一种安全的纠错网络编码

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　西安　710071)

摘　要：该文利用消息空间的所有子空间上的一种度量，给出了一种安全的纠错网络编码。首先，此度量下的最小距离译码法可以纠正一定维数的错误。另外，在此编码方法下，当攻击者能窃听到的信道数目小于网络的最大流时，攻击者得不到关于信源的任何信息。最后，当攻击者能窃听网络中所有信道时，本文通过让信源和信宿共享一个随机数生成器和一个秘钥，进一步给出了能防此类强攻击者的安全纠错网络编码。

关键词：网络编码；纠错；窃听；安全
中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1009-5896(2009)09-2237-05

Secure Error-Correction Network Coding

Zhou Ye-jun　　Li Hui　　Ma Jian-feng
(*Key lab of CNIS Ministry of Education Xidian University*, *Xi'*an, 710071, *Shaanxi*, *China*)

Abstract: In this paper, a secure error-correcting network coding is proposed using a metric on the space of all subspaces of a message vector space. It shows that a minimum distance decoder for this metric can correct errors of a limited dimension. On the other hand, when the number of channels the adversary can eavesdrop on is less than the max-flow of a network, the adversary can not get any information about the source. Furthermore, when the source and the destination shares a Pseudo-Random number generator and a secret key, the coding scheme can prevent adversary who can eavesdrop on all the channels of a network.

Key words: Network coding; Error correction; Eavesdropping; Security

1　引言

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 Ho 等人[3]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。Geil1 等人[4]也证明了此问题。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。其中污染主要指信道噪声、连接失败、网络阻塞、及恶意篡改等。

Cai 和 Yeung[6]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。Feldman 等[7]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的编码算法。Chan1 和 Grant[8]则给出了安全网络编码所能达到的多播容量的界限。Bhattad 和 Narayanan[9]首次分析了一种弱安全模型，当窃听者窃听到的信道数小于网络的最大流时设计了一种弱安全的网络编码。当窃听者的计算能力有限时，Jain[10]利用单向函数同样设计了一种弱安全的网络编码体制。Lima 等[11]则考虑了窃听者窃听结点而不是信道这样一种更一般的情况。

Ho 等[12]提出了一种能检测污染攻击是否存在的网络编码。Jaggi 等人[13]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[14]则对 Jaggi 等人的算法进行了改进。Yu 等人[15]利用同态签名给出了一种防污染的网络编码。Cai 和 Yeung[16−18]首次提出了纠错网络编码，并且给出了编码域。随后 Yang 和 Yeung[19, 20]给出了更加精确的编码域。Zhang[21, 22]以及 Yeung[23]则给出了存在信道噪声时网络纠错编码的具体的编译码算法。

Koetter 和 Kschischang[24]把传输的消息看成是一个向量空间 $\boldsymbol{V}$，而不是经典编码理论中的向量。向量空间 $\boldsymbol{V}$ 的基由要传输的消息向量生成。在随机网络编码的变换下(没有污染的情况下)，空间 $\boldsymbol{V}$ 是

2008-10-06收到，2009-03-17改回
国家自然科学基金(60772136，60633020)，国家 863 计划项目(2007AA01Z435，2007AA01Z429) 和广西信息与通讯技术重点实验室资助课题

保持不变的。信宿收到的向量空间$\boldsymbol{U}$由接收到的信息包作为基来张成。当$\boldsymbol{U}$和$\boldsymbol{V}$的交集足够大时，信宿便可以正确译码。

本文同时考虑污染和窃听这两类攻击者，即：攻击者可以污染部分信道，同时窃听另一部分信道。Jaggi等人[13]考虑了此类模型，在他们的模型中攻击者利用窃听到的信息来对传输的信息进行污染，但他们的算法不能防窃听。Ngai和Yang[25]构造了一种能同时防窃听和防污染的安全纠错网络编码，但在他们的模型中，信宿需要知道所有信源消息的集合，这在很多情况下是不实际的。另外，针对能窃听网络中所有信道的窃听者，本文给出了一种能防此类强窃听者的编码方法。

本文的主要工作在于，在文献[24]中编码体制的基础上，给出了一种安全的纠错网络编码体制。本文中编码体制可以使得信源消息安全无误地传输到信宿。本文进一步给出了当攻击者能窃听网络中所有信道时的安全纠错网络编码。

2 基本概念

本文假设攻击者在较长的时间段里污染网络中固定的信道。下面，将给出本文的网络模型并简要介绍文献[24]中的编码体制。

2.1 网络模型

本文只考虑单信源单信宿的简单情况，并设信源为 Alice，信宿为 Bob，攻击者 Calvin 通过窃听网络中的信道来获取 Alice 传送给 Bob 的消息，并在网络中加入污染消息。

假设 Alice 传输的消息的形式如下：

$$\boldsymbol{u}=\begin{pmatrix} u_{01} & u_{02} & \cdots & u_{0n} \\ u_{11} & u_{12} & \cdots & u_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{k-1,1} & u_{k-1,2} & \cdots & u_{k-1,n} \end{pmatrix}=\begin{pmatrix} \boldsymbol{u}_0 \\ \boldsymbol{u}_1 \\ \vdots \\ \boldsymbol{u}_{k-1} \end{pmatrix} \tag{1}$$

我们称$\boldsymbol{u}_i, i=0,1,\cdots,k-1$为信息包。

设$\boldsymbol{W}$为F_q上的N维向量空间。所有的传输和接收到的信息包都是$\boldsymbol{W}$上的向量。此网络模型中所有传输和接收到的向量空间都是$\boldsymbol{W}$的子空间，且传输的向量空间是由要传输的信息包生成的。记$P(\boldsymbol{W})$为$\boldsymbol{W}$的所有子空间。$\boldsymbol{V}\in P(\boldsymbol{W})$的维数记为$\dim(\boldsymbol{V})$。$P(\boldsymbol{W},l)$表示$\boldsymbol{W}$的所有的维数为$l$的子空间。

2.2 编码算法

给定消息$\boldsymbol{u}$，传输的向量空间$\boldsymbol{V}$生成如下：

设$\boldsymbol{F}=F_{q^n}$为有限域F_q的一个扩域。$\boldsymbol{F}$可看作是F_q上的一个n维向量空间。设$\boldsymbol{A}=\{\boldsymbol{a}_1,\cdots,\boldsymbol{a}_l\}$为此空间上的一组线性无关的向量，这组向量张成了$\boldsymbol{F}$上的一个子空间$\langle\boldsymbol{A}\rangle\subseteq\boldsymbol{F}$。显然$l\le n$，向量空间$\boldsymbol{W}=\langle\boldsymbol{A}\rangle\oplus\boldsymbol{F}=\{(\alpha,\beta):\alpha\in\langle\boldsymbol{A}\rangle,\beta\in\boldsymbol{F}\}$是$F_q$上的一个$l+n$维空间。

记$\boldsymbol{F}^k[\boldsymbol{x}]$为$\boldsymbol{F}$上的相关次数为$k-1$的线性多项式。$f(\boldsymbol{x})\in\boldsymbol{F}^k[\boldsymbol{x}]$为以消息$\boldsymbol{u}$为系数的线性多项式：

$$f(\boldsymbol{x})=\sum_{i=0}^{k-1}\boldsymbol{u}_i\boldsymbol{x}^{[i]} \tag{2}$$

这里，$\boldsymbol{x}^{q^i}$记为$\boldsymbol{x}^{[i]}$，其相关次数为i。假设$\beta_i=f(\alpha_i)$，那么$(\alpha_i,\beta_i),i=1,\cdots,l$可看作$\boldsymbol{W}$上的一组向量。$\{(\alpha_1,\beta_1),\cdots,(\alpha_l,\beta_l)\}$张成$\boldsymbol{W}$上的一个$l$维向量子空间$\boldsymbol{V}$。记由信源消息作为系数的多项式$f(\boldsymbol{x})\in\boldsymbol{F}^k[\boldsymbol{x}]$到线性空间$\boldsymbol{V}\in P(\boldsymbol{W},|\boldsymbol{A}|)$上的映射为$\mathrm{ev}_A$。当$l=|\boldsymbol{A}|\ge k$时，此映射为单射，且此映射下的向量空间$\boldsymbol{C}$满足$D(\boldsymbol{C})\ge 2(l-k+1)$($D$的定义如下)。

传输的向量空间$\boldsymbol{V}$和接收到的向量空间$\boldsymbol{U}$满足：$\boldsymbol{U}=\boldsymbol{V}\oplus\boldsymbol{E}$，这里，$\boldsymbol{E}\in P(\boldsymbol{W})$是任意的错误空间。$\oplus$代表两空间的直接相加，$\boldsymbol{V}\oplus\boldsymbol{E}=\{\boldsymbol{v}+\boldsymbol{e}:\boldsymbol{v}\in\boldsymbol{V},\boldsymbol{e}\in\boldsymbol{E}\}$。

向量空间$\boldsymbol{C}$上的度量定义如下：

$$d(\boldsymbol{A},\boldsymbol{B})\coloneqq\dim(\boldsymbol{A}+\boldsymbol{B})-\dim(\boldsymbol{A}\cap\boldsymbol{B}) \tag{3}$$

以$|\boldsymbol{C}|$表示$\boldsymbol{C}$的大小，$\boldsymbol{C}$上最小距离定义为

$$D(\boldsymbol{C})\coloneqq\min_{\boldsymbol{X},\boldsymbol{Y}\in\boldsymbol{C}:\boldsymbol{X}\ne\boldsymbol{Y}}d(\boldsymbol{X},\boldsymbol{Y}) \tag{4}$$

空间$\boldsymbol{C}$中元素的最大维数记为：

$$l(\boldsymbol{C})\coloneqq\max_{\boldsymbol{X}\in\boldsymbol{C}}\dim(\boldsymbol{X}) \tag{5}$$

2.3 译码算法

设Bob收到的向量空间$\boldsymbol{U}$的维数为$r=l+t$，$\dim(\boldsymbol{U}\cap\boldsymbol{V})=l$，$d(\boldsymbol{U},\boldsymbol{V})=t$，这里$r$是网络的最大流，$t$为错误空间$\boldsymbol{E}$的维数。

记$(\boldsymbol{x}_i,\boldsymbol{y}_i),i=1,\cdots,r$为$\boldsymbol{U}$的一组基，Bob利用这组基构造一个如下形式的双变量多项式$Q(\boldsymbol{x},\boldsymbol{y})$：

$$Q(\boldsymbol{x},\boldsymbol{y})=Q_{\boldsymbol{x}}(\boldsymbol{x})+Q_{\boldsymbol{y}}(\boldsymbol{y}),\ \text{满足}\ Q(\boldsymbol{x}_i,\boldsymbol{y}_i)=0,\ i=1,\ldots,r \tag{6}$$

其中，$Q_{\boldsymbol{x}}(\boldsymbol{x})$为$F_{q^n}$上相关次数为$\tau-1$的线性多项式，$Q_{\boldsymbol{y}}(\boldsymbol{y})$为$F_{q^n}$上相关次数为$\tau-k$的线性多项式。显然$Q(\boldsymbol{x},\boldsymbol{y})$对所有的$(\boldsymbol{x},\boldsymbol{y})\in\boldsymbol{U}$都满足$Q(\boldsymbol{x},\boldsymbol{y})=0$。

当$r=l+t<2\tau-k+1$时上述多项式有非零解。

由于$f(\boldsymbol{x})$也是F_{q^n}上的线性多项式，所以下式$Q(\boldsymbol{x},f(\boldsymbol{x}))$也为线性多项式

$$Q(\boldsymbol{x},f(\boldsymbol{x}))=Q_{\boldsymbol{x}}(\boldsymbol{x})+Q_{\boldsymbol{y}}(f(\boldsymbol{x}))=Q_{\boldsymbol{x}}(\boldsymbol{x})+Q_{\boldsymbol{y}}(\boldsymbol{x})\otimes f(\boldsymbol{x}) \tag{7}$$

由于$f(\boldsymbol{x})$相关次数为$k-1$，所以$Q(\boldsymbol{x},f(\boldsymbol{x}))$的相关次数为$\tau-1$。

现在，假设$\{(\boldsymbol{a}_1,\boldsymbol{b}_1),\cdots,(\boldsymbol{a}_l,\boldsymbol{b}_l)\}$为$\boldsymbol{U}\cap\boldsymbol{V}$的一组基，那么这组基满足$\boldsymbol{b}_i=f(\boldsymbol{a}_i)$，$i=1,\cdots,l$，结合式

(7)有：

$$Q(\boldsymbol{a}_i,\boldsymbol{b}_i)=Q(\boldsymbol{a}_i,f(\boldsymbol{a}_i))=0,\ i=1,\cdots,l \tag{8}$$

因此，$a_1,\cdots,a_l$ 为多项式 $Q(\boldsymbol{x},f(\boldsymbol{x}))$ 的一组线性无关的根。当 $l\geq\tau$ 时，多项式 $Q(\boldsymbol{x},f(\boldsymbol{x}))$ 的线性无关的根的个数大于其次数，当且仅当 $Q(\boldsymbol{x},f(\boldsymbol{x}))\equiv 0$ 才能满足。由于

$$Q(\boldsymbol{x},\boldsymbol{y})=Q_{\boldsymbol{y}}(\boldsymbol{y}-f(\boldsymbol{x}))+Q(\boldsymbol{x},f(\boldsymbol{x})) \tag{9}$$

当 $Q(\boldsymbol{x},f(\boldsymbol{x}))\equiv 0$ 时，$Q(\boldsymbol{x},\boldsymbol{y})=Q_{\boldsymbol{y}}(\boldsymbol{y}-f(\boldsymbol{x}))$。我们便可以从 $Q(\boldsymbol{x},\boldsymbol{y})$ 中解出 $\boldsymbol{y}-f(\boldsymbol{x})$。同时可以用多项式分解的方法从 $Q_{\boldsymbol{y}}(\boldsymbol{x})\otimes f(\boldsymbol{x})+Q_{\boldsymbol{x}}(\boldsymbol{x})\equiv 0$ 中解出 $f(\boldsymbol{x})$。

综上所述，当条件 $r=l+t<2\tau-k+1$ 和 $l\geq\tau$ 同时满足，即：$t<l-k+1$ 时空间 $\boldsymbol{U}$ 是可解得。

3　网络的纠错能力及其安全性

定理1　设 $\boldsymbol{V}\in\boldsymbol{C}$ 为要传输的向量空间。$\boldsymbol{U}=\boldsymbol{V}\oplus\boldsymbol{E}$ 为接收到的向量空间，其中 $\dim(\boldsymbol{E})=t$，如果：

$$2t<D(\boldsymbol{C}) \tag{10}$$

那么可以由接收到的空间 $\boldsymbol{U}$，通过 $\boldsymbol{C}$ 上的最小距离译码得到传输的空间 $\boldsymbol{V}$。

证明　对于空间 $\boldsymbol{V}$，有 $d(\boldsymbol{V},\boldsymbol{U})\leq t$。如果 $\boldsymbol{T}\neq\boldsymbol{V}$ 是 $\boldsymbol{C}$ 上的另一向量空间，那么 $D(\boldsymbol{C})\leq d(\boldsymbol{V},\boldsymbol{T})\leq d(\boldsymbol{V},\boldsymbol{U})+d(\boldsymbol{U},\boldsymbol{T})$，由此可得 $d(\boldsymbol{U},\boldsymbol{T})\geq D(\boldsymbol{C})-d(\boldsymbol{V},\boldsymbol{U})\geq D(\boldsymbol{C})-t$。如果式 (10) $2t<D(\boldsymbol{C})$ 成立，那么 $d(\boldsymbol{U},\boldsymbol{T})>d(\boldsymbol{U},\boldsymbol{V})$，于是最小距离译码得到传输的空间 $\boldsymbol{V}$。

证毕

定理2　当攻击者能窃听到的信道数小于网络的最大流时，他不能得到关于信源的任何信息。

证明　假设攻击者窃听到维数为 $r'<r$ 的空间 $\boldsymbol{U}'$。由于攻击者污染的信道数目不变，我们有 $\boldsymbol{U}'=\widehat{\boldsymbol{V}}\oplus\boldsymbol{E}$，其中 $\dim(\boldsymbol{E})=t$。于是 $d(\boldsymbol{U}'\cap\widehat{\boldsymbol{V}})<l$，显然攻击者由 $\boldsymbol{U}'$ 恢复不出 $\boldsymbol{V}$。

以下证明攻击者不能得到关于信源的任何信息。

用反证法，假设他能由 $\boldsymbol{U}'$ 得到信源消息 $\boldsymbol{u}$ 的部分信息。

译码方法与第 2 节同，他首先找到 $\boldsymbol{U}'$ 的一组基 $(\boldsymbol{x}_i,\boldsymbol{y}_i),i=1,\cdots,r'$ 并构造一个非零双变量多项式 $Q'(\boldsymbol{x},\boldsymbol{y})$ 如下：

$$Q'(\boldsymbol{x},\boldsymbol{y})=Q'_{\boldsymbol{x}}(\boldsymbol{x})+Q'_{\boldsymbol{y}}(\boldsymbol{y}) \tag{11}$$

对所有的 $(\boldsymbol{x},\boldsymbol{y})\in\boldsymbol{U}'$ 有 $Q'(\boldsymbol{x}_i,\boldsymbol{y}_i)=0$。

如果可以找到如下形式的一个非零多项式 $f'(\boldsymbol{x})$：

$$f'(\boldsymbol{x})=\sum_{j=i_1}^{i_k}\boldsymbol{u}_j\boldsymbol{x}^{[j]},i_1,\cdots,i_k\in\{0,\cdots,k-1\},\ \boldsymbol{u}_j\in\boldsymbol{u} \tag{12}$$

那么攻击者便可得到关于 $\boldsymbol{u}$ 的部分信息。

现在假设 $\{(\boldsymbol{a}_1,\boldsymbol{b}_1),\cdots,(\boldsymbol{a}_l,\boldsymbol{b}_l)\}$ 为 $\boldsymbol{V}\cap\boldsymbol{U}'$ 的一组基。显然，$\boldsymbol{V}\cap\boldsymbol{U}'$ 中的向量都不能满足多项式方程 $\boldsymbol{y}=f'(\boldsymbol{x})$，于是攻击者不能从 $Q'(\boldsymbol{x},\boldsymbol{y})$ 解出 $f'(\boldsymbol{x})$，也就不能得到关于信源的任何信息。　　证毕

4　防强窃听者的纠错网络编码

本模型中，假设 Alice 和 Bob 共享一个随机数产生器和一个秘钥 K。

如第2节，设 $\boldsymbol{u}=(\boldsymbol{u}_0,\cdots,\boldsymbol{u}_{k-1})\in\boldsymbol{F}^k$ 为要传输的消息，$f(\boldsymbol{x})=\sum_{i=0}^{k-1}\boldsymbol{u}_i\boldsymbol{x}^{[i]}\in\boldsymbol{F}^k[\boldsymbol{x}]$ 为对应的线性多项式。$\{(\alpha_1,\beta_1),\cdots,(\alpha_l,\beta_l)\}$，其中 $\beta_i=f(\alpha_i)$，张成一个 l 维的空间 $\boldsymbol{V}\in\boldsymbol{W}$。

Alice 的编码算法：Alice 对 $\boldsymbol{V}$ 的基 $\{(\alpha_1,\beta_1),\cdots,(\alpha_l,\beta_l)\}$ 进行如下编码：

(1)在有限域 F_p 随机选取 $r=l+t$ 个随机数 $m_1,\cdots,m_r$，这里$p<<q$。

(2)用AES加密选取的随机数 $m_1,\cdots,m_r$ 并将密文提前传输到信宿。这里用AES加密以保证密文和明文的长度相同。

注意　这里要求 $p<<q$ 并用 AES 加密是为了保证明文密文的长度尽量小。

(3)用随机数 $m_1,\cdots,m_r$ 在随机数产生器中产生 r 个向量 $\boldsymbol{l}_1,\cdots,\boldsymbol{l}_r$，其中每个向量的维数为 r。记 $\boldsymbol{L}=[\boldsymbol{l}_1,\cdots,\boldsymbol{l}_r]^{\mathrm{T}}$。

(4)在 $\boldsymbol{V}$ 中选择t个向量 $\{(\boldsymbol{g}_1,\boldsymbol{h}_1),\cdots,(\boldsymbol{g}_t,\boldsymbol{h}_t)\}$，显然 $\{(\boldsymbol{g}_1,\boldsymbol{h}_1),\cdots,(\boldsymbol{g}_t,\boldsymbol{h}_t)\}$ 是 $\{(\alpha_1,\beta_1),\cdots,(\alpha_l,\beta_l)\}$ 的一些线性组合。

$$\boldsymbol{M}=\begin{pmatrix}\alpha_1,\beta_1\\ \vdots\ \vdots\\ \alpha_l,\beta_l\\ \boldsymbol{g}_1,\boldsymbol{h}_1\\ \vdots\ \vdots\\ \boldsymbol{g}_t,\boldsymbol{h}_t\end{pmatrix}=(\boldsymbol{A},\boldsymbol{B}) \tag{13}$$

这里，$\boldsymbol{A}$ 是 $\boldsymbol{M}$ 的左边的r列，$\boldsymbol{B}$ 是剩余的列。

(5)将 $\boldsymbol{A}$ 右乘矩阵 $\boldsymbol{L}$ 得 $\boldsymbol{M}'$ 如下：

$$\boldsymbol{M}'=(\boldsymbol{AL},\boldsymbol{B}) \tag{14}$$

(6)最后传输的向量空间为 $\boldsymbol{V}'=\langle\boldsymbol{M}'\rangle$。

Bob的译码算法:

(1)由共享的秘钥 K 和接收到的密文解密出随机数 $m_1,\cdots,m_r$，并在随机数产生器中生成向量 $\boldsymbol{l}_1,\cdots,\boldsymbol{l}_r$。

(2)记$(\boldsymbol{x}_i,\boldsymbol{y}_i),i=1,\cdots,r$为 Bob 收到的空间$\boldsymbol{U}''$的一组基。

$$\boldsymbol{M}''=\begin{pmatrix}\boldsymbol{x}_1,\boldsymbol{y}_1\\ \vdots\ \vdots\\ \boldsymbol{x}_r,\boldsymbol{y}_r\end{pmatrix}_{r\times 2m} \tag{15}$$

(3)记$\boldsymbol{M}''=\begin{pmatrix}\boldsymbol{x}_1,\boldsymbol{y}_1\\ \vdots\ \vdots\\ \boldsymbol{x}_r,\boldsymbol{y}_r\end{pmatrix}=(\boldsymbol{F},\boldsymbol{H})$，其中$\boldsymbol{F}$是$\boldsymbol{M}''$的左边$r$列，$\boldsymbol{H}$是剩余的列。

(4)计算：$\widehat{\boldsymbol{M}}=\left(\boldsymbol{F}\boldsymbol{L}^{-1},\boldsymbol{H}\right)$。

(5)以$\widehat{\boldsymbol{M}}$作为线性空间的基，构造双变量多项式$Q(\boldsymbol{x},\boldsymbol{y})$。

(6)用多项式分解法从$Q(\boldsymbol{x},\boldsymbol{y})=Q_y(\boldsymbol{y}-f(\boldsymbol{x}))$中解出$f(\boldsymbol{x})$。

定理 3 假设传输的向量空间为$\boldsymbol{V}'=\left\langle\boldsymbol{M}'\right\rangle\in\boldsymbol{C}$，信宿收到的空间为$\boldsymbol{U}''=<\boldsymbol{M}''>=\boldsymbol{V}'\oplus\boldsymbol{E}$，其中$\dim(\boldsymbol{E})=t$。如果$2t<D(\boldsymbol{C})$，那么$\boldsymbol{C}$上的最小距离译码方法可以从空间$\boldsymbol{U}''$中得到$\boldsymbol{V}$（$\boldsymbol{V}$为原始信源消息$\boldsymbol{u}$生成的要传输的向量空间)。

证明 Alice传输向量空间$\boldsymbol{V}'=\left\langle\boldsymbol{M}'\right\rangle$。设$\boldsymbol{T}$是Alice到Bob之间的线性变换，$\boldsymbol{T}_{Z\to Y}$是从Calvin到Bob之间的变换，我们有：

$$\boldsymbol{M}''=\begin{pmatrix}\boldsymbol{x}_1,\boldsymbol{y}_1\\ \vdots\ \vdots\\ \boldsymbol{x}_r,\boldsymbol{y}_r\end{pmatrix}=\boldsymbol{T}(\boldsymbol{A}\boldsymbol{L},\boldsymbol{B})\oplus\boldsymbol{T}_{Z\to Y}\boldsymbol{E}=\boldsymbol{T}(\boldsymbol{A}\boldsymbol{L},\boldsymbol{B})$$
$$\oplus\boldsymbol{T}'_{Z\to Y}(\boldsymbol{E}')=\widehat{\boldsymbol{T}}(\boldsymbol{A}'\boldsymbol{L},\boldsymbol{B}')=(\boldsymbol{F},\boldsymbol{H}) \tag{16}$$

这里$\boldsymbol{E}'=\begin{pmatrix}\boldsymbol{E}_1\\ \boldsymbol{E}\end{pmatrix}_{r\times 2m}$，其中$\boldsymbol{E}_1$是由$\boldsymbol{E}$上的$l$个向量组成的矩阵。

于是$\widehat{\boldsymbol{M}}=(\boldsymbol{F}\boldsymbol{L}^{-1},\boldsymbol{H})=\widehat{\boldsymbol{T}}(\boldsymbol{A}',\boldsymbol{B}')=\boldsymbol{T}(\boldsymbol{A},\boldsymbol{B})\oplus\boldsymbol{E}''$，其中$\boldsymbol{E}''=\boldsymbol{T}'_{Z\to Y}(\boldsymbol{E}')\boldsymbol{L}^{-1}$是由$\boldsymbol{E}'$变换得到，且$\dim(\boldsymbol{E}'')=t$。

设$\widehat{\boldsymbol{U}}=<\widehat{\boldsymbol{M}}>$，对于向量空间$\boldsymbol{V}$，有$d(\boldsymbol{V},\widehat{\boldsymbol{U}})\le t$且$\widehat{\boldsymbol{U}}=\boldsymbol{V}\oplus\boldsymbol{E}''$。由定理 1 的证明可知，$\boldsymbol{C}$上的最小距离译码方法可以从空间$\boldsymbol{U}''$中得到$\boldsymbol{V}$。

证毕

定理4 如上定义的编码体制可防能窃听网络中所有信道的攻击者的窃听。

证明 当攻击者对窃听到的向量进行译码时，他首先构造一个线性函数$Q(\boldsymbol{x},\boldsymbol{y})$，然后由此解出$f(\boldsymbol{x})$。但由于他窃听到的向量空间并非有原始信源消息$\boldsymbol{u}$直接生成的，而他不知道密钥$K$，因此他无法窃听到任何信源消息。 证毕

5 结束语

针对污染和窃听问题同时存在的网络，本文设计了一种安全的纠错网络编码。首先，本文编码体制可纠正维数低于$\left\lfloor\dfrac{D-1}{2}\right\rfloor$的错误。其次，当攻击者能窃听到的信道数目小于网络的最大流时，他得不到关于信源的任何信息，这里D为消息空间上度量的最小距离。最后，对能窃听网络中所有信道的强攻击者，同样给出了安全的纠错网络编码体制。

参 考 文 献

[1] Ahlswede R, Cai N, and Li S Y, *et al*.. Network information flow [J]. *IEEE Transactions on Information Theory*, 2000, 46(4): 1204–1216.

[2] Li S Y, Yeung R W, and Cai N. Linear network coding [J]. *IEEE Transactions on Information Theory*, 2003, 49(2): 371–381.

[3] Ho T, Koetter R, and Medard M, *et al*.. The benefits of coding over routing in a randomized setting [C]. IEEE International Symposium on Information Theory, Yokohama Japan, 2003: 442.

[4] Geil1 O, Matsumoto R, and Thomsen1 C. On field size and success probability in network coding [C]. Lecture Notes in Computer Science, 2008, 5130: 157–173.

[5] 武广柱, 王劲林, 齐卫宁. ARLNC Stream: 自适应随机网络编码流媒体系统[J]. 电子与信息学报, 2008, 30(1): 25–28.
Wu Guang-zhu, Wang Jin-lin, and Qi Wei-ning. ARLNC stream: Adaptive random linear network coding for media streaming system [J]. *Journal of Electronics & Information Technology*, 2008, 30(1): 25–28.

[6] Cai N and Yeung R W. Secure network coding [C]. IEEE International Symposium on Information Theory, Lausanne, Switzerland, 2002：323.

[7] Feldman J, Malkin T, and Stein C, *et al*.. On the capacity of secure network coding [C]. In Proc. 42nd Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, Sep. 2004.

[8] Chanl T and Grant A. Capacity bounds for secure network coding [C]. Communication theory workshop, Australian, 2008: 95–100.

[9] Bhattad K and Narayanan K R. Weakly secure network coding [C]. In Proc. of the First Workshop on Network Coding, Theory, and Applications (NetCod), Riva del, Garda, Italy, 2005.

[10] Jain K. Security based on network topology against the wiretapping attack [J]. *IEEE Wireless Communications*, 2004, 11(1): 68–71.

[11] Lima L, Medard M, and Barros J. Random linear network

coding: A free cipher? [C]. IEEE International Symposium on Information Theory, Nice, France, 2007: 546–550.

[12] Ho T, Leong B, and Koetter R, *et al*.. Byzantine modification detection in multicast networks using randomized network coding [C]. IEEE International Symposium on Information Theory, Chicago, USA, 2004: 144.

[13] Jaggi S, Langberg M, and Katti S, *et al*.. Resilient network coding in the presence of Byzantine adversaries [C]. 26th IEEE International Conference on Computer Communications, Anchorage, Alaska, 2007: 616–624.

[14] Nutman L and Langberg M. Adversarial models and resilient schemes for network coding [C]. IEEE International Symposium on Information Theory, Toronto, Ontario, Canada, 2008: 171–175.

[15] Yu Zhen, Wei Ya-wen, Ramkumar B, and Guan Yong. An efficient signature-based scheme for securing network coding against pollution attacks [C]. Proc 27th Annual IEEE Conference on Computer Communication, INFOCOM, (Anchorage, AK), 2008: 1409–1417.

[16] Cai N and Yeung R W. Network coding and error correction [C]. IEEE Information Theory Workshop, Bangalore, India, 2002: 119–122.

[17] Yeung R W and Cai N. Network error correction, part I: basic concepts and upper bounds [J]. *Communications in Information and Systems*, 2006, 6(1): 19–36.

[18] Cai N and Yeung R W. Network error correction, part II: lower bounds [J]. *Communications in Information and Systems*, 2006, 6(1): 37–54.

[19] Yang Sheng-hao and Yeung R W. Refined coding bounds for network error correction [C]. IEEE Information Theory Workshop, Bergen, Norway, 2007: 1–5.

[20] Yang Sheng-hao, Ngai C K, and Yeung R W. Construction of linear network codes that achieve a refined singleton bound [C]. IEEE International Symposium on Information Theory, Nice, France 2007: 1576–1580.

[21] Zhang Z. Network error correction coding in packetized networks [C]. IEEE Information Theory Workshop, Chengdu China, 2006: 433–437.

[22] Zhang Z. Linear network error correction codes in packet networks [J]. *IEEE Transactions on Information Theory*, 2008, 54(1): 209–218.

[23] Yang Sheng-hao and Yeung R W. Characterizations of network error correction/ detection and erasure correction [C]. In Proc. of the Third Workshop on Network Coding, Theory, and Applications, San Diego, California, 2007.

[24] Koetter R and Kschischang F R. Coding for errors and erasures in random network coding [J]. *IEEE Transactions on Information Theory*, 2008. 2008, 54(8): 3579–3591.

[25] Ngai C K and Yang Sheng-hao. Deterministic secure error-correcting (SEC) network codes [C]. IEEE Information Theory Workshop, Bergen, Norway, 2007: 96–101.

周业军： 男，1983 年生，博士生，研究方向为网络编码、网络安全.

李 晖： 男，1968 年生，教授，博士生导师，研究方向为信息与网络安全、网络编码.

马建峰： 男，1963 年生，教授，博士生导师，研究方向为信道编码、信息与网络安全.