4 与无网络编码系统相比较的性能

为了进一步验证网络编码是否能够提高P2P内容分发系统的性能，本文分别在不同分发节点数、不同文件大小以及不同分块大小的情况下，比较了使用了稀疏线性网络编码和无编码的系统性能，比较的指标有总吞吐率、平均下载时间和总分发时间。由于解码工作可以离线进行，因此总分发时间里并没有将解码时间考虑进去。用作对比的无编码系统与有编码的系统结构一致，仅去除了编码的部分。无编码系统使用局部最稀缺优先算法作为分块选择算法。

图3-14显示了在50个节点中分发128MB大小的文件时，使用稀疏编码与无编码系统分别可达到的吞吐率。可以看到，与无编码系统相比，使用了稀疏编码的系统达到了更高的最大吞吐率，并且到达最大值也更快。这是因为相较于未编码分块，节点更容易在编码分

块中获取稀缺分块的信息。这样一来，稀缺分块就不再是编码系统吞吐率的瓶颈了，因此网络编码加快了内容分发过程。

图3-15显示了在40个节点中，分块大小由64KB至1024KB不等，对128MB的文件进行分发的仿真结果。由图中可以看出，当分块大小由64KB增加到256KB时，使用稀疏编码系统的下载时间和分发时间随之变化很小，但是下载时间比无编码系统少了15-20%，分发时间也较无编码系统少了10-15%。对于固定大小的文件来说，分块越小，分块总数就越多，从而系数矩阵的阶数也就越大，而使用稀疏编码和传送分块的开销也会越高。但是随着分块大小继续增加，使用稀疏编码系统的下载时间和分发时间就增加了。与无编码系统相比，当分块大小为512KB时，稀疏编码系统的下载时间和分发时间要小一些，但是在分块大小为1024KB的情况下，反而更大。

图3-16是以固定大小的分块（256KB）来分发不同大小文件（从8MB到256MB不等）时的性能比较。结果表明，在文件不小于64MB时，使用稀疏编码的系统性能要优于无编码系统；而当文件小于32MB时，性能反而变差。当文件增大（$\geq 64MB$），使用稀疏编码的系统性能优于无编码系统。

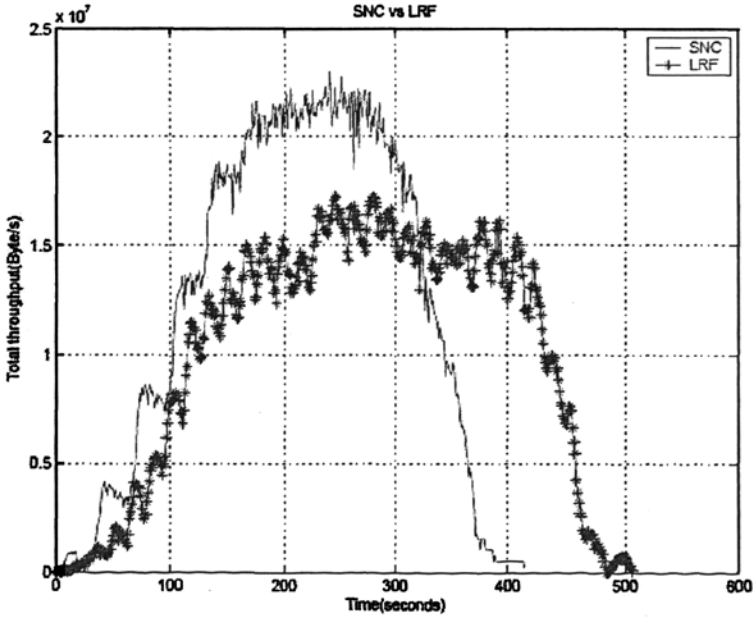


图3-14 使用稀疏编码的系统与无编码系统可达吞吐率的比较

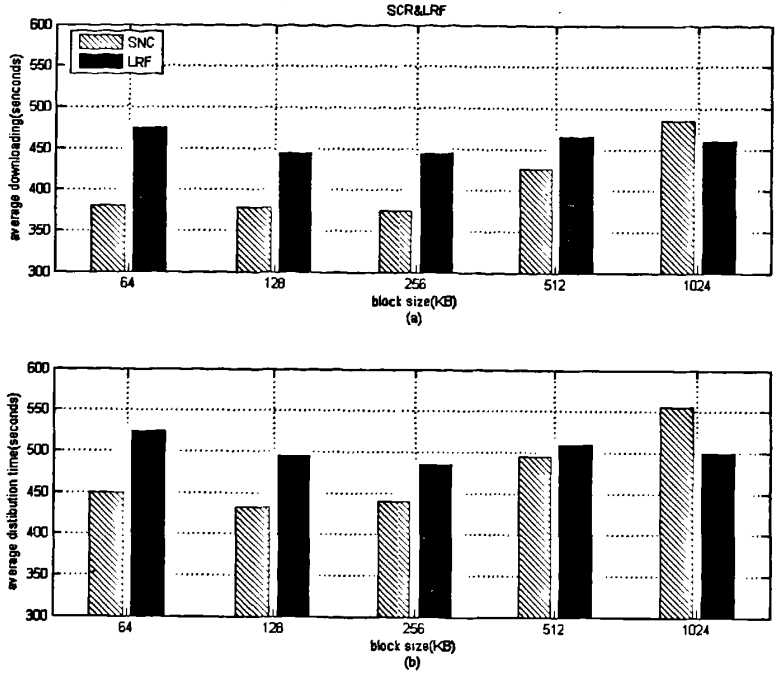


图 3-15 使用不同分块大小分发 128MB 文件的性能比较

(a) 平均下载时间；(b) 平均分发时间

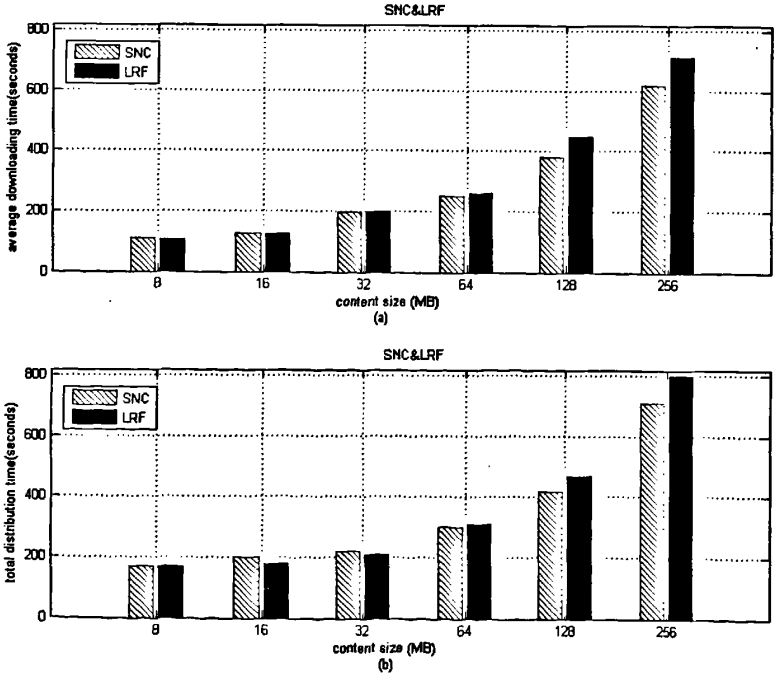


图 3-16 以固定大小的分块分发不同大小文件时的性能比较

(a) 平均下载时间；(b) 总分发时间

3.3 网络编码在安全方面的应用介绍

通过上述章节的研究我们知道，在通信网络和协议中，网络编码提供了一种理论上颇具吸引力的组网概念：通过允许网络的中间节点对多个数据分组进行代数组合来混合不同数据流，能够极大地提高网络的数据吞吐量和鲁棒性。然而，在网络编码大大提高网络各方面性能的同时，也引发了许多颇具挑战的安全问题。这一小节中，我们从网络安全的角度去介绍当前网络编码中的一些热点方向。

为了研究网络编码的安全性，有必要先将网络编码方案分成 2 类：

(1) 无状态的网络编码方案：此类网络编码方案不需要依赖于任何形式的状态信息来决定何时以及如何混合发送队列中的数据分组；

(2) 有状态意识的网络编码方案：此类网络编码方案部分或者完全依靠网络的状态信息（例如邻居节点的缓冲区状态、网络拓扑结构或者链路开销）来计算出网络码或者动态确定实行网络编码的机会。

针对这两类网络编码方案的安全性攻击有很大的不同，这主要是因为后者需要将状态信息和节点身份信息传播到网络中，从而更易受到冒名顶替和控制流的攻击。

3.3.1 实际网络编码方案

3.3.1.1无状态网络编码方案

此类方案的一个典型代表是随机线性网络编码（*Random Linear Network Coding*，RLNC）——一个用来组合不同信息流的完全分布式的方案[2]。RLNC 在 2.3 小节已经提到过了，本文在这里再简要叙述一下其基本原理。网络中的每个节点随机独立地选择一组系数，然后将它所接收到的数据符号（或分组）的线性组合发送出去。图 3-17 演示了中间节点 V 所执行的线性操作（为了简便，我们将系数都设为整数）。符号 x，y 和 z 表示承载了源信息的数据分组，它们会在接收端通过高斯消去法被恢复出来。P1 和 P2 通过中间节点 V 的输入链路到达 V；P3 是 P1 和 P2 在节点 V 的一个随机线性组合，对应的组合系数分别选择为 1 和 2，它通过 V 唯一的一条输出链路被传送出去。

RLNC的全局编码向量（*global encoding vector*），也就是记录有源数据分组从信源到信宿所经历的线性变换的系数矩阵，被存放在数据分组的头部一起传送，以确保接收端能够正确译出源数据。已有研究证明，如果从一个足够大的域中随机选取编码系数，那么接收端就能够使用高斯消去法以极大的概率正确译码[3][4]。另有研究表明，即使是在异步有

损的分组网络中，利用RLNC同样能够使其达到最大容量[5]。

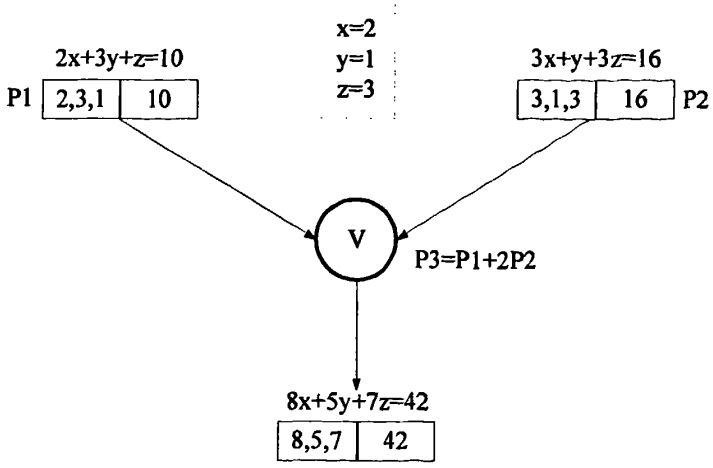


图 3-17 随机线性网络编码（RLNC）实例

3.3.1.2 有状态意识的网络编码方案

有状态意识的网络编码方案需要依靠可利用的状态信息来最优化每个节点执行的编码操作。这个最优化过程可以是以吞吐量为目标，当然也可以将网络延时等性能作为其目标。最优化的范围可以是局部的或全局的，这取决于此最优化的目标是局限于某个节点邻近节点的所有操作，还是针对整个网络的端对端通信。例如，如果邻居节点相互交换控制流的话，每个节点都能够实行局部最优化，及时确定怎样混合并传送接收到的数据分组。一种可以用来实现全局范围最优化的协议的方法是使用网络编码的多项式时间算法[13]。在这种算法中，只要给定网络的拓扑结构，就能够在进行通信之前确定出最优化的网络码。由于利用了无线媒介的广播特性，并在一定的控制方式下传播经过编码的信息，此类有状态意识的网络编码方案在提高吞吐量、对抗节点失效和分组丢失等方面都具有很好的性能。网络在效率方面的增益，主要是因为节点可以利用他们监听到的所有的数据分组；在一些研究中，所需的控制信息的减少同样能够带来效率增益。

此类方案的典型代表则是 Katti 等人提出的一种叫做 COPE 的协议[14]。COPE 协议在 IP 层和 MAC 层之间增加了一个编码层，用来检测编码机会。节点监听并存储在它们发射范围内进行交换的数据分组，然后节点会向其邻居节点发送接收报告，将自己缓冲区中存储了哪些分组告知它们。在不断更新这些信息的基础上，每个节点计算多个数据分组的最佳异或组合，从而减少传输次数。研究表明，这种方法能够使动态网络的吞吐量和鲁棒性获得很大提高。Toledo 和 Wang 等[15]以及 Sengupta 等人[16]分别将路由和网络编码结合起来进行了研究。

3.3.2 安全问题的挑战

上述的网络编码方案需要各个节点正常工作以满足下列规则：

1. 节点正确地将收到的数据分组进行编码，从而获得网络编码带来的预期增益；
2. 节点正确地将编码过后的数据分组进行转发，从而使信宿节点能够正确恢复出所需的信息；
3. 节点自动忽略目标节点并非本身的数据，从而保证最基本的数据保密的要求。

在有状态意识的网络编码方案中，必须多加上一条规则：

4. 节点能够及时参与正确的状态信息的分发，从而为动态网络编码操作提供可靠的信息。

综上所述，我们可以得出结论：出现针对基于网络编码方案的安全攻击，一定是由于一个或多个网络码打破了上述的一个或多个基本规则。

表 3-2 将可能出现的安全攻击以及它们分别对传统网络模式和基于网络编码方案的模式所造成的影响进行了归类。本文重点研究了通信网络中，能够突出网络编码方案在抵抗一些典型攻击上的显著功效的安全攻击。众所周知，每种类型的安全攻击都是针对特定的网络协议规则的。因此在研究安全攻击时，就有必要对上述的无状态和有状态意识的网络编码方案进行区分。

如果对其适当地加以运用，基于 RLNC 的无状态网络编码方案能够更好地抵抗传统路由协议易遭受的一些安全攻击。首先，无状态方案的执行不依赖于拓扑信息或缓冲区状态信息的交换，而这些信息往往是最容易被伪造的（比如通过链路欺骗攻击）；其次，由于无状态方案中，信息通过网络编码方式进行传播，因此这类方案具有内在的健壮性，从而能够减小业务中继拒绝造成的影响；第三，信息的恢复不依赖于节点的身份信息，而仅依靠接收到的数据，这就使得无状态方案能在一定程度上抵抗身份伪装攻击。

与无状态方案不同，有状态意识的网络编码方案需要依赖于节点之间传播的、易受攻击的控制信息来最优化编码操作。一方面，这种特性导致该类方案易遭受产生虚假控制信息的安全攻击；另一方面，控制流信息也可以被用来有效抵抗主动攻击，比如错误分组的注入。对作用于局部范围的方案来说，主动攻击产生的影响只局限于邻近节点；而对于端对端的网络编码来说，这种攻击产生的破坏性要强得多。机会网络编码依赖于邻居节点在无线介质上监听的信息，它显然比一些有线环境下的方案更容易遭受窃听攻击。更一般地说，不管方案是否有状态意识，与传统路由相比，使用网络编码后，恶意（拜占庭）节点将损坏的分组注入信息流所产生的破坏很有可能会更大。由于网络编码会将不同数据分组的内容进行混合，一个损坏的分组很容易就会在任意时刻破坏从发送端到接收端的整个数

据流。

表 3-2 无状态和有状态意识的网络编码方案所遭受的安全攻击及与路由的对比

攻击类型	攻击描述	传统路由方式	无状态 NC	有状态意识 NC
身份伪装	某个节点伪装成另一节点来产生信息	攻击者通过伪装成另一节点来产生路由信息，可以制造相互冲突的路由线路或路由环，从而导致网络分离。	无状态NC方案不依靠节点的身份信息来执行任何操作，因此不受其影响	有状态意识的NC方案需要依靠网络的节点来获取状态信息，因此节点身份被伪装会导致其传达错误的信息。
拜占庭伪造	某个节点产生包含虚假信息的消息	一旦产生了包含虚假信息的路由消息，攻击者就可以致使网络的通信能力退化，并且拦截通信业务。	无状态NC方案在获得的增益以及处理时间上（由于错误分组加入信息流而导致）会受到这种攻击的影响。	有状态意识的NC方案同样会受到这种攻击的影响。例如，如果一个特殊的信息(比如控制流）受到了攻击，而这个信息又可以被用来快速检测此类攻击并阻止伪造的分组在网络中传播。
拜占庭修改	某个节点恶意修改网络中传输的消息	攻击者通过改变传输中的数据分组头部的消息（比如改变其目的节点），可以导致业务瘫痪和拒绝服务。	无状态NC方案中，攻击者可以通过改变传输中的编码分组来对通信网络产生影响。特别是通过改变编码系数或用于产生源分组的有效负载，从而导致源分组无法被译码。	有状态意识的NC方案中，攻击者可以通过改变编码数据分组或控制分组 来破坏通信网络。同样地，在这种情况下，这些控制分组也可以被用来检测并抵抗此类攻击。
拜占庭重传攻击	某个节点向网络中发送“旧”的(之前传送过的）消息	攻击者通过发送“旧”的路由消息，使得过时、冲突或错误的信息进入网络，从而导致错误的路由。	无状态NC方案会由于在信息流中重复传送的错误分组的加入，而受到此类攻击的影响，表现为网络编码所能获得的增益和处理时间受到影响。	有状态意识的NC方案会由于编码数据分组或控制分组被修改而受到此类攻击的影响。同样地，这种情况下，上述控制分组也可以用来抵抗此类攻击。
黑洞攻击	某个节点拒绝帮助其他节点中继通信业务	攻击者能够导致拒绝服务（DOS）和通信状态退化。	无状态NC方案会由于通信能力退化而受到影响。然而，这类方案仍然能够得益于网络编码的内在冗余，从而提高网络的鲁棒性和成功交付的概率[2]。	有状态意识的NC方案同样会由于通信能力退化而受到影响。但是也有可能得益于这种基于网络编码方案的内在冗余。
窃听（内部或外部）	节点与方案很好地合作， 但是这些节点想（非法）获取尽可能多的信息	攻击者通过不同程度地窃听节点将要中继的消息，可以获取不同等级的信息。	如果某个中间节点（或某个窃听者）能够获取足够多的数据分组的线性独立组合，这个节点就能译出这些分组，并获得所有传送的信息。	有状态意识的NC方案同样可能受到窃听攻击。控制流可以被用来抵抗此类攻击，但也有可能反过来加强其攻击性。

3.4 本章小结

在前章介绍网络编码概念的基础上，本章研究了无线网络中网络编码的一些应用及优势。本章首先介绍了网络编码在无线网络中的一些应用，包括基于网络编码的信息交换、网络节能、P2P 内容分发系统以及网络编码在无线自组织网络中的一些应用。之后本章重点研究了基于网络编码的 P2P 内容分发系统，并针对一种特殊的稀疏网络编码，研究了，并对其进行了性能仿真。最后，本章通过分类网络编码方案及其容易遭受的网络攻击，引出了本文将要重点研究的网络编码在安全性方面的应用。具体怎样运用网络编码方案抵抗各种网络攻击，我们将在下面的篇幅中进行详细研究。

第四章 安全网络编码方案研究

在上一章，3.3 节中给出了安全攻击的分类，阐明了网络编码安全方面的弱点，本章研究如何寻找合适的方案来使网络编码更安全，主要包括如何利用网络编码的特性来抵抗各种不同的安全攻击，重点研究抵抗窃听攻击的网络编码方案。对于抵抗拜占庭攻击的方案，我们只简单介绍其原理和进展。为了进一步证明网络编码在安全方面的潜力，本章还对无线传感器网络中基于网络编码的的移动密钥分发方案进行了研究，结果表明，网络编码能为抵御安全攻击增加一道额外的防线。

4.1 抵抗窃听攻击的网络编码方案

本小节研究了三种不同的攻击场景，并针对不同场景提出对抗被动攻击的措施。首先，我们考虑一些不具攻击性但想获取非法信息的节点（Nice but curious nodes），这些节点的操作仅违反上述四条规则中的第三条，即节点不会自动忽略目标节点并非本身的数据。第二种情况是窃听者可以窃听某些链路上传送的信息的攻击场景。由于定理的证明比较复杂，我们将其单独列为一章，在下一章对其进行详细研究，在前人研究工作的基础上，提出一种改进的安全网络编码方案，并进行性能分析和验证。最后一种场景是最坏情况下的窃听，窃听者能够获取网络中所有通信中的信息。

4.1.1 网络存在恶意窃听节点

首先考虑这样一个安全威胁模型：网络完全由不具攻击性但想获取非法信息的节点组成，也就是说，这些节点完全按照通信协议正常工作，但总是想从经过它们的通信数据流中获取尽可能多的信息（很有可能是带恶意的）。在这种场景下， RLNC 方案本身就具有一定的安全性[17]，因为在很多实际网络中，由于编码字母表的大小和网络的拓扑结构的限制，中间节点具有足够的自由度去执行高斯消去法，从而获取被传输的数据集的可能性很小。

基于上述结论，就可以根据[17]中定义的代数安全标准将由中间节点引发的安全威胁的等级进行分类，这种代数标准考虑到了中间节点接收到的全局编码向量的元素个数。如图 4-1 所示（为简便起见，系数都选择为整数），上面第一个传输方案（未经过编码）会将数据泄露给中间节点，使得部分数据无法被保护；而下面第二种经过网络编码的方案中，

中间节点 2 和 3 则无法获得传输中的数据符号，可以认为是代数安全的。

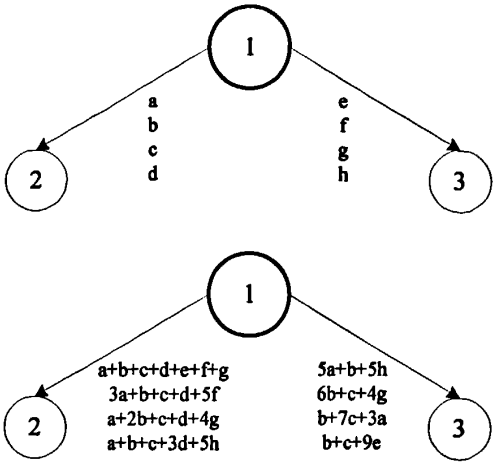


图 4-1 网络编码具有的代数安全实例

4.1.2 最坏情况下的窃听

本小节针对最坏情况下的窃听问题进行研究，这种情况下的攻击者能够获取网络中传送的所有数据分组，但不包括合法通信用户所共享的密钥。针对这种攻击，我们利用 RLNC 内在的安全特性，采用 2.4 小节中提到的一种改进的 RLNC 方法—实际网络编码（PNC）来构造一个低复杂度的加密方案，以减少保密通信所需的加密操作的总量。方案的原理是：只需加密信源处产生的用于译出线性编码数据的系数（即锁定系数），而允许中间节点使用未加密的系数（即未锁定系数）去执行网络编码操作。这些未经加密的系数并不会威胁到数据的保密性，而且它们存储着数据分组在网络中所经历的操作（变换）。

4.1.2.1 网络模型和假设

要构造加密方案，我们首先需要对网络模型、网络编码模型以及攻击模型进行描述。

(1) 网络模型

假设网络的信源节点和中间节点都能够知道信宿节点的标识符（例如 IP 地址），这样构造出来的方案就能够很容易地应用到许多具有相同特征的网络中去，尤其是无法获取网络拓扑结构或者编码函数的集中信息的网络。同时我们还假定信源、信宿节点共享对称密钥，根据需要来加密数据。共享密钥的交换可以用很多方案实现，比如用于密钥预分配的离线机制，诸如 Kerberos 或者公钥基础设施(*Public Key Infrastructure*，PKI)的鉴权协议等。

(2) 实际网络编码（PNC）

Chou等人在2003年提出了一个分组化的网络编码结构－实际网络编码（*Practical Network Coding*, PNC）[6]，这是一种改进的随机网络编码方法，综合了RLNC对于分组丢失、网络阻塞、网络拓扑结构改变等破坏的抵抗力，确保了数据在高度动态网络中以最小的控制信息代价进行健壮传输。在PNC方案中，定义了一个分组格式和一个缓冲模型。分组格式将‘全局编码向量放置在其数据分组的头部。数据分组的有效负载根据域的大小（比如2^8或2^{16}，即每个符号分别用8或16个比特表示）被分为多个向量。然后，节点会将这些符号当作分块来执行线性操作。

PNC中的缓冲模型将数据分组流分割成许多*Generation*，每个*Generation*的大小都为h，这样一来，处于同一个*Generation*中的分组都被标记上一个共同的*Generation*号，而网络中的每个节点都会根据接收到的分组的*Generation*号将这些分组分类存放于一个缓冲区。当一条输出链路上有传输数据的机会时，将要发送数据的节点会产生一个新的数据分组，这个分组是缓冲区中所有属于当前*Generation*的分组的随机线性组合。如果一个分组并不承载任何新的信息，即此分组不能增加接收端译码矩阵的秩，那么这个分组立即被丢弃。只需等到宿端接收到的数据分组的矩阵一满秩，就可以使用高斯消去法恢复出源数据分组。

(3) 攻击模型

我们考虑的最坏情况下的窃听者特征如下：

(a) 窃听者能够观察网络中的所有传输；

(b) 窃听者知道通信中使用的编码和解码方案；

(c) 窃听者计算受限，因此无法破解传统密码学中的加密操作；

(d) 窃听者能够任意丢弃或删除网络中的数据分组（流量中继拒绝）；

(e) 窃听者能够任意向网络注入新的流量，从而引入伪造的分组，导致系统分集性和健壮性的降低。

本文下面主要研究抵抗攻击(a)-(c)的安全方案。

4.1.2.2 加密方案

这里我们具体研究抵抗最坏情况下窃听的安全网络编码方案。此方案将网络编码内在的安全特性与标准加密方案结合起来，以达到抵抗上述攻击的目的。方案针对基于RLNC的实际网络编码方案，在发送端和接收端进行了改进。在此我们定义两种类型的系数：(1)未锁定系数，一般是编码过的数据分组所对应的单位矩阵的某一行；(2)锁定系数，实际上是用于编解码操作的系数，需要被密钥加密（密钥在接收端共享）。将未锁定系数和锁定系数连接起来，并在新数据分组产生的时候加到其头部。所有系数（包括加密和未加密的）

都要按照基于RLNC的网络编码算法的数据融合规则经过中间节点的处理。也就是说，此方案不需要改变中间节点遵循的规则。要实现这一点，就必需使用输出密文与明文长度相等的加密系统来加密锁定系数，比如高级加密标准AES（*Advanced Encryption Standard*）。有了上述前提，本章研究的方案就具有很大的优势，因为对一个*Generation*中的每个数据分组都只需进行一次系数加密。在信宿节点处，起主要作用的是未锁定系数，因为它们存储了网络中对锁定系数进行的操作。只有对这些操作进行了逆操作，信宿节点才能对锁定系数进行解密，从而获得被隐藏的信息。

这里需要强调的是，未锁定系数在锁定系数未被解密的情况下，是不会泄露解码数据分组的信息的－它们仅能用来判断数据分组之间是否线性独立，并被用来完成原来的基于RLNC的网络编码方案。此外，有效负载中的每个符号都是用随机系数进行线性组合而产生的，而这些随机系数在这个方案中是要被加密的，窃听者无法得到，所以网络中的有效负载在此处考虑的攻击下是安全的。

如上所述，除了加密机制的一般要求（例如效率和强安全性），此方案所用的加密机制还必需满足另一个要求，即输出密文须与明文等长。这样就使得中间节点可以在没有解密密钥的情况下，直接对锁定系数进行操作。作为示例，这里首先假设符号都用8比特表示（有限域大小为2^8）。对于某个*Generation*（大小为h）中发送的数据分组来说，h个系数相连，构成一个h字节的明文字符串。对该系数字符串整体进行加密后，就产生了一个h字节的密文。随后，密文被分为h个8比特的分组，每个分组对应于一个将被加入数据分组传送的锁定系数。为了更好地对原理进行阐述，本文用图4-2表示了该方案实现的具体过程，数据分组的白色部分代表未经加密的信息，而加密过的信息则用灰色部分表示。在实际应用中，灰色部分里的初始锁定系数(3,2)和(5,1)被加密成为了等长的其他符号。为了叙述方便，此方案中的系数都选为整数。

具体步骤如下：

（1）信源节点 1 随机产生 2 个系数 ，并将其用满足前述条件的加密机制进行加密，密钥与信宿节点 6 和 7 共享。而每个分组对应的未锁定系数则被用来检验分组是否线性独立，以及用来实现常规的网络编码方案；

（2）中间节点对数据分组执行常规的线性组合（例如节点 4 将从节点 2 和 3 接收到的分组用编码向量(1,1)进行组合）。中间节点并不区分锁定系数和未锁定系数，它们对这些系数执行统一的操作；

（3）当信宿节点 6 和 7 接收到足够的信息之后，它们便开始用自己所知道的线性变换的信息来恢复原来的锁定系数，这些信息都保存在未锁定系数中。接着，便将锁定系数解密，

计算其与未锁定系数的乘积。最后，信宿节点执行高斯消去法，恢复源数据分组。

表4-1对此方案进行了详细总结。

表 4-1 安全方案总结

1. 初始化（信源节点处）： → 使用密钥管理机制与信宿节点交换共享密钥，该密钥被用来加密锁定系数； → 信源节点将信息分组$w_1,w_2,\ldots,w_h$存储到其内存中； → 信源节点在内存中产生这h个信息分组（当前*Generation*中的）的一个随机线性组合，并将其放入一个数据分组中，等待发送； → 将对应于$h\times h$单位矩阵某一行的系数加入每个编码过的分组的头部。这些系数就是前面提到的未锁定系数； → 数据分组的全局编码向量被共享密钥加密，并且被放置在每个分组的头部。这些系数就是前述的锁定系数。
2. 中间节点的操作 → 当接收到一个数据分组时，节点将其存储到自己的内存中； → 为了在输入链路传输数据，节点对其缓冲区中的数据分组进行线性组合，从而产生一个新的数据分组，根据基于标准RLNC方案的规则对未锁定和锁定系数进行统一操作。
3. 解码（信宿节点处） → 当信宿节点接收到足够的数据分组时： • 接收端使用未锁定系数（存储了锁定系数在传输过程中经历的操作），将网络中对锁定系数所作的操作逆反，从而得到原来的锁定系数； • 接收端解密上一步中得到的锁定系数； • 接收端通过计算未锁定系数与对应锁定系数的乘积来获得译码矩阵； • 接收端执行高斯消去法，恢复出信源数据分组。

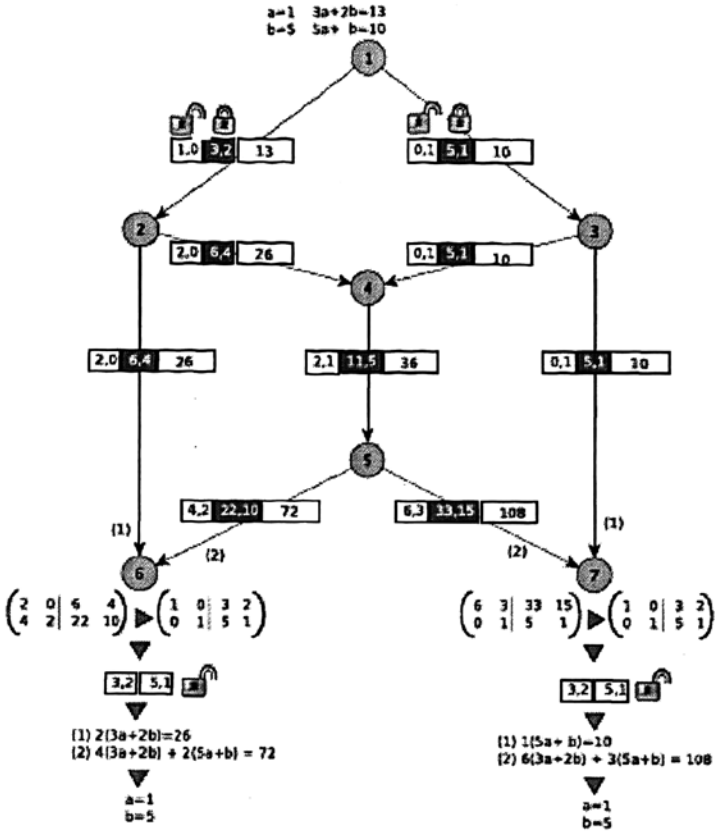


图4-2 抵抗最坏情况下窃听的安全方案

4.1.2.3 性能分析

本章节从加密数据的总量、所需空间及其计算开销三个方面来评价上述方案的性能。

(1) 加密数据总量

为了将上述方案与传统端对端加密方案的效率进行对比，图 4-3 比较了不同明文长度下 2 种方法所需加密的数据总量。假设网络负载最大为 1480 字节（以太网的标准大小），并且每个被上述方案编码过的 *Generation* 都有 h 个编码分组。在使用传统加密机制（对整个网络负载实行端对端加密）的情况下，必需加密的数据总量随着被加密的负载的大小而线性增加。我们不难看出，由于仅需要对锁定系数进行加密，上述方案大大减小了需要加密的信息总量（无论系数表示为 8 比特或 16 比特），而仍然能够保证网络负载的高度机密性。

这里需要注意的是，由于只有当负载长度（大小）超过一个标准 IP 分组的最大负载长度时，才会需要产生新的 h 个锁定系数，并将其包含在下一个 IP 分组中，因此上述方案中需要加密的信息总量是呈离散状态增加的。如果我们考虑比标准 IP 分组的最大负载长度

（1480 字节）更长的 IP 分组，上述方案的相关增益将比这种标准情况更大。这是因为此时分组可以携带发送更多的数据，而分组所包含的锁定系数集是相同的。

一般来说，所需的加密操作的总量与上述需要进行加密的数据总量直接相关。如果考虑一个序列密码，加密时执行的操作量随其总量而线性增加，因此正如图 4-3 所示，上述方案大大减少了加密操作的数量。在分组密码（如 AES，其分组长度为 128 比特）的情况下，每个加密操作至多允许 128 比特的输入数据，即 16 个来自 2^8 大小有限域中的系数，或 8 个来自 2^{16} 大小有限域中的系数。

(2) 所需空间

这个方案中，减少加密数据是以在分组中存放锁定系数为代价的。假定使用一种明文与密文长度相等的加密机制（例如序列密码模式的 AES），传输一个含有 h 个编码分组的 *Generation* 的总开销就取决于 IP 分组的最大长度。

表 4-2 显示了该方案为每个数据分组引入大小为 8 或 16 比特的系数所需的开销。表中的开销值是通过计算锁定系数长度与一个 IP 分组的最大长度之间的比例得出的。随着参与编码的分组数量 h 的增加，分组开销也随之增加，这是因为每增加一个新的分组参与编码，将需要向 IP 分组中增加一个新的锁定系数。对于 h 很大的情况，上述开销将会变得非常大，尤其是当 IP 分组长度较小时。例如，编码 200 个分组，而 IP 分组最大长度为 1500 字节（包括 20 字节的分组头部），这种情况将导致开销为 13.3%（有限域大小为 2^8）或 26.7%（有限域大小为 2^{16}）。然而，这个开销可以通过增加数据分组长度来减少。如表中所示，同样是编码 200 个分组，对于大小为 2^8 和 2^{16} 的有限域来说，通过增加分组长度，开销就可以分别降为 2.4%和 4.8%。

(3) 计算开销

由于在数据分组中包含了附加的系数集（锁定系数），上述方案在网络节点处引入了一般基于RLNC的方案中不存在的额外操作。对应的计算开销对于信源节点、中间节点和信宿节点来说是不同的。为了分析简便，我们在这里假定与乘法操作相比，加法操作的复杂度可忽略不计。同时，我们将矩阵相乘的复杂度规定为$O(n^3)$（以最通用的方法实现矩阵相乘，需要$O(n^3)$次操作）。尽管存在更为简单，计算复杂度更低的算法（通常只运用于大型矩阵），但它们对上述方案产生的差异并不大，可忽略不计。

表4-3对上述方案在不同类型节点处引入的计算开销进行了详细的评估。

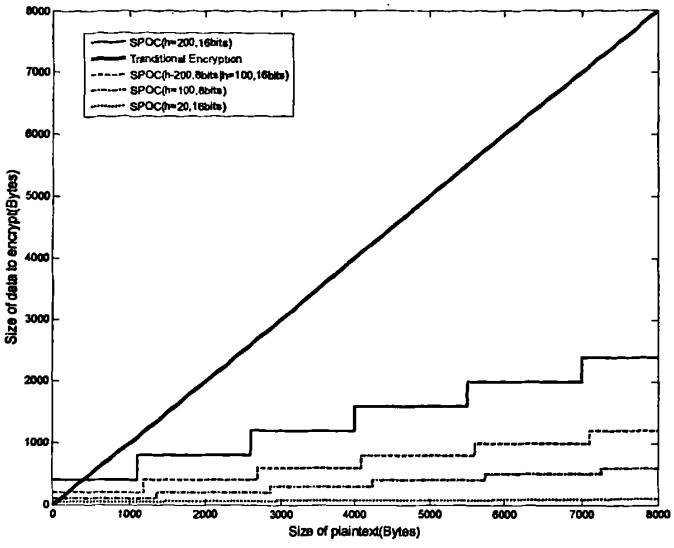


图4-3 传统加密方案（对所有数据加密）与本文方案所需加密的数据大小的比较

表 4-2 锁定系数在总体数据中所占比例（每个分组）

IP 分组最大长度	参与编码的分组数目 h	不同大小有限域（F_q）时的开销 $q=2^8$	$q=2^{16}$
1500	20	1.3%	2.7%
	50	3.3%	6.7%
	100	6.7%	13.3%
	200	13.3%	26.7%
5000	20	0.4%	0.8%
	50	1.0%	2.0%
	100	2.0%	4.0%
	200	4.0%	8.0%
8192	20	0.2%	0.5%
	50	0.6%	1.2%
	100	1.2%	2.4%
	200	2.4%	4.8%

表 4-3 引入锁定系数的计算开销（针对每个大小为 h 的 *Generation*）

节点	操作	具体开销	总开销
信源节点	产生单位矩阵向量	可忽略不计	$O(h^2)$
	加密要保密的系数	见本小节	
	执行随机线性操作	h^2 次乘法和 $(h\text{-}1)h$ 次加法操作	
中间节点	执行随机线性操作（将 n 个数据分组进行组合）	nh 次乘法和 $(n\text{-}1)h$ 次加法操作	$O(nh)$
信宿节点	将未锁定系数矩阵 M_U 逆转 $\rightarrow M_U^{-1}$	$O(h^3)$	$O(h^3)$
	将锁定系数矩阵 $\hat{M}_L$ 与 M_U^{-1} 相乘 $\rightarrow M_P = M_U^{-1} \times \hat{M}_L$	$O(h^3)$	
	解密锁定系数，得到原系数矩阵 M_L	见本小节	
	$M = M_U \times M_L$ →获得最终的矩阵，并据此执行高斯消去法	$O(h^3)$	

4.2 抵抗拜占庭攻击的网络编码方案

尽管拜占庭攻击对经过网络编码后的信息完整性破坏很大，我们还是可以运用线性网络码特有的属性来有效抵抗业务中继拒绝或错误分组注入带来的破坏。RLNC 已被证明对由节点的恶意行为引入的分组丢失具有很强的鲁棒性[5]。还有一些更为复杂的抵抗策略，需要对编码后数据分组的格式进行改变，主要分为 2 类：(1)端对端纠错；(2)恶意行为检测。这些方案都可以经由逐个分组的模式或基于 *Generation* 的模式来实现。

4.2.1 端对端纠错

端对端纠错码的主要优势在于，运用差错控制技术给网络带来的负担完全交给了信源端和信宿端，如此一来，中间节点就不需要改变它们的工作模式了。一个典型的用于端对端网络编码的传输模型可以用一个矩阵信道 $Y = AX + Z$ 表示，其中 X 表示以传输的分组为行向量的矩阵；Y 是以接受到的分组为行向量的矩阵；Z 表示经网络传播后，注入的错误分组所对应的矩阵；A 描述的是系统转移矩阵，与数据分组经过网络时，作用于它们的全局线性变换相对应。从性能角度来看，纠错方案可以纠正信源与信宿之间的至多相当于最小割数量的错误。在这种场景下，Koetter 和 Kschischang[27]提出了一种基于 RLNC 的 Rank-metric 纠错码（秩度量纠错码），其研究结果被 Silva 等人拓展到信道可以提供差错的部分信息的情形下[28，29]。这里所说的差错的部分信息可以是 *Erasures*（指只是知道差错的位置，而不知道具体的值）和 *Deviations*（指只是知道差错的值，而不清楚差错的具体位置）的形式。仍然是基于同样的场景，Silva 等人[30]又研究了一种概率差错模型下的随机网络编码，计算了其容量界限，并提出了一种简单的、具有多项式复杂度的编码方案，使该随机网络编码方案在同时考虑分组长度和域大小的前提下，仅以指数级低的失效概率达到容量。Montanari 和 Urbanke[31]扩展了 Koetter 和 Kschischang 在[27]中所做的工作，基于随机稀疏图提出了一个纠错方案，同时又为一种概率差错模型提出了一个低复杂度的译码算法。Cai 和 Yeung 在[32]中给出了有差错通信环境下最大可达速率的界限，并在此基础上获得了 Hamming 界限和 Gilbert-Varshamov 界限的网络推广。

Jaggi 等人也研究了一种与上述方案稍有不同的网络纠错方法[33]。他们提出了一种具有多项式时间复杂度的、可以在发生主动攻击的情况下达到最佳速率的健壮网络码。这种方案的基本思想是，把对手节点注入的数据分组当作第二种信息来源，并加入足够的冗余信息，使得信宿节点能够区分有用的和错误的数据分组。这种方案所能达到的容量不仅取

决于攻击者获取信息的速率，还取决于信源和信宿之间共享的信息。Nutman 和 Langberg 将上述研究工作进行了拓展[34]，他们在[33]的基础上又引入了 3 种攻击模型，并得出了每个模型的最佳速率$C-z$，其中C是网络容量，z则是被攻击者控制的链路数量。

4.2.2 恶意行为检测

基于*Generation*的检测方案通常具有与网络纠错码相似的优势，因为检测由拜占庭攻击引入的分组修改这类计算代价较大的任务，是由信宿节点来完成的。基于*Generation*的检测方案，其最大劣势在于只有拥有一个*Generation*中足够多分组的节点才能检测出恶意修改，因而使用这类方案会导致较大的端到端延时。针对这个问题，Ho等人[4]提出了一种用于检测拜占庭攻击的信息理论框架。其最基本的假设是攻击者无法得知网络中其他所有分组的信息，从而无法利用这些信息来制造恶意修改的分组。他们证明了可以使用一种具有多项式复杂度的哈希方法，这样就不需要再进行密钥分发。

基于分组的检测方案的核心思想是，网络中的一些中间节点能够即时检测出被破坏的数据，并将有关的数据包丢弃，从而只会中继正确的数据。然而，基于分组的检测方案需要中间节点的主动参与，并且取决于通常计算代价较大哈希函数。当然，我们还可以通过使用基于同型哈希函数的签名方案来降低这种类型攻击的破坏性。同型哈希函数非常适合于网络编码方案，因为如果使用该种哈希函数，一个编码分组的哈希值就可以很容易地由之前的编码分组得到，从而使得中间节点能够在用代数方法混合数据分组之前，就验证编码分组的正确性。但是，同型哈希函数的计算代价仍然很大。

Charles等人[35]为网络编码提出了一种基于椭圆曲线密码学Weil对的同型数字签名方案。Krohn等人[36]还针对组播通信，在对等内容分发的环境下，将同型哈希函数与无比率限制纠错编码（Rateless Erasure Codes）结合起来进行了研究。为了防止浪费大量带宽以及破坏网络客户端的下载缓存，每个文件被压缩至一个较小的哈希值，接收者可以利用它来检查下载分块的完整性。除了与编码速率相独立，此过程的最大优势还在于当文件较大时，其计算代价相对于传统的转发纠错码（比如Reed-Solomon码）来说较小。

Gkantsidis和Rodriguez在[37]中针对基于网络编码的文件分发，提出了一种协作安全策略，用于对注入对等网络中的恶意分块进行即时检测。为了减少即时检验信息的代价，同时有效阻止恶意分块的传播，他们提出一种分布式体制，每个节点各自以一定概率检查分块，当发现可以分块时，及时通知邻居节点。另外，他们还研究了预防拒绝服务（DOS）攻击的技术。

Zhao等人所发表论文[38]的基本思想，是利用在线性网络编码中，任何传送中正确的数据分组都属于由原向量集合张成的子空间。因此，他们使用了一种签名方案来检查某个分组是否属于它的原子空间。他们证明了要使一个不属于该子空间的签名通过分组检查是几乎不可能的。

Kim等人[39]将拜占庭纠错和各种基于网络编码的检测方案所需的带宽开销进行了比较。他们将中间节点分为普通节点和信任节点两类，只有信任节点才能获取拜占庭检测方案使用的公钥。在这种设定下，Kim等人证明了当攻击概率很高时，基于分组的检测是最好的；而当攻击概率较低时，基于*Generation*的方式对带宽利用更加有效。

4.3 无线传感器网络中的密钥分发方案

如果要确保密码学上的安全，能否以一种安全的方式分配密钥显然是最基本的一项要求。在高度受限的移动 ad-hoc 网络和传感器网络中，密钥的预分配方案[40]要优于其他方案，这主要是因为此类方案所需的计算量和通信资源大大少于信任方策略[41]以及公钥体系[42]。其主要的不足之处在于只能以一定概率完成安全互连，也就是说，如果某个节点拥有了足够多的密钥（在一个固定集合内随机生成），那么这个节点就可以较高的概率与它的每个邻居节点共享至少一个密钥。Oliveira 等人[43]通过研究证明，网络编码可以成为在低复杂度传感器节点之间建立安全连接的一个有效工具。与单纯的密钥预分配方案相比，此方案中的移动节点（例如一个手持设备或笔记本电脑）能够激活网络，并且帮助建立节点间的安全连接。研究表明[43]，利用网络编码的优势，我们可以设计出一种密钥分配方案，它只需要用到少量预先存储的密钥，但仍然可以确保以概率 1 建立共享密钥连接，并且移动节点并不知道分配的密钥。这个方案的基本思想如图 4-4 所示，传感器节点 A 和 B 想要通过一个移动节点 S 交换 2 个密钥。在该过程中，S 首先将 HELLO 消息进行广播。收到这个消息之后，每个传感器节点回送一个密钥标识符 $i(\cdot)$ 作为响应，$i(\cdot)$ 对应于该节点的密钥 $K_{i(\cdot)}$。然后，节点 S 将密钥 $K_{i(A)}$ 和 $K_{i(B)}$ 的异或值进行广播。一旦该过程终止，传感器节点 A 和 B 就可以用 $K_{i(A)}$和 $K_{i(B)}$这 2 个密钥与对方通信了（一个方向上只能传送一个消息）。注意，这里 $E_{K_{i(A)}}(m_{A\to B})$表示一个由 A 发送至 B、用 $K_{i(A)}$ 进行加密的消息，而 $E_{K_{i(B)}}(m_{B\to A})$ 则表示一个由 B 发送至 A、用 $K_{i(B)}$ 进行加密的消息。

在这里，本文将其总结成如下步骤：

(1) 配置传感器节点之前：

(a) 有一个包含 N 个密钥的集合 P，离线产生这些密钥对应的 N 个标识符；

(b) 从 P 中随机产生一个包含 L 个密钥的不同的子集，并将其对应的 L 个标识符装入每个传感器节点的内存中；

(c) 用 N 个密钥和 N 个序列创建一张表，这 N 个序列由每个密钥与共同的保护序列 X 之间的异或作用产生。

(d) 将上述表格存入移动节点的内存中。

(2) 配置传感器节点之后：

(a) 移动节点广播消息“HELLO”，该消息在其无线发射范围内被任何传感器节点接收；

(b) 每个传感器节点以一个密钥标识符来响应；

(c) 根据接收到的密钥标识符，移动节点开始查找对应的被 X 保护的序列，然后将它们通过一种异或（XOR）网络编码操作组合起来，因此消除了 X，同时获得了对应密钥的异或值；

(d) 移动节点对得到的异或序列进行广播；

(e) 通过将接收到的异或序列与它们各自的密钥组合起来，每个节点可以轻易地恢复其邻居节点的密钥，因而可以共享一对对移动节点保密的密钥。

尽管这里所使用的网络编码受限于异或操作，但是可以通过使用存储密钥的线性组合来得到一种更有效的密钥分配方案。

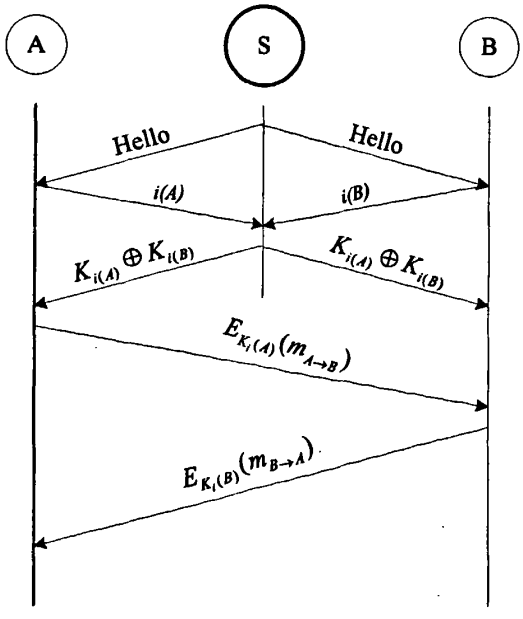


图 4-4 传感器网络中基于网络编码的密钥分配方案

4.4 本章小结

本章主要研究了抵抗各种安全攻击的网络编码方案，根据当前本领域的研究现状，本文研究的攻击主要包括窃听攻击和拜占庭攻击。网络编码有许多内在特性，而其中最主要的一点就是数据分组与多条路径上的信息分发可能性之间的代数依赖性。利用这一点，我们可以构造出更加简单的密钥分配方案或窃听攻击下的保密通信方案。由于运用网络编码而引起的最严重的安全问题，来自不同种类的拜占庭攻击，这类攻击以控制流或网络码本身为攻击目标，因此需要与目前一些方案相比，更为复杂的解决方案。然而，在这一领域中，还有许多问题尚待解决，例如怎样构造及维护拜占庭攻击（针对网络编码）下的健壮网络的拓扑[44]；怎样将网络编码和原始的密码学方案最有效地结合起来；怎样将网络编码的特性应用到匿名通信中（例如[45]中提出的信息分层方法），以及怎样利用网络编码去进行安全多端计算。近年来，网络编码方案层出不穷。针对上述的一些考虑，网络编码安全领域的研究将会越来越活跃。

第五章 抵抗窃听攻击的网络编码方案研究

针对网络编码安全性的问题，研究者还提出了一种不同的模型，该模型假设存在一个或多个可以获取部分通信链路信息的外部窃听者（窃听器）。应对这类安全问题的核心，就是要构造出一组能够以某种方法将数据“分裂”到不同通信链路上的网络码，使得攻击者很难或无法重构信息。本章要研究的就是在这种存在外部窃听节点的情况下，如何运用网络编码来抵抗此类攻击。与上一章中基于实际网络编码（PNC）来抵抗最坏情况下窃听攻击的安全方案不同，本章使用向量空间角度构造的线性网络编码来抵抗窃听节点的攻击。在本章中，作者还在文献[18]的基础上提出了一种改进的安全网络编码方案，并验证了它的安全性和可达性。

5.1 线性网络编码模型和窃听模型

5.1.1 线性网络编码模型

为了简化对问题的分析，我们主要集中讨论一类无延时、非循环的单信源多信宿组播通信网络。组播通信网络的任务是将信源处产生的信息传送到每个信宿。Li 和 Yeung 已经在[46]中证明了线性网络码足够使组播网络达到最大容量，那么我们就以他们的线性网络码模型为基础来构造安全网络码。本文在第二章中已经介绍过从向量空间角度构造的线性网络编码的原理和实现，为了便于理解将要讨论的安全网络编码方案，本小节再简要描述一下该线性网络编码的模型。

上述的组播通信网络可以用三元组(G,S,T)来表示，其中 G 代表与实际网络具有相同结构的有向图，S 是该通信网络中唯一的信源，而 T 是信宿的集合。有向图 G 还可以写成二元组(V, E)的形式，其中 V 是有向图中所有节点的集合，而 E 是所有的边集合。G 中的有向边可用来传递数据，所有的边都具有单位容量，即每单位时间传送 1 比特信息。

为构造网络码，我们将方案中所有的运算和数值都限制在有限域$GF(q)$中，有限域大小 q（阶）是其特征 p (素数)的幂，即 $q = p^m$。有限域$GF(p)$的扩展域亦可表为$GF(p^m)$或$GF^m(p)$，因此有限域$GF(q)$也可称为有限域$GF(p)$的扩展域，而 p 则是有限域的特征值。需要指出的是，在由通信网络抽象成的有向图中，我们将会用 $tail(e)$来表示边 e 的尾节点

（即 e 的起点），而用 $head(e)$表示边 e 的头节点（即 e 的终点）。

定义 5-1：一个定义在 $G=(V,E)$ 上的 n 维线性网络码，是对 G 中的每条边 $e\in E$ 分配一个向量 $l(e)$，称为“全局编码核”（*global encoding kernel*），使其满足：

1. 分配给信源 S 的向量空间为 $s(S)=GF^n(q)$，即一个 n 维向量空间；

2. 分配给信道（边）$e\in E$ 的向量 $l(e)$，必须是所有到达节点 $tail(e)$ 的边上向量的线性组合；若 e 的尾节点是信源 S，则 e 上的向量从 $s(S)$中选取；

3. 在每个信宿节点上，必须有能够恢复信源信息的特定函数操作。

我们用 $s(X)$表示节点 X 的向量空间，并注意到对于任何非源节点 X，$s(X)$是到达 X 的所有边上向量的所有可能线性组合的集合。因此可以很容易判断出，对于任意 $e\in E$，有 $l(e)\in s(tail(e))$。如果 $tail(e)$是源节点 S，那么分配给边 e 的 n 维向量应从 $GF^n(q)$中挑选；如果 $tail(e)$是非源节点，那么分配给边 e 的 n 维向量就应该是分配给 $tail(e)$所有输入链路的向量的线性组合。这就是“确定网络编码”，这种方案需要知道网络的整体拓扑结构。此外，在信道 XY 上传递的数据是 n 维信源信息的行向量与特定网络编码方案分配给每条边的 n 维列向量 $l(XY)$的乘积。注意，根据组播通信网络的最大流限，只有信源 S 与每个信宿之间的最大流都大于等于 n 时，数据才能使用上述网络编码，以速率 n（比特每单位时间）在网络中传送。

5.1.2 窃听网络上的通信系统（窃听攻击模型）

Cai 和 Yeung[18]针对外部窃听问题，提出了一个窃听网络上的通信系统模型（*Communication System on a Wiretap Network*，CSWN）。接下来我们就对这个模型进行介绍。

一个 CSWN 由下列几项元素构成：

(1) 多重有向图 G：二元组 $G=(V,E)$ 被称为多重有向图，其中 V 和 E 分别是 G 的节点集和边集。在这个模型中，假设 G 是无环的，即 G 中不包含有向环。

(2) 源节点s：节点集V中包含一个源节点s，它产生取值于字符集$\mathcal{M}$的随机消息M。

(3) 用户节点集U：如果V中的一个节点，它能够完全被需要以零差错接收随机消息M的合法用户所获取，这个节点就叫做用户节点。 通常一个网络中都会有不止一个的用户节点。用户节点的集合用U表示。

(4) 被窃听的边集的集合 λ：某个攻击者能够获取网络中一个边集（其中最多有k条边）上

传送的所有信息，并将这个边集构成的集合定义为λ。λ中的每个成员（边集）的信息都有可能被窃听者窃取，但窃听者每次只能窃取λ中一个成员中传送的信息。如果用ψ来表示λ的成员，那么$|\psi|\le k$。

由上可得，我们将四元组(G,s,U,λ)称为窃听网络上的通信系统（CSWN），用多重图G来表示一个网络，并用边集E中的边代表信道。我们的任务是要设计一个安全网络编码方案，保障传输系统在存在上述窃听者的情况下，不会向其泄露任何源信息，达到信息论中的完善保密，亦即无论攻击者获取了λ中哪个成员中传送的信息，他仍然无法得知源信息。

5.2 反窃听的安全网络编码模型

针对上述窃听攻击，Cai 和 Yeung[18]提出了一种安全网络编码方案，构造如下：首先，对原来的线性网络码进行特定的线性变换，即将原网络码分配给每条边的向量$f_e(e\in E)$变为$f_e'=Q^{-1}f_e$，这也就是构造出来的新的网络码字，其中Q应为一个满足特定条件的$n\times n$可逆矩阵。然后，将信源的输入信息由向量m转换成(m,k)，这里(m,k)是将$GF^{n-r}(q)$中的向量m与$GF^r(q)$中随机选择的密钥向量k按比特连接起来。这样，每条边上传输的信息就变成了$(m,k)f_e'$。此安全方案与一般网络编码方案的对比如图 5-1 所示。Cai 和 Yeung 在文献[18]中从理论上证明了该码字的安全性和可达性。

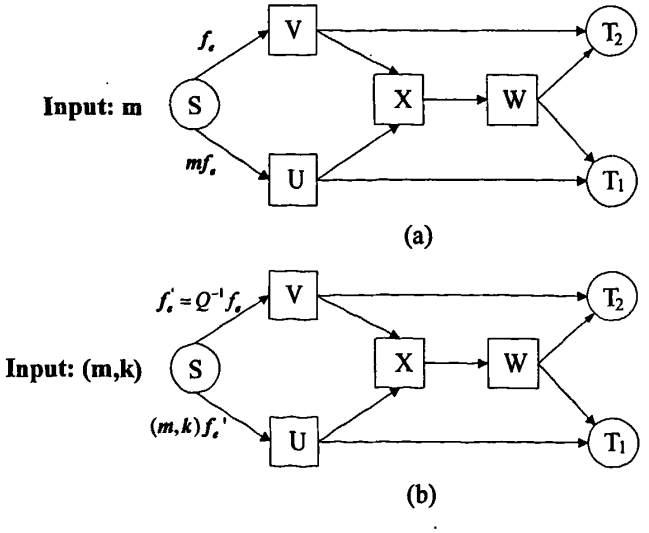


图 5-1 CSWN 上安全网络编码方案与一般网络编码方案的对比

定理 5-1[18]：如果在 $GF(q)$域上存在一组 n 维线性网络码，对于所有的用户节点 $u \in U$ 有：

$$\dim(V_u) = n \tag{5.1}$$

并且对于所有被窃听的信道 $\psi \in \lambda$，有：

$$\dim(V_\psi) \le r \tag{5.2}$$

那么当 $q > |\lambda|$ 时，在有向图 G 中的 $GF(q)$域上就能够通过上述方法构造一组可达码。其中，$V_u = \langle \{ f_e : e \in In(u) \} \rangle$，$In(u)$ 表示节点 u 的入度；$V_\psi = \langle \{ f_e : e \in \psi \} \rangle$。

证明：由于证明过程比较复杂，本文就不详细描述了，具体可以参见文献[18]中第 7 小节中关于定理 2 的证明。

此外，Feldman 等人[19]也提出了一种安全方案，与上述方案有些许不同，他们保持原来分配的网络码不变，只对输入的信源信息作线性变换，即只改变通信网络的输入信息。与 Cai 和 Yeung[18]的方案类似，此处同样需要一个 $n \times n$ 可逆矩阵 Q。该方案将信源的输入向量$(\boldsymbol{m},\boldsymbol{k})$乘以 Q^{-1}，每条边上传输的信息就成为 $((\boldsymbol{m},\boldsymbol{k})Q^{-1})\boldsymbol{f}_e$。我们很容易可以看出，此方案需要一条专门的加密信道来传送变换用的矩阵 Q，否则，信宿节点将无法恢复源信息 $\boldsymbol{m}$ 和随机密钥 $\boldsymbol{k}$。

5.3 单信源组播通信中一种改进的反窃听网络编码方案

5.3.1 基本思想

基于降低网络节点处理复杂度和网络开销的目的，本文提出一种改进的安全网络编码方案来抵抗此类窃听攻击。本方案将网络编码与密码学中的“一次一密”（*One-time Pad*）相结合，使得不需要加密矩阵就能够进行保密传输，因此复杂度得以降低。“一次一密”的原理是使用与传送信息等长的密钥对信息进行加密，并且对不同信息使用不同的随机密钥来加密。我们假设需要传送的信息为 $\boldsymbol{m}$，用来加密的密钥为 $\boldsymbol{k}$，两向量具有相同的长度。假设使用网络编码后，网络的组播容量是 n，则 $\boldsymbol{m}$ 和 $\boldsymbol{k}$ 都是 $n/2$ 维的向量，都属于有限域 $GF^{n/2}(q)$。注意，这里假设 n 是偶数。如果 n 是奇数，则用 $\lfloor n/2 \rfloor$ 来代替 $n/2$ 即可。

现在我们用上述线性网络码来构造一种改进的安全网络码，如下所示（假设 n 是偶数）：

(1) 为通信网络分配一组 n 维线性网络码，保证使用这组网络码之后，信源信息能够正确传送到每个信宿节点；

(2) 假设信源信息向量 m 的长度为 $n/2$（此处 m 不必须满足在 $GF^{n/2}(q)$上均匀分布），独立的随机密钥向量 k 的长度也为 $n/2$。令 $m'=m+k(\mathrm{mod}q)$（这里的加法是指 m 与 k 按位模 q 加），因此整个网络的输入信息就变成向量 $I=(m',k)$。假设 $m=(m_1,m_2,\ldots,m_{n/2})$，$k=(k_1,k_2,\ldots,k_{n/2})$，那么就有：

$$I=(m_1+k_1,m_2+k_2,\ldots,m_{n/2}+k_{n/2},k_1,k_2,\ldots,k_{n/2}) \tag{5.3}$$

(3) 将信源信息向量 I 编码，在每条信道上传送的值为 $I\cdot l(e)$。

从上述构造可以看出，此改进方案进行保密通信是不需要加密矩阵的，因此也就不需要加密信道传送此矩阵。同时，此方案也没有改变原来的网络码，只是改变了网络的输入信息。鉴于原网络编码方案的可行性，每个信宿节点都能够顺利解出 m'，同时作为附加产品，密钥 k 也能被同时解出。将 m'与 k 执行按位减后，很容易就能译出原本要传送的源信息向量 m。接下来我们从安全性和复杂度的角度对此方案的性能进行分析。

5.3.2 性能验证与分析

5.3.2.1 安全性和可达码

本文将在这一子小节中，对上述改进方案的安全性及其可达码进行分析。

引理 5-1：“一次一密”（*One-time Pad*）能够使系统达到信息论的完善保密。

证明：我们将要传送的原始消息叫做“明文”（*plaintext*），而加密过的消息就叫“密文”（*ciphertext*）。由于 $m'=m+k(\mathrm{mod}q)$，m'就是密文，而 m 是明文，k 是随机密钥。

因为密钥 k 与 m 独立，并且均匀分布在 $GF^{n/2}(q)$上，这样，$GF^{n/2}(q)$中的每个向量 k 都有同等的机会去加密（随机化）m。将加密函数和解密函数分别描述为 $e_k(m)=m'$和 $d_k(m')=m$。对于任意的 $m,m'\in GF^{n/2}(q)$以及每个 $e_k(m)=m'$，存在唯一的 k 满足上面两个等式。为了简化证明，我们用 Ω 来表示 $GF^{n/2}(q)$，就可以得到：

$$\begin{aligned}\Pr[Y=m']&=\sum_{k\in\Omega}\Pr[K=k]\Pr[M=d_k(m')]\\&=\sum_{k\in\Omega}\frac{1}{q^{n/2}}\Pr[M=m'-k]=\frac{1}{q^{n/2}}\sum_{k\in\Omega}\Pr[M=m'-k]=\frac{1}{q^{n/2}}\end{aligned} \tag{5.4}$$

由此可得，对于任意的 m' $\in\Omega$，有 $\Pr[m']=\frac{1}{q^{n/2}}$ (5.5)

接着我们来计算条件概率 $\Pr[m'|m]$。对于任意的 $m,m'\in GF^{n/2}(q)$，$K=(m'-m)\bmod q$ 是

唯一符合等式$e_k(m)=m'$的密钥，因此得到：

$$\Pr[m'|m]=\Pr[K=(m'-m)\bmod q]=\frac{1}{q^{n/2}} \tag{5.6}$$

最后，利用贝叶斯定理可以得到下面的结果：

$$\Pr[m|m']=\frac{\Pr[m]\Pr[m'|m]}{\Pr[m']}=\frac{\Pr[m]\frac{1}{q^{n/2}}}{\frac{1}{q^{n/2}}}=\Pr[m] \tag{5.7}$$

综上所述，引理 5-1 成立。这个定理说明，窃听者在得到加密后的信息 m'之后，只要获取不到密钥 k，就无法得到任何信源信息。

在使用“一次一密”的基础上，如果使用路由技术来传送消息，那么进行保密通信最大的问题就在于如何保护密钥 k，很明显这里就需要保密信道将加密密钥传送至信宿节点，否则信宿就无法对收到的消息进行解密，这样就增加了网络的开销。而本文的构造方案使用网络编码技术传送消息，将密钥连接到密文之后，就能够使密钥跟密文同时被当作一般输入信息传送至信宿端，而密钥不会被泄露。具体阐述如下。

定理 5-2：只要在 $GF^n(q)$上存在一组 n 维线性网络码，对于所有的信宿节点 $t\in T$，满足：

(1) $In(t)=n$（$In(t)$指信宿节点 t 的入度），并且所有满足 $head(e)=t$ 的 $l(e)$都线性独立；

(2) $n/2\geq\max(|\psi|)$（λ和ψ已在前面的章节中定义过），

那么本文构造的方案就能够将信源信息安全传输到信宿节点，不会泄露任何信息给窃听者。

证明：从网络编码的原理可以看出它的一个很重要的作用是能够将要传送的信息向量比特进行混合。通过研究 Cai 和 Yeung 提出的方案，发现该方案之所以能够对传送信息起到保密作用，是因为该方案使用了一个可逆矩阵 Q (Q^{-1})，将其与分配给每条链路（边）的网络码相乘，构成了一组新的安全网络码 $f_e'=Q^{-1}f_e$。假设网络容量为 n 比特，随机密钥为 r 比特的行向量，因此源信息为 $n-r$ 比特的行向量。由于可逆矩阵需要满足特定要求，即要使得 f_e'（列向量）底部的 r 个元素不全为 0。因为只有这样，密钥 k 才能通过网络码与信源信息混合起来。如果底部 r 个元素都为 0，那么窃听者就会通过窃听某条边上的信息而得到信源信息 m 中元素的线性组合，这样系统就不保密了。

在本文的安全方案中，根据信道分配的原网络码，可以将窃听者窃听到的信道分为两种：

(1) 全局编码核（列向量）底部的 $n/2$ 个元素全为 0：窃听者获取了此类信道上传输的信息之后，所能得到的是密文 $\boldsymbol{m}'$中元素的线性组合。此时，由于密钥 $\boldsymbol{k}$ 的 $n/2$ 个元素所对应相乘的全局编码核的元素为全 0，密钥就相当于被此网络码“隐藏”了，因此窃听者既得不到有关信源的信息，也得不到密钥 $\boldsymbol{k}$。由引理 4-1 得知，用“一次一密”方法加密过的信息是完善保密的，因此我们得出结论，即此种情况下，通信网络对于窃听者是完善保密的。

(2) 全局编码核（列向量）底部的 $n/2$ 个元素不全为 0：窃听者获取了此类信道上传输的信息之后，所能得到的是密文 $\boldsymbol{m}'$与密钥 $\boldsymbol{k}$ 的元素间的线性组合。根据 Cai 和 Yeung 的 CSWN 模型[18]，窃听者通过对获取的信息执行线性变换来得到自己想要的信息（建立线性方程组），因此要达到完善保密，本文的方案还必须满足下述条件：$n/2 \geq \max(|\psi|)$，$\max(|\psi|)$ 是窃听者每次最多允许窃听到的边的数目。这个条件用来防止窃听者窃取 $n/2$ 位的密钥向量。而定理中的约束条件 $In(t)=n$ 是用来保证线性网络码的可译性的。根据定理 5-1（只需将 f_e'替换为 $l(e)$即可），本定理得证。因此可以得出结论，即本文改进的安全网络编码方案能够用来进行保密通信。

综上所述，本文的安全网络编码方案既不需要满足特定条件的可逆矩阵来对原网络码进行变换，因此也就不需要保密信道来传送该矩阵，降低了节点的执行复杂度。利用网络编码成功将数据传输到信宿节点的核心是：每个信宿节点都能够根据接收到的符号（至少 n 个），建立一个具有 n 个未知数（网络的输入符号）和 n 个线性方程的方程组。在此基础上，每个信宿端都能够顺利恢复出网络的输入符号，即同时恢复出加密后的源信息 $\boldsymbol{m}'$和密钥 $\boldsymbol{k}$。最后，将 $\boldsymbol{m}'$与 $\boldsymbol{k}$ 执行按位减法，就能够得到所需要的信源信息 $\boldsymbol{m}$。

图 5-1 给出了一个具体的例子来进一步说明本文方案的安全性和可行性。根据定理 5-2，在下图的网络拓扑情况下，窃听者最多只允许窃听 1 条信道。此外，需要将基域选择为 $GF(3)$。信源节点 S 组播符号 m 到信宿节点 T_1 和 T_2，网络编码分配的全局编码核如下：

$$l(SU)=l(UT_1)=l(UX)=\begin{pmatrix}1\\0\end{pmatrix},$$

$$l(SV)=l(VT_2)=l(VX)=\begin{pmatrix}0\\2\end{pmatrix},$$

$$l(XW)=l(WT_1)=l(WT_2)=\begin{pmatrix}2\\2\end{pmatrix}。$$

具体每条信道上传输的数据如图 5-2 所示。从图中可以看到，信宿节点 T_1 和 T_2 都从

各自的输入链路中接收到了 2 个符号，它们可以根据这 2 个符号和输入链路上分配的全局编码核，分别建立 2 个含有 2 个线性方程的方程组，随之利用高斯消去法计算出符号 m' 和 k。最后，将 m'减去 k 得到 m。无论窃听者获取了哪一条信道上的信息，它都无法得到信源信息 m。

5.3.2.2 安全复杂度

这里将安全复杂度定义为实现保密通信所需对原网络码及网络输入进行操作的步骤数。根据 Cai 和 Yeung、Feldman 以及本文的方案，我们很容易计算出复杂度分别为 $O(n^2|E|)$、$O(n^2)$和 $O(n)$。据此可以看出，本文的方案将安全复杂度降低了一个数量级。

最后本章详细叙述一下用本文提出的安全网络编码方案进行数据传输时的解码过程（仍假设要传送的源信息为 m）：

步骤 1：对于每个信宿节点 $t \in T$ →根据从 n 条输入链路接收到的数据（符号）和链路上分配到的全局编码核建立 n 个线性方程→使用高斯消元法计算出 n 维向量(m', k)的每个元素符号；

步骤 2：$m = m' - k \pmod q$ →得到源信息 m。

但需要说明的是，本文提出的方案虽然降低了复杂度和网络开销，但同时是以降低编码效率为代价的。在本文的方案中，编码效率约为 50%，而另 2 种已有方案的编码效率是 $(n-r)/n$（r 是随机密钥所占的比特数），它们的效率受到实际情况的影响，尤其受到窃听者攻击能力的影响。窃听者的攻击能力越强，编码效率就越低。

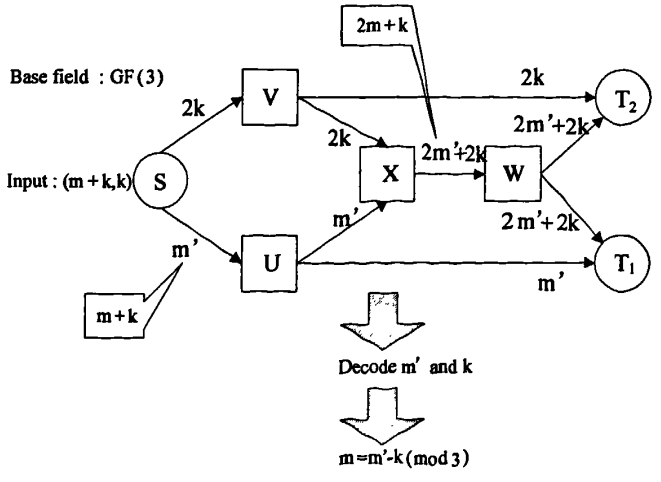


图 5-2 改进的安全网络编码示例

5.4 本章小结

本章对外部窃听节点造成的安全攻击进行了研究，详细研究了 Cai 和 Yeung 针对此问题提出的抵抗方法[18]，并在其基础上提出了一种改进的安全网络编码方案。通过证明，我们得出结论，本文提出的方案能够在降低节点的计算复杂度。

此外，还有一些学者在这个方向上也做了努力，提出了一些性能较好的算法。Cai 和 Yeung 将[18]中的结论推广到了多信源线性网络码，并利用该码的代数结构，得出安全码的必要和充分条件[20]。他们还进一步验证了[18]中提出的安全网络码的最优性问题[21]，并通过理论证明该码能够在最大化安全组播信息量的同时，最小化必需的随机信息量。Silva 和 Kschischang 在[22]中构造了一个编码方案，此方案能够达到$n-\mu$信息论上保密分组可达的最大速率，其中 n 是信源到每个信宿的分组数量，μ 是窃听者可以窃听到的链路数目。这一方案可以应用于任何通信网络，而不需要知道底层网络码的任何信息，同样也没有任何编码限制。其基本思想是使用一种“非线性”外部码（该码在扩展域F_{q^m}上是线性的），并对这个扩展域的优势加以利用。Bhattad 和 Narayanan 提出了一个不同的安全标准[23]：只要窃听者无法获得任何未经编码的或可直接译出的源数据（即“有意义”的数据），一个通信系统就被认为是安全的。此外，Tan 和 Medard[24]利用网络的拓扑结构来使攻击者无法获取任何有意义的信息，并且在原有安全网络编码问题的基础上增加了一个代价函数，原有问题则演化成为寻找一个能使网络开销和攻击者成功获取所需信息的概率都最小化的编码方案。由于具有局部最优码、有状态意识的网络编码方案[14]要求邻居节点能够译出他们收到的所有分组，就必须通过端对端的加密方式保障其保密性。

第六章 总结与展望

网络编码思想自诞生以来，越来越受到国内外众多学者的关注。目前，网络编码已被证明是可以逼近网络容量理论传输极限的有效方法，已被国际学术界和美国军方认定为解决网络问题的重要手段。具有确定拓扑的有线网络的网络编码已受到广泛的关注，但网络编码的无线研究和应用还处于探索阶段。无线链路的不可靠性和物理层广播特性非常适合使用编码的方法。网络编码在无线网络中的应用可以提高网络的吞吐量，尤其是多播吞吐量；可以减少数据包的传播次数，降低无线发送能耗。采用随机网络编码，即使网络部分节点或链路失效，最终在目的节点仍然能恢复出原始数据，增强网络的容错性和鲁棒性；无需复杂的加密算法，采用网络编码就可以提高网络的安全性。无线网络编码技术的研究具有重要的理论意义和应用价值。

本文在对网络编码的基本理论进行深入学习和研究的基础上，着重讨论其在无线网络和安全性方面的应用。应用网络编码思想，对无线网络编码技术做了一些研究，并尝试对一种基于网络编码的 P2P 内容分发系统的性能进行了验证。通过仿真实验表明：与一般网络编码相比，稀疏网络编码能够减小分发系统中编码分块的线性相关性，降低编码计算复杂度，并且解码成功率较高。与无编码的分发系统相比，基于稀疏网络编码的分发系统在吞吐量、平均下载时间和总分发时间等方面的性能都要优于前者。

本文还在安全网络编码这一新兴的研究领域中做了一些探讨，研究了单源组播通信中一种改进的反窃听安全网络编码方案，并对其安全性和可达性进行了理论验证。目前，网络编码技术在安全性方面的应用还处于初级阶段，对它的研究与探索仍然将继续下去。由于时间和个人能力的限制，本文的研究工作还不够深入，在以下几个方面还有待于进一步的探索：

1．由于拜占庭攻击对于使用网络编码技术的网络具有很强的攻击性，因此必须考虑如何构造和维护对于拜占庭攻击具有强鲁棒性的网络拓扑；

2．考虑如何进一步将网络编码与各种经典密码学技术有效结合；

3．考虑将网络编码技术运用到匿名通信中；

4．考虑如何将网络编码技术的优势运用到保密多端计算中。

致谢

时光如梭，转眼三年的研究生生活即将结束。这期间，无论在专业知识方面还是科研方法方面我都有非常大的收获，借此机会，我要向所有帮助过我的老师、同学、家人致以最诚挚的感谢。

首先，衷心感谢我的导师徐澄圻教授。徐老师深厚渊博的学识，敏锐深刻的科学洞察力，严谨求实的治学态度和精益求精的工作作风深深地影响了我的成长，同时也为我树立了榜样。在今后的工作学习中，我将牢记徐老师的谆谆教诲，踏踏实实做事，坦坦荡荡做人，为社会以及通信行业的发展贡献自己的力量。

其次，我要感谢多年来关心、支持我的家人、同学和朋友，是你们帮助我愉快、顺利的完成了硕士阶段的学习生活。

最后，非常感谢在百忙之中抽出时间来审阅本文，参加答辩并给予我批评和指导的各位专家，谢谢你们宝贵的意见和建议！

参考文献

[1]. R. Ahlswede, N. Cai, S. Li, R. Yeung, "Network information flow", *IEEE Transactions on Information Theory 46,* 4 (July), 1204–1216, 2000.

[2]. T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, J. Shi, B. Leong, "A random linear network coding approach to multicast", *IEEE Transactions on Information Theory 52,* 10 (October), 4413–4430, 2004.

[3]. T. Ho, R. Koetter, M. Medard, D. Karger, M. Effros, "The benefits of coding over routing in a randomized setting", *IEEE International Symposium on Information Theory (ISIT)*, 2003.

[4]. T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, D. Karger, "Byzantine modification detection in multicast networks using randomized network coding", *IEEE International Symposium on Information Theory (ISIT)*, 2004.

[5]. D. Lun, M. Medard, R. Koetter, M. Effros, "On Coding for Reliable Communication over Packet Networks", *Proc. 42nd Annual Allerton Conference on Communication, Control, and Computing*, 2005.

[6]. P. Chou, Y. Wu, K. Jain, "Practical Network Coding", *Allerton Conference on Communication, Control, and Computing*, 2003.

[7]. J. Widmer, J.-Y.L. Boudec, "Network coding for efficient communication in extreme networks", In *WDTN '05: Proceeding of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking.* ACM Press, Philadelphia, Pennsylvania, USA, 284–291, 2005.

[8]. A. Elfawal, K. Salamatian, D. Cavin, Y. Sasson, J.-Y.L. Boudec, "A framework for network coding in challenged wireless network", 2006.

[9]. S. Deb, M. Effros, T. Ho, D. Karger, R. Koetter, D. Lun, M. Medard, N. Ratnakar, "Network coding for wireless applications: A brief tutorial", *In proc of IWWAN, London, UK, May,* 2005.

[10]. A. Dimakis, P. Godfrey, M. Wainwright, K. Ramchandran, "Network coding for distributed storage systems", *26th IEEE International Conference on Computer Communications (INFOCOM 2007)*, 2000-2008, 2007.

[11]. C. Gkantsidis, P. Rodriguez, "Network coding for large scale content distribution", In *Proceedings of IEEE Infocom.* Miami, Florida, 2005.

[12]. S. Acedanski, S. Deb, M. Medard, R. Koetter, "How good is random linear coding based distributed networked storage?" , In *Proceedings of the First Workshop on Network Coding, Theory and Applications (Netcod),* Riva del Garda, Italy, 2005.

[13]. S. Jaggi, P. Sanders, P. Chou, M. Effros, S. Egner, K. Jain, L. Tolhuizen, "Polynomial time algorithms for multicast network code construction", *IEEE Transactions on Information Theory 51,* 6, 1973–1982, 2005.

[14]. S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, J. Crowcroft, "Xors in the air: practical wireless network coding", In *SIGCOMM '06: Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications.* ACM Press, Pisa, Italy, 243–254, 2006.

[15]. L. Toledo, A. Wang, "Efficient Multipath in Sensor Networks using Diffusion and Network Coding", In *Proceedings of the 40th Annual Conference on Information Sciences and Systems*, 2006.

[16]. S. Sengupta, S. Rayanchu, S. Banerjee, "An Analysis of Wireless Network Coding for Unicast Sessions: The Case for Coding-Aware Routing", In *Proceedings of the 26th Annual IEEE Conference on Computer Communication (INFOCOM 2007)*, 2007.

[17]. L. Lima, M. Medard, J. Barros, "Random linear network coding: A free cypher?", In *Proceedings of the IEEE International Symposium on Information Theory*, Nice, France, 2007.

[18]. N. Cai, R. Yeung, "Secure network coding", In *Proceedings of the IEEE International Symposium on Information Theory*, Lausanne, Switzerland, 2002.

[19]. J. Feldman, T. Malkin, C. Stein, and R. A. Servedio, "On the capacity of secure network coding", 42nd Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, Sept 29-Oct 1, 2004.

[20]. N. Cai, R. Yeung, "A Security Condition for Multi-Source Linear Network Coding", In *IEEE International Symposium on Information Theory (ISIT)*, Nice, France, 2007.

[21]. R. Yeung, N. Cai, "On the Optimality of a Construction of Secure Network Code", In *IEEE International Symposium on Information Theory (ISIT)*, 2008.

[22]. D. Silva, F. R. Kschischang, "Security for Wiretap Networks via Rank-Metric Codes", In *IEEE International Symposium on Information Theory (ISIT)*, 2008.

[23]. K. Bhattad, K. Narayanan, "Weakly secure network coding", *Proc. of the First*

Workshop on Network Coding, Theory, and Applications (NetCod), 2005.

[24]. J. Tan, M. Medard, "Secure Network Coding with a Cost Criterion", *Proc. 4th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt'06), Apr*, 2006.

[25]. E. Ayday, F. Delgosha and F. Fekri, Location-Aware Security Services for Wireless Sensor Networks Using Network Coding, In Proc. of 26th IEEE International Conference on Computer Communications (INFOCOM 2007), May 2007, pp. 1226-1234.

[26]. L. Lima, J. P. Vilela, J. Barros, M. Medard, "An Information-Theoretic Cryptanalysis of Network Coding – is protecting the code enough?", *Submitted for publication*, 2008.

[27]. R. Koetter, F. Kschischang, "Coding for errors and erasures in random network coding", *Arxiv preprint* http://arxiv.org/abs/cs/0703061, 2007.

[28]. D. Silva, F. Kschischang, R. Koetter, "A Rank-Metric Approach to Error Control in Random Network Coding", *IEEE Information Theory Workshop on Information Theory for Wireless Networks*, 1–5, 2007.

[29]. D. Silva, F. Kschischang, "Using rank-metric codes for error correction in random network coding", *Proc. Of the 2007 IEEE International Symposium on Information Theory*, 2007.

[30]. D. Silva, F. Kschischang, R. Koetter, "Capacity of random network coding under a probabilistic error model", *Arxiv preprint arXiv/0807.1372*, 2008.

[31]. A. Montanari, R. Urbanke, "Coding for Network Coding", *Arxiv preprint arXiv: 0711.3935*, 2007.

[32]. N. Cai, R. Yeung, "Network error correction", *Proceedings of the IEEE International Symposium on Information Theory, Yokohama, Japan, July*, 2003.

[33]. S. Jaggi, M. Langberg, S. Katti, [illegible], D. Katabi, M. Medard, "Resilient Network Coding In the Presence of Byzantin[illegible]rsaries", In *Proceedings of INFOCOM 2007*. Anchorage, Alaska, 2007.

[34]. L. Nutman, M. Langberg, "Adversarial Models and Resilient Schemes for Network Coding", In *IEEE International Symposium on Information Theory (ISIT)*, Toronto, Canada, 2008.

[35]. D. Charles, K. Jain, K. Lauter, "Signatures for network coding", *Proceedings of the 40th Annual Conference on Information Sciences and Systems, Princeton, USA, March,*

857-863, 2006.

[36]. M. N. Krohn, M. J. Freedman, D. Mazieres, "On-the-fly verification of rateless erasure codes for efficient content distribution", In *Proceedings of the 2004 IEEE Symposium on Security and Privacy*, 226–240, 2004.

[37]. C. Gkantsidis, P. R. Rodriguez, "Cooperative security for network coding file distribution", In *Proceedings of IEEE Infocom*. Barcelona, Spain, 2006.

[38]. F. Zhao, T. Kalker, M. Medard, K. J. Han, "Signatures for content distribution with network coding", In *International Symposium on Information Theory (ISIT)*, Nice, France, 2007.

[39]. M. Kim, M. Medard, J. Barros, "Counteracting Byzantine Adversaries with Network Coding: An Overhead Analysis", *Arxiv preprint arXiv: 0806.4451*, 2008.

[40]. L. Eschenauer, V. D. Gligor, "A key-management scheme for distributed sensor networks", In *CCS '02: Proceedings of the 9th ACM conference on Computer*

a) *and communications security*. ACM Press, New York, USA, 41–47, 2002.

[41]. A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, D. E. Culler, "SPINS: Security protocols for sensor networks", *Wireless Networks 8,* 5, 521–534, 2002.

[42]. D. Malan, M. Welsh, M. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography", In *First IEEE International Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, California*, 2004.

[43]. P. F. Oliveira, R. A. Costa, J. Barros, "Mobile Secret Key Distribution with Network Coding", In *Proc. of the International Conference on Security and Cryptography (SECRYPT)*, 2007.

[44]. D. Wang, F. R. Kschischang, "Constricting the Adversary: A Broadcast Transformation for Network Coding", *Allerton Conference on Communication, Control, and Computing, Monticello, IL, September 26-28*, 2007.

[45]. S. Katti, J. Cohen, D. Katabi, "Information Slicing: Anonymity Using Unreliable Overlays", In *Proc. of the 4th USENIX Symposium on Network Systems Design and Implementation (NSDI)*, 2007.

[46]. S.-Y. R. Li, R. W. Yeung and N. Cai, "Linear network coding", IEEE Trans. Info. Theory, IT-49: 371-381, 2003.

[47]. R. Koetter and M. Medard, "An algebraic approach to network coding,",

a) *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, 2003.

[48]. 48. R. Koetter and M. Medard, "Beyond Routing: An algebraic Approach to network coding," Proceedings of the 2002 TEEE Infocom, vol.1, pp. 122-130, June 2002.

[49]. 卢开澄、卢华明，图论及其应用（第二版），清华大学出版社.

[50]. 车书玲，《无线网络编码研究》，西安电子科技大学硕士学位论文，2005.

[51]. 池凯凯，《网络编码原理及其纠错性分析》，西安电子科技大学硕士学位论文，2005年.

[52]. 陈巍，《浅谈网络信息论中若干前沿问题》，网络拥塞研讨会 special talk，2004 年 4 月.

[53]. R. Dougherty, C. Freiling, and K. Zeger, "Linearity and solvability in multicast networks," IEEE Transactions on Information Theory, vol. 50, No. 10, pp. 2243-2256, Oct. 2004

[54]. S. Riis, "Linear versus non-linear boolean functions in network flow," *preprint* (available on-line at http://nick.dccs.quml.ac.uk/smriis), Dec. 2003.

[55]. R. Dougherty, C. Freiling, and K. Zeger, "Insufficiency of linear coding in network information flow," IEEE Transactions on Information Theory, vol. 51, No. 8, pp. 2745-2759, Aug. 2005.

[56]. 彭木根，王月新，王文博，无线自组织网络的网络编码技术，中兴通讯技术，2007年第 4 期，pp.56-60.

[57]. P. Sanders, S. Egger and L. Tolhuizen, "Polynomial time algorithms for network information flow. 15th ACM Symposium on Parallel Algorithms and Architectures. 2003, 7(3): PP. 286-294.

[58]. T. Ho, M. Medard, R. Koetter, et al. Toward a random operation of networks, IEEE Transactions on Information Theory. Vol. 50. pp. 532-537, May 2004.

[59]. M. Medard, M. Effros, T. Ho, D. Karger, On Coding for Non-multicast Networks, 41st Annual Allerton Conference on Communication Control and Computing, Monticello, Illinois, October 2003.

[60]. T. Ho, M. Medard, J. Shi, et al. On Randomized Network Coding, In: 41st Annual Allerton Conference on Communication, Control and Computing, Oct.2003.

[61]. 孙利民，李建中，陈渝等，无线传感器网络，北京：清华大学出版社，2005.

[62]. I.F. Akyildiz, Xudong Wang, A Survey on Wireless Mesh Networks, IEEE

Communication Magazine 2005, 43(9): 23-30.

[63]. J.E. Wieselthier, G.D. Nguyen and A. Ephremides, On the Construction of Energy-efficient Broadcast and Multicast Trees in Wireless Networks. In *Proceedings of IEEE Infocom*, March 2000.

[64]. J.E. Wieselthier, G.D. Nguyen and A. Ephremides, Resource-limited Energy-efficient Wireless Multicast of Session Traffic, In *Proceedings of 34th International Conference on System Sciences*, January 2000.

[65]. Song Guo and Oliver Yang, Minimum-Energy Broadcast Routing in Wireless Multihop Networks, *International Performance, Computing and Communications Conference*(IEEE IPCCC 2003), Phoenix, Arizona, April 9-11, 2003, pp. 273-280.

[66]. Jun Yuan, Zongpeng Li, Wei Yu, et al. A Cross-layer Optimization Framework for Multicast in Multi-hop Wireless Networks. In Proc. of 1st International Conference of Wireless Internet (WICON), 2005: 47-54.

[67]. Yunnan Wu, P.A. Chou, Q. Zhang, et al. Network Planning in Wireless Adhoc Networks: A Cross-layer Approach, IEEE J. Selected Areas Communication, 2005, 23(1): 136-150.

[68]. Yunnan Wu, S-Y. Kung, Reduced-complexity Network Coding for Multicasting Over Adhoc Networks, In Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2005, 3: 18-23.

[69]. Yunnan Wu, P.A. Chou, S.-Y. Kung, Minimum Energy Multicast in Mobile Adhoc Networks Using Network Coding, IEEE Transactions on Communications, 2005, 53(11): 1906-1918.

[70]. D.S. Lun, M. Medard, R. Koetter, Efficient Operation of Wireless Packet Networks Using Network Coding, In Proceedings of International Workshop on Convergent Technologies (IWCT), 2005.

[71]. D.S. Lun, N. Ratnakar, M. Medard, et al. Minimum-cost Multicast Over Coded Packet Networks, IEEE Transactions on Information Theory, 2006, 52(6): 2608-2623.

[72]. D.S. Lun, N. Ratnakar, R. Koetter, et al. Achieving Minimum-cost Multicast: A Decentralized Approach Based on Network Coding, IEEE INFOCOM 2005.

[73]. A. Ahluwalia, E. Modiano, L. Shu, On The Complexity and Distributed Construction of Energy-efficient Broadcast Trees in Wireless Ad Hoc Networks, IEEE Transactions on Wireless Communications, 2005, 4(6): 2136-2147.

[74]. W. Liang, Constructing Minimum-energy Broadcast Trees in Wireless Ad hoc Networks, In Proc. of 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing, 2002: 112-122.

[75]. J. Widmer, C. Fragouli, J-Y. Boudec, Low-complexity Energy-efficient Broadcasting in Wireless Ad-hoc Networks Using Network Coding, In Proc. WINMEE, RAWNET and NETCOD 2005 Workshops, 2005.

[76]. D.S. Lun, M. Medard, R. Koetter, Network Coding for Efficient Wireless Unicast, IEEE International Zurich Seminar on Communications, 2006: 74-77.

[77]. Y. Chen, S. Kishore, J. Li, Wireless Diversity Through Network Coding, In Proc. of IEEE Wireless Communications and Networking Conference, 2006, 3: 1681-1686.

[78]. 孙岳，《网络编码及网络容错的研究》，西安电子科技大学硕士学位论文，2005.

[79]. Y. Wu, P.A. Chou, S.-Y. Kung, Information Exchange in Wireless Networks With Network Coding and Physical-layer Broadcast, Microsoft Technical Report, MSR-TR-2004-78, Aug. 2004.

[80]. 刘亚杰，《P2P 流媒体内容分发关键技术研究》，国防科学技术大学博士学位论文，2005.

[81]. Y. Wu, P.A. Chou, Q. Zhang, K. Jain, W. Zhu and S.-Y. Kung, Achievable Throughput for Multiple Multicast Sessions in Wireless Ad hoc Networks, Submitted to IEEE Globecom 2004, March 2004.

[82]. M. Wang, B. Li, How Practical Is Network Coding?, In Proc. of 14th IEEE International Workshop on Quality of Service 2006. Yale University, New Haven, Connecticut, 2006.

[83]. C. Cooper, On the Distribution of Rank of A Random Matrix Over a Finite Field, Journal of Random Struct. Algorithms, 2000, 17 (3-4): 197-212.

[84]. Guanjun Ma, Yinlong Xu, Minghong Lin and Ying Xuan, A Content Distribution System based on Sparse Linear Network Coding, In Proc. of 3rd Workshop on Network Coding, Theory, and Applications, 2007, San Diego, California.

[85]. I. Stoica, R. Morris, D. Karger, et al. Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications, ACM SIGCOMM 2001, 2001.

[86]. 罗杰文，Peer to Peer（P2P）综述，http://docs.huihoo.com/p2p/1/index.html，2005.

[87]. 俞嘉地，Bit Torrent 对等网文件共享系统关键技术研究，上海：上海交通大学，2007.

[88]. A.G. Dimakis, V. Prabhakaran, Ubiquitous Access to Distributed Data in Large-scale

Sensor Networks Through Decentralized Erasure Codes, In Proc. of the Symp. on Information Processing in Sensor Networks (IPSN), Los Angeles, 2005.

[89]. C. Intanagonwiwat, R. Govindan, D. Estrin, Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks, In Proc. of the ACM Mobicom, Boston: ACM Press, 2000, 56-67.

[90]. D. Kempe, J. Kleinberg, A. Demers, Spatial Gossip and Resource Location Protocols, Journal of ACM, 2004, 51 (6): 9432967.

[91]. Yu Wang, I.D. Henning, D.K. Hunter, Efficient Information Exchange in Wireless Sensor Networks using Network Coding, In Proc. of Fourth Workshop on Network Coding, Theory and Applications (NetCod 2008), Jan. 2008, pp. 1-6.

[92]. Zhiqiang Xiong, Wei Liu, Jiaqing Huang, Wenqing Cheng, Bo Cheng, Network Coding Approach for Intra-Cluster Information Exchange in Sensor Networks, In Proc. of IEEE 66th Vehicular Technology Conference (VTC-2007), 2007, pp. 164-168.

[93]. A. Dimakis, V. Prabhakaran and K. Ramchandran, Decentralized Erasure Codes for Distributed Networked Storage, IEEE Trans. Information Theory, Jun. 2006.

[94]. D. Wang, Q. Zhang and J. Liu, Partial Network Coding: Theory and Application for Continuous Sensor Data Collection, In Proc. of 14th IEEE International Workshop on Quality of Service (IWQoS), 2006.

[95]. V. Raghunathan, C. Schurgers, S. Park and M.B. Srivastana, Energy-aware Wireless Microsensor Networks, IEEE Signal Processing Magazine 2002, 19 (2): 40-50.

[96]. E. Ahmed, N. Kamal Jamal and Al-Karaki, Routing Techniques in Wireless Sensor Networks: A Survey, IEEE Journal of Wireless Communications, 11pp. 6-28, Dec. 2004.

[97]. J.S. Park, D.S. Lun, F. Soldo, et al. Performance of Network Coding in Ad Hoc Networks, In Proc. of The 25th Military Communications Conf. (MILCOM 2006), Washington D.C., 2006.

[98]. Y.E. Sagduyu and A. Ephremides, Crosslayer Design for Distributed MAC and Network Coding in Wireless Ad Hoc Networks, In Proc. of IEEE International Symposium on Information Theory, Adelaide, Australia, pp. 1863-1867, Sep. 2005.

[99]. S. Katti, D. Katabi, W. Hu, et al. The Importance of Being Opportunistic: Practical Network Coding for Wireless Environments, In Proc. of 43rd Annual Allerton Conference on Communication, Control and Computing, Sep. 2005.

[100]. T. Ho, B Leong, M. Medard, R. Koetter, Y. Chang and M. Effros, On the Utility of Network Coding in Dynamic Environments, International Workshop on Wireless Ad-hoc Networks (IWWAN), Jun. 2004.

[101]. D. Petrovic, K. Ramchandran and J. Rabaey, Coding for Sensor Networks Using Untuned Radios, In Proc. of IEEE 6th Workshop on Signal Processing Advances in Wireless Communications, Jun. 2005, pp. 1093-1097.

[102]. X. Zhang and S.B. Wicker, Robustness vs Efficiency in Sensor Networks, In Proc. of 4th International Symposium on Information Processing in Sensor Networks (IPSN), Apr. 2005, pp. 225-230.

[103]. K. Jain, Security based on Network Topology Against the Wiretapping Attack, IEEE Wireless Communications, pp. 68-71, Feb. 2004.

[104]. T. Chan, A. Gtant, Capacity Bounds for Network Coding, In Proc. of Australian Communications Theory Workshop (AusCTW 2008), Jan. 2008, pp. 95-100.

[105]. P. Popovski and H. Yomo, Physical Network Coding in Two-way Wireless Relay Channels, In Proc. of 26th Annual IEEE Conf. on Computer Communications (INFOCOM 2007), Anchorage, AK, USA, 2007.

[106]. C. Peng, Q. Zhang, M. Zhao, et al. On the Performance Analysis of Network-coded Cooperation in Wireless Networks, In Proc. of 26th Annual IEEE Conf. on Computer Communications (INFOCOM 2007), Anchorage, AK, USA, 2007.

[107]. S. L. Zhang, S.C. Liew, et al. Joint Design of Network Coding and Channel Decoding for Wireless Networks, In Proc. of IEEE Wireless Communication & Networking Conf (WCNC), Hong Kong, 2007.

[108]. S. Jaggi, M. Langberg, T. Ho, et al. Correction of Adversarial errors in Networks, In Proc. of 2005 International Symposium on Information Theory and its Applications, Adelaide, Australia, 2005.

[109]. Liu Yajie and Dou Wenhua, The P2P Streaming Media Based on Network Coding, Journal of Computer Engineering & Science, 2006, 28 (9): 33-38 (in Chinese).

[110]. M. Wang and B.C. Li, Lava: A Reality Check of Network Coding in Peer-to-Peer Live Streaming, In Proc. of 26th Annual IEEE Conf. on Computer Communications (INFOCOM 2007), Anchorage, AK, USA, 2007.

[111]. E. Erez and M. Feder, Convolutional Network Codes, IEEE International Symposium

on Information Theory (ISIT 2004), p. 146, June 27th-July 2nd, 2004.

[112]. C. Fragouli and E. Soljanin, A Connection between Network Coding and Convolutional Codes, IEEE International Conference on Communications, vol. 2, pp. 661-666, Jun. 2004.

[113]. C. K. Ngai and R. W. Yeung, Multisource Network Coding with Two Sinks, In Proc. of International Conference on Communications, Circuits and Systems (ICCCAS), pp. 34-37, Jun. 27-29, 2004.

[114]. J. Barros and S. D. Servetto, Network Information Flow with Correlated Sources, IEEE Transactions on Information Theory, vol. 52, No. 1, pp. 155-170, Jan. 2006.

[115]. S. Riis and R. Ahlswede, Problems in Network Coding and Error Correcting Codes, Netcod 2005, Italy, Apr. 2005.

攻读硕士学位期间发表的论文

1. Yan Zhang, Chengqi Xu, Feng Wang, A Novel Scheme for Secure Network Coding Using One-time Pad, 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009.
2. 张岩，“一种改进的安全网络编码方案的研究”，全国第十五届信息论学术年会，2008。