一种防窃听的随机网络编码

周业军，李 晖，马建峰
(西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071)

摘要：针对应用随机网络编码进行文件传输时的安全问题，提出了一种防窃听的网络编码算法.应用该算法，窃听者得不到关于信源的任何有意义的信息，称之为弱安全.该算法通过舍弃少量带宽使得随机网络编码能以很高的概率达到弱安全性的要求.另外，当信源和信宿共享有秘密信道时，秘密信道编码算法达到弱安全性要求的概率为 1，且能达到网络的最大流.该编码算法仅是在原随机编码体制的基础上对信源和信宿进行了改变，中间节点编码保持不变.

关键词：网络编码；窃听；网络安全
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1001-2400(2009)04-0696-06

Random network coding against the eavesdropping adversaries

ZHOU Ye-jun, *LI Hui*, *MA Jian-feng*
(Ministry of Education Key Lab. of Computer Network and Information Security, Xidian Univ., Xi'an 710071, China)

Abstract: An algorithm against eavesdropping adversaries is presented. By means of this algorithm an eavesdropper is unable to get any meaningful information about the source, which we call practical security. We show that if we give up a small amount of overall capacity, then a random code achieves the practically secure condition at a much higher probability. When there is a low rate secret channel between the source and destination, the shared secret algorithm not only achieves the max-flow but also the practically secure condition at a probability of one. Furthermore, implementing the algorithm involves only a slight modification of the source and destination with the operations at the intermediate nodes remaining unchanged.

Key Words: network coding; eavesdropping; network security

2000 年 Ahlswede 等人[1]首次提出了网络编码理论，通过网络编码可以实现网络流量的最大化.2003 年，Li, Yeung 和 Cai[2]证明了线性网络编码就可以实现网络的最大流.随后 T. Ho 等人[3-4]提出了随机网络编码理论，其思想是在网络中参与传输的节点，其输出信道上传输的数据是该点多条输入信道上传输的数据的随机线性组合，他们并且证明了接收节点能以很大的概率正确恢复出信源所发送的信息.

网络编码提高了网络的吞吐量和可靠性[5]，但同时也带来了不可忽视的安全问题，主要包括污染和窃听两类问题.T. Ho 等[6]提出了一种能检测污染攻击是否存在的网络编码.Jaggi 等人[7]针对攻击者能力的不同设计了一种适应性的安全网络编码.Nutman 和 Langberg[8]对 Jaggi 等人的算法进行了改进.Cai 和 Yeung[9]首次提出了网络纠错编码，Zhang[10-11]给出了存在信道噪声时网络纠错编码的具体编译码算法.孙岳等[12]考虑了网络编码下的多播网络故障恢复问题.

Cai 和 Yeung[13]针对能窃听网络中一定数量信道的窃听者设计了一种信息论安全的网络编码并且给出了具体的编码方法.J. Feldman 等人[14]也考虑了此类问题，并通过舍弃少量带宽给出了在较小的有限域上

收稿日期：2008-10-27
基金项目：国家自然科学基金资助(60772136；60633020)；863 国家高技术研究发展计划资助(2007AA01Z435；2007AA01Z429)；广西信息与通讯技术重点实验室资助
作者简介：周业军(1983-)，男，西安电子科技大学博士研究生，E-mail：yjzhou@mail.xidian.edu.cn.

的编码算法. T. Chan1 和 A. Grant[15] 给出了安全网络编码所能达到的多播容量的界限. Rouayheb 和 Soljanin[16] 从另外一个角度解决了此类问题. Silva[17] 等人则用 Rank-Metric Codes 的方法解决了此类问题.

在实际应用中对安全性的要求并不一定要像信息论安全这样高. 例如,如果窃听者得到了关于信源的两个比特的异或 $b_1 \oplus b_2$,他虽然得到了关于信源的一个比特的信息,但他却无法得到关于信源的任何"有意义"的信息,即他无法得到 b_1 或 b_2. 在实际应用中这样的安全性就足够了. 这样的安全性是弱于信息论安全的,称之为"弱安全". Bhattad 和 Narayanan[18] 最早分析了这样一种弱安全模型. 当窃听者窃听到的信道数小于网络的最大流时他们设计出了一种弱安全的网络编码. 文[19]也考虑了此类弱安全模型,并给出了编码方法. 当窃听者的计算能力有限时,K. Jain[20] 利用单向函数同样设计了一种弱安全的网络编码体制. Vilela[21] 用加密部分编码系数的方法也给出了一种弱安全的编码方法. Lima 等[22] 则考虑了窃听者窃听节点而不是信道这样一种更一般的情况.

当窃听者窃听到的信道数小于网络的最大流值时,笔者通过在信源消息中加入少量冗余使得随机网络编码弱安全的概率远高于 Bhattad 和 Narayanan[18] 给出的概率,其代价仅仅是少量的带宽. 当信源和信宿共享有一秘密信道时,文中秘密信道编码算法可使随机网络编码能防窃听的概率为 1 且能在弱安全的条件下达到网络的最大流.

1　基本模型与概念

1.1　网络模型

对于一个无环多播网络 $G=(V, E)$,V 是点的集合,E 是信道的集合,信源以单位时间产生如下形式的消息:

$$\boldsymbol{X}=\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{pmatrix}=\begin{pmatrix} \boldsymbol{X}_1 \\ \boldsymbol{X}_2 \\ \vdots \\ \boldsymbol{X}_m \end{pmatrix},$$

称 $\boldsymbol{X}_i, i=1,2,\cdots,m$ 为信息包,其中 $x_{ij} \in F_q$(这里 q 为一大素数).

对于线性网络编码,信道 $e_j \in E$ 传输的数据可写作 $\boldsymbol{\Gamma}_{e_j} X$,这里 $\boldsymbol{\Gamma}_{e_j}$ 是一个 m 维向量,称之为信道$e_j \in E$ 上的全局编码向量.

1.2　攻击模型

考虑单信源单信宿的简单模型,多信宿的情况与此类似. 定义信源为 Alice,信宿为 Bob. 攻击者 Calvin 通过窃听一些信道来获取 Alice 发给 Bob 的信息. 假设一个信道集合 $\Lambda=\{\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_{|\Lambda|}\}$,其中$\boldsymbol{A}_i \in E$ 是 Calvin 单位时间能窃听到的信道且这个集合是不随时间而变的. $\boldsymbol{A}_i$ 表示由 Calvin 窃听到的信道 $\boldsymbol{A}_i \in E$ 上所有线性无关的全局编码向量组成的矩阵. 这样 Calvin 窃听到的消息可以表示为 $\boldsymbol{A}_i X$. $\boldsymbol{A}_i$ 的行数用 k_i 来表示,并定义$k=\max_i k_i$. 用"$\boldsymbol{A}_i \in \Lambda$ 的行空间"来表示 $\boldsymbol{A}_i$ 的行空间,以 $\boldsymbol{a}_{i,j}$ 为向量表示矩阵 $\boldsymbol{A}_i$ 的第 j 行.

1.3　概　　念

网络最大流:Alice 在单位时间内,理论上最多能给 Bob 发的信息包的个数. 文中假设信源 Alice 与信宿 Bob 之间的最大流均为 m.

多播容量:在具体的编码体制下,当存在攻击者时,Alice 在单位时间内能给 Bob 发的信息包的个数.

弱安全:以 M 表示任意消息的集合,U 表示信源消息 X 的一个子集,如果 $I(U; M)=0$ 称 M 没有给出关于U 的任何信息. 如果 $I(\boldsymbol{X}_i; M)=0, \forall \boldsymbol{X}_i \in U$ 称M 没有给出关于U 的任何有意义的信息. 考虑上述定义的特殊情况,当$U=X$ 时有:如果 $I(X; M)=0$ 称 Calvin 没有得到关于 X 的任何信息,其中 M 是 Calvin 所窃听到的消息. Cai 和 Yeung[13] 考虑的便是这种情况,称为信息论安全. 如果 $I(\boldsymbol{X}_i; M)=0, \forall \boldsymbol{X}_i \in X$ 称 Calvin 没有得到关于 X 的任何有意义的信息,称为"弱安全",同样 M 为 Calvin 所窃听到的消息.

例如:如果 Calvin 得到了 $\boldsymbol{X}_1 \oplus \boldsymbol{X}_2$,其中 $\boldsymbol{X}_1$ 和 $\boldsymbol{X}_2$ 为信源消息的两个信息包. 这里 $I(\boldsymbol{X}_1, \boldsymbol{X}_2; \boldsymbol{X}_1 \oplus \boldsymbol{X}_2)=I(\boldsymbol{X}_1; \boldsymbol{X}_1 \oplus \boldsymbol{X}_2)+I(\boldsymbol{X}_2; \boldsymbol{X}_1 \oplus \boldsymbol{X}_2 \mid \boldsymbol{X}_1) \neq 0$,而 $I(\boldsymbol{X}_1; \boldsymbol{X}_1 \oplus \boldsymbol{X}_2)=I(\boldsymbol{X}_2; \boldsymbol{X}_1 \oplus \boldsymbol{X}_2)=0$.

如图 1 所示,图中网络的最大流为 2,假设 Calvin 能窃听图中网络的任一信道,$\boldsymbol{X}_1$ 和 $\boldsymbol{X}_2$ 是两个信息包,$\boldsymbol{W}$ 是一个与 $\boldsymbol{X}_1$ 和 $\boldsymbol{X}_2$ 无关的随机向量. 图 1(a)中表示的是 Cai 和 Yeung[13] 提出的信息论安全的网络编码. 图 1(a)所示的编码体制中,每个信道上传输的消息的形式为 $a\boldsymbol{X}+b\boldsymbol{W}$, $b\neq 0$,显然当 $b\neq 0$ 时 $I(\boldsymbol{X}_1;\ a\boldsymbol{X}_1+b\boldsymbol{W})=0$. 在信息论安全的条件下,该网络能达到的多播容量是 1. 当对安全性的要求降低到弱安全时(如图 1(b)所示),便可以达到网络的最大流 2.

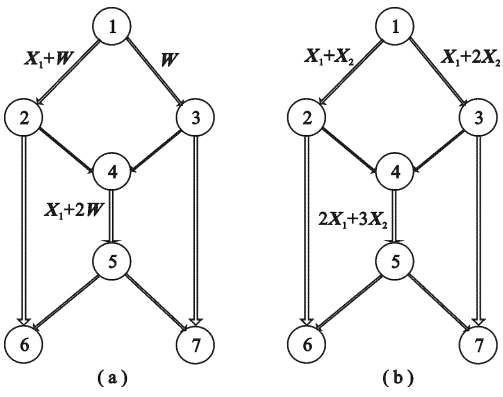

图 1 网络

如果 Alice 传输 $\boldsymbol{X}$ 的线性变换 $\boldsymbol{PX}$,而不是 $\boldsymbol{X}$ 本身,那么在信道 $e_j\in E$ 传输的消息将变成 $\boldsymbol{\Gamma}_{e_j}\boldsymbol{PX}$,其中 $\boldsymbol{P}$ 是一个 Calvin 不知道的 $m\times m$ 阶矩阵. 这样,即使 Calvin 能窃听网络中的所有信道,他得到的也只是 $\boldsymbol{X}$ 的线性变换 $\boldsymbol{PX}$. 当 $|\boldsymbol{P}|\neq 0$ 时,$I(\boldsymbol{X};\ \boldsymbol{PX})\neq 0$,而 $I(\boldsymbol{X}_i;\ \boldsymbol{PX})=0$. 也就是说,Calvin 得不到关于信源的任何有意义的信息. 笔者考虑的便是在 Calvin 不知道矩阵 $\boldsymbol{P}$ 的情况下的弱安全的网络编码.

2 弱安全网络编码及随机网络编码

2.1 弱安全网络编码

Alice 的编码算法:Alice 通过以下步骤对 $\boldsymbol{X}$ 进行编码.

首先,选择一个随机数 r 并用它生成一个如下形式的范德蒙行列式:

$$\boldsymbol{P}=\begin{pmatrix} r & r+1 & r+2 & \cdots & r+m-1 \\ r^2 & (r+1)^2 & (r+2)^2 & \cdots & (r+m-1)^2 \\ \vdots & \vdots & \vdots & & \vdots \\ r^m & (r+1)^m & (r+2)^m & \cdots & (r+m-1)^m \end{pmatrix}, \tag{1}$$

对消息 $\boldsymbol{X}$ 左乘 $\boldsymbol{P}$ 得

$$\hat{\boldsymbol{X}}'=\boldsymbol{PX}=\begin{pmatrix} \hat{x}_{11} & \hat{x}_{12} & \cdots & \hat{x}_{1n} \\ \hat{x}_{21} & \hat{x}_{22} & \cdots & \hat{x}_{2n} \\ \vdots & \vdots & & \vdots \\ \hat{x}_{m1} & \hat{x}_{m2} & \cdots & \hat{x}_{mm} \end{pmatrix}, \tag{2}$$

在 $\hat{\boldsymbol{X}}'$ 每个信息包中加入一个单位冗余得到如下的新信源消息 $\hat{\boldsymbol{X}}$:

$$\hat{\boldsymbol{X}}=\begin{pmatrix} \hat{x}_{11} & \hat{x}_{12} & \cdots & \hat{x}_{1n} & r \\ \hat{x}_{21} & \hat{x}_{22} & \cdots & \hat{x}_{2n} & q_1 \\ \vdots & \vdots & & \vdots & \vdots \\ \hat{x}_{m1} & \hat{x}_{m2} & \cdots & \hat{x}_{mm} & q_{m-1} \end{pmatrix}, \tag{3}$$

其中 $q_1,\cdots,q_{m-1}$ 是随机数.

这里 $r,q_1,\cdots,q_{m-1}$ 使得多播容量由 m 降低到 $m-m/n$,详见推论 1.

Bob 的解码算法:Bob 首先解码出 Alice 编码后的消息 $\hat{\boldsymbol{X}}$ 并得到 r,行列式 $\boldsymbol{P}$ 可以由 r 得到. Bob 最后对去掉冗余后的消息 $\boldsymbol{PX}$ 左乘 $\boldsymbol{P}^{-1}$ 而得到原始信源消息 $\boldsymbol{X}$.

注意到,以上编码体制仅是在原随机网络编码体制的基础上对信源和信宿进行了改变,中间节点编码保持不变.

定理 1 当窃听者 Calvin 能窃听到的信道数小于网络的最大流,即 $k=\max\limits_{\boldsymbol{A}_i\in\Lambda}\operatorname{rank}(\boldsymbol{A})<m$ 时,以上对信源和信宿的编译码算法可以达到弱安全性的要求,其编码复杂度为 $O(m^2n)$.

证明 以上算法中,Alice 传输的是编码后的新消息 $\hat{\boldsymbol{X}}$,因此 Calvin 能窃听到的消息是 $\boldsymbol{A}_i\hat{\boldsymbol{X}}$. 只要 Calvin 得不到 Alice 开始选的数 r,他便不能得到关于 $\boldsymbol{X}$ 的全局编码向量,进而他也就得不到关于 $\boldsymbol{X}$ 的任何

有意义的信息.也就是说只要Calvin对他所得到的消息 $\boldsymbol{A}_i\hat{\boldsymbol{X}}$ 作线性变换得不到 r,那么

$$\boldsymbol{b}_i\boldsymbol{A}_i\hat{\boldsymbol{X}} \neq [a,0,\cdots,0]\hat{\boldsymbol{X}} \quad , \quad \forall\, \boldsymbol{b}_i,i,a \neq 0 \quad , \tag{4}$$

其中 $\boldsymbol{b}_i$ 是域 F_{q^m} 上的一个 $k_i \times m$ 矩阵.

Alice 通过在新信源消息 $\hat{\boldsymbol{X}}$ 上再左乘一个 $m \times m$ 阶矩阵 $\boldsymbol{C}$ 来达到所述弱安全性条件,这样条件(4)变为

$$\boldsymbol{b}_i\boldsymbol{A}_i\boldsymbol{C}\hat{\boldsymbol{X}} \neq [a,0,\cdots,0]\hat{\boldsymbol{X}} \quad . \tag{5}$$

上式两边同右乘以 $\boldsymbol{C}^{-1}$ 得

$$\boldsymbol{b}_i\boldsymbol{A}_i \neq [a,0,\cdots,0]\boldsymbol{C}^{-1} \quad . \tag{6}$$

只要取矩阵 $\boldsymbol{C}^{-1}$ 的第一行不在每个 $\boldsymbol{A}_i \in \Lambda$ 所张成的空间中,条件(6)便可以满足.

另外,即使 Calvin 得到了数 r,他也不一定就能恢复出任何信源消息,如下式所示:

$$\boldsymbol{b}_i\boldsymbol{A}_i\boldsymbol{P} \neq \boldsymbol{I}_{m,n} \quad ,\forall \quad \boldsymbol{b}_i,n,i,a \neq 0 \quad . \tag{7}$$

上式两边同右乘以矩阵 $\boldsymbol{P}^{-1}$ 得

$$\boldsymbol{b}_i\boldsymbol{A}_i \neq \boldsymbol{I}_{m,n}\boldsymbol{P}^{-1} \quad . \tag{8}$$

只要取矩阵 $\boldsymbol{P}^{-1}$ 的每一个行向量不在每个 $\boldsymbol{A}_i \in \Lambda$ 所张成的空间中,条件(8)便可以满足.

推论 1　在一个最大流为 m 的网络中,如果能被同时窃听的信道数小于其最大流,在弱安全的条件下能达到的多播容量为 $m - m/n$ (m/n 为 Alice 加入信源消息中的冗余所带来的).

证明　文献[2]证明了线性网络编码就可以实现网络的最大流,定理 1 中证明了当 $k < m$ 时可以通过对信源和信宿的变换而构造一个弱安全的编码算法,引理得证.

2.2　随机网络编码的弱安全性

定理 2　给定网络,当 $k = \max\limits_{\boldsymbol{A}_i \in \Lambda} \operatorname{rank}(\boldsymbol{A}) < m$ 时,对其中间节点应用随机编码时 Calvin 能窃听到有意义信息的概率小于 $|\Lambda|^2 k^2 m / q^{2(m-k)}$.

证明该定理前,首先证明以下两个引理.

由定理 1 的证明,只要 Calvin 对他所得到的消息 $\boldsymbol{A}_i\hat{\boldsymbol{X}}$ 作线性变换得不到 r,他就得不到关于 X 的任何有意义的信息.

引理 1　对给定网络的中间节点应用随机网络编码时,Calvin 得到数 r 的概率小于 $|\Lambda| k / q^{(m-k)}$.

证明　当 $\boldsymbol{A}_i$ 的行向量张成的空间中包含 $[a,0,\cdots,0]$ 时 Calvin 能恢复出 r,这里 $\boldsymbol{A}_i$ 中有 k_i 行是相互独立的,其余各行是它们的线性组合. Calvin 能得到数 r 的概率可以用如下的方法求得:

设 ε_1 是行向量空间中不包含 $[a,0,\cdots,0]$ 的矩阵 $\boldsymbol{A}_i$ 的个数,则有

$$\varepsilon_1 \geqslant (q^m - q)(q^m - q^2)\cdots(q^m - q^{k_i}) \quad . \tag{9}$$

当 $\boldsymbol{A}_i$ 中各元素在 F_q 中取值时,$\boldsymbol{A}_i$ 的所有可能的取值个数为 q^{mk_i}. 式(9) 右端中的每个部分为给定 $\boldsymbol{a}_{i,1},\boldsymbol{a}_{i,2},\cdots,\boldsymbol{a}_{i,j-1}$ 时使得 $\{\boldsymbol{a}_{i,1},\cdots,\boldsymbol{a}_{i,j}\}$ 所张成空间中不包含 $[a,0,\cdots,0]$ 的所有可能的 $\boldsymbol{a}_{i,j}$ 取值个数,其中 a 是一个元素,$\boldsymbol{a}_{i,j}$ 是向量. 如果用 p_i 来表示 $\boldsymbol{A}_i$ 的行向量空间中不包含 $[a,0,\cdots,0]$ 的概率,则有

$$p_i \geqslant \Big(\prod_{j=1}^{k_i}(q^m - q^j)\Big)\Big/q^{mk_i} = \prod_{j=1}^{k_i}\left(1 - \frac{1}{q^{(m-j)}}\right) \quad , \tag{10}$$

进而得到 Calvin 不能得到 r 的概率 p_p:

$$\begin{aligned} 1 - p_p &\leqslant \sum_i (1 - p_i) \leqslant \sum_i \left(\prod_{j=1}^{k_i}\left(1 - \frac{1}{q^{(m-j)}}\right)\right) \leqslant \\ &\sum_i \left(1 - \left(1 - \frac{1}{q^{(m-k_i)}}\right)^{k_i}\right) \leqslant \sum_i \frac{k_i}{q^{(m-k_i)}} \leqslant \frac{|\Lambda| k}{q^{(m-k)}} \quad . \end{aligned} \tag{11}$$

由定理 1 的证明,即使 Calvin 得到了数 r,他也不一定就能恢复出任何信源消息.

引理 2　在 Calvin 能得到 r 的前提下,他能得到信源的有意义信息的概率小于 $|\Lambda| km / q^{(m-k)}$.

证明　设 ε_2 是行向量空间中不包含 $\boldsymbol{P}^{-1}$ 的行向量的矩阵 $\boldsymbol{A}_i$ 的个数. 同上,$\boldsymbol{A}_i$ 中各元素在 F_q 中取值.

$$\varepsilon_2 \geqslant (q^m - qm)(q^m - q^2 m)\cdots(q^m - q^{k_i} m) \quad . \tag{12}$$

如用 p_i' 来表示 $\boldsymbol{A}_i$ 的行向量空间中不包含 $\boldsymbol{P}^{-1}$ 行向量的概率,则有

$$p_i' \geqslant \Big(\prod_{j=1}^{k_i}(q^m - mq^j)\Big)\Big/q^{mk_i} = \prod_{j=1}^{k_i}\left(1 - \frac{m}{q^{(m-j)}}\right) \quad , \tag{13}$$

进而得到在 Calvin 能得到 r 的前提下,得不到信源的有意义信息的概率 p_s 为

$$1-p_s \leqslant \sum_i (1-p_i) \leqslant \sum_i \left(\prod_{j=1}^{k_i}\left(1-\frac{m}{q^{(m-j)}}\right)\right) \leqslant$$
$$\sum_i \left(1-\left(1-\frac{m}{q^{(m-k_i)}}\right)^{k_i}\right) \leqslant \sum_i \frac{mk_i}{q^{(m-k_i)}} \leqslant \frac{|\Lambda|km}{q^{(m-k)}} \quad . \tag{14}$$

下面证明定理 2.

证明　Calvin 要想得到关于 X 的有意义的信息必须先得到 r，进而再对窃听到的信息作线性变换以得到一些信源消息. 由上边的引理，Calvin 得到数 r 的概率小于 $|\Lambda|k/q^{(m-k)}$，在能得到 r 的前提下，他能得到信源的有意义信息的概率小于 $|\Lambda|km/q^{(m-k)}$. 于是，随机网络编码弱安全的概率 p_{ps} 为

$$1-p_{ps}=(1-p_p)(1-p_s) \leqslant |\Lambda|^2k^2m/q^{2(m-k)} \quad . \tag{15}$$

3　秘密信道模型

此模型下，Alice 和 Bob 共享有一个秘密信道，窃听者无法窃听到秘密信道上所传输的消息. 此模型下的编码算法称为秘密信道编码算法.

Alice 的编码算法：Alice 经秘密信道向 Bob 传输一组随机数 $r_1,\cdots,r_m$.

Alice 用所述的随机数 $r_1,\cdots,r_m$ 生成一个范德蒙行列式 $\boldsymbol{P}$：

$$\boldsymbol{P}=\begin{pmatrix} r_1 & r_2 & \cdots & r_m \\ r_1^2 & r_2^2 & \cdots & r_m^2 \\ \vdots & \vdots & & \vdots \\ r_1^m & r_2^m & \cdots & r_m^m \end{pmatrix} \quad , \tag{16}$$

Alice 对消息 $\boldsymbol{X}$ 左乘 $\boldsymbol{P}$ 得

$$\boldsymbol{X}'=\boldsymbol{PX}=\begin{pmatrix} x'_{11} & x'_{12} & \cdots & x'_{1n} \\ x'_{21} & x'_{22} & \cdots & x'_{2n} \\ \vdots & \vdots & & \vdots \\ x'_{m1} & x'_{m2} & \cdots & x'_{mn} \end{pmatrix} \quad , \tag{17}$$

Alice 最后要传输的信息为上述 $\boldsymbol{X}'$.

Bob 的解码算法：Bob 首先通过秘密信道得到随机数 $r_1,r_2,\cdots,r_m$，计算出行列式 $\boldsymbol{P}$. 然后对消息 $\boldsymbol{PX}$ 左乘 $\boldsymbol{P}^{-1}$ 而得到原始消息 $\boldsymbol{X}$.

定理 3　给定网络，应用随机网络编码时，当窃听者能窃听网络中的所有信道(除秘密信道外)时，秘密信道编码算法能以概率 1 达到弱安全性的要求，其计算复杂度为 $O(m^2n)$.

证明　由于随机数 $r_1,\cdots,r_m$ 由秘密信道传输，因此 Calvin 无法得到 $r_1,\cdots,r_m$，进而无法得到关于 $\boldsymbol{X}$ 的全局编码向量，他也就得不到关于 $\boldsymbol{X}$ 的任何有意义的信息.

推论 2　在一个最大流为 m 的网络中，如果信源与信宿间有一秘密信道，那么在弱安全的条件下能达到的多播容量为 m.

证明　由定理 2 和引理 1 的证明，引理 2 得证.

4　总　　结

网络编码提高了网络的吞吐量，但同时也带来了不可忽视的安全问题，窃听是网络遭受的主要威胁之一. 针对应用网络编码进行文件传输时如何防窃听的问题，笔者设计了一种弱安全的编码算法并给出了随机编码达到这种弱安全性的概率. 首先，当舍弃少量带宽时，对信源消息的编码能使随机网络编码以概率 $1-|\Lambda|^2k^2m/q^{2(m-k)}$ 达到弱安全性的要求. 其次，当信源和信宿共享有秘密信道时，笔者给出的秘密信道编码算法不仅能防窃听而且在弱安全的条件下可达到网络的最大流. 最后，笔者给出的编码算法仅对信源和信宿的编译码算法进行了改变，中间结点编码保持不变.

参考文献：

[1]　Ahlswede R, Cai N, Li S-Y R, et al. Network Information Flow [J]. IEEE Trans on Inf Theory, 2000, 46(4):

1204-1216.
[2] Li S-Y R, Yeung R W, Cai N. Linear Network Coding [J]. IEEE Trans on Inf Theory, 2003, 49(2): 371-381.
[3] Ho T, Koetter R, Medard M, et al. The Benefits of Coding Over Routing in a Randomized Setting [C]//IEEE Intl Symp Inf Theory. Yokohama: IEEE Press, 2003: 442.
[4] Ho T, Medard M, Shi J, et al. On Randomized Network Coding [EB/OL]. [2007-06-08]. http://web.mit.edu/people/medard/allerton3.pdf.
[5] 王静, 刘景美, 王新梅, 等. 一种网络编码的多播路由算法 [J]. 西安电子科技大学学报, 2008, 35(1): 71-75.
Wang Jing, Liu Jingmei, Wang Xinmei, et al. Multicast Routing Algorithm for Network Coding [J]. Journal of Xidian University, 2008, 35 (1): 71-75.
[6] Ho T C, Leong B, Koetter R, et al. Byzantine Modification Detection in Multicast Networks Using Randomized Network Coding [C]//IEEE Intl Symp Inf Theory. Chicago: IEEE Press, 2004: 144.
[7] Jaggi S, Langberg M, Katti S. Resilient Network Coding in the Presence of Byzantine Adversaries [C]//26th IEEE International Conference on Computer Communications. Anchorage: IEEE Press, 2007: 616 - 624.
[8] Nutman L, Langberg M. Adversarial Models and Resilient Schemes for Network Coding [C]//IEEE Intl Symp Inf Theory. Toronto: IEEE Press, 2008: 171-175.
[9] Cai N, Yeung R W. Network Coding and Error Correction [C]//IEEE Inform Theory Workshop. Bangalore: IEEE Press, 2002: 119-122.
[10] Zhang Z. Network Error Correction Coding in Packetized Networks [C]//IEEE Information Theory Workshop. Chengdu: IEEE Press, 2006: 433-437.
[11] Zhang Z. Linear Network Error Correction Codes in Packet Networks [J]. IEEE Trans on Inf Theory, 2008, 54(1): 209-218.
[12] 孙岳, 杨远, 王新梅. 基于网络编码的多播网络故障恢复[J]. 西安电子科技大学学报, 2007, 34(1): 122-125.
Sun Yue, Yang Yuan, Wang Xinmei. Multicast Fault Recovery on Network Coding [J]. Journal of Xidian University, 2007, 34(1): 122-125.
[13] Cai N, Yeung R W. Secure Network Coding [C]//IEEE Intl Symp Inf Theory. Lausanne: IEEE Press, 2002: 323.
[14] Feldman J, Malkin T, Stein C, et al. On the Capacity of Secure Network Coding [EB/OL]. [2007-06-08]. http://people.csail.mit.edu/jonfeld/pubs/sflow_Allerton04_final.pdf.
[15] Chanl T, Grant A. Capacity Bounds for Secure Network Coding [C]//Communication Theory Workshop. Australian: IEEE Press, 2008: 95-100.
[16] Rouayheb S Y E, Soljanin E. On Wiretap Network II [C]//IEEE Intl Symp Inf Theory. Nice: IEEE Press, 2007: 551-555.
[17] Silva D, Kschischang F R. Security for Wiretap Networks Via Rank-Metric Codes [C]//IEEE Intl Symp Inf Theory. Toronto: IEEE Press, 2008: 176-180.
[18] Bhattad K, Narayanan K R. Weakly Secure Network Coding [EB/OL]. [2007-05-22]. http://netcod.org/papers/06Bhattad N-final.pdf.
[19] Silva D, Kschischang F R. Universal Secure Network Coding Via Rank-Metric Codes [EB/OL]. [2008-11-10]. http://arxiv.org/PS_cache/arxiv/pdf/0809/0809.3546v1.pdf.
[20] Jain K. Security Based on Network Topology Against the Wiretapping Attack [J]. IEEE Wireless Communications, 2004, 11(1): 68-71.
[21] Vilela J P, Lima L, Barros J. Lightweight Security for Network Coding [C]//Proc of the IEEE International Conference on Communications (ICC). Beijing: IEEE Press, 2008: 1750-1754.
[22] Lima L, Medard M, Barros J. Random Linear Network Coding: a Free Cipher? [C]//IEEE Intl Symp Inf Theory. Nice: IEEE Press, 2007: 546-550.

(编辑: 郭　华)