网络编码在窃听网络中的应用

曹张华 吉晓东 刘 敏
(南通大学电子信息学院 南通 226019)

摘 要 在窃听者窃听能力受限的网络中使用网络编码传输数据时,将网络编码允许中间节点混合收到的数据组这一特点与传统密码学中一次一密的思想相结合,提出了一个基于线性网络编码的有效对抗窃听攻击的安全通信方案。该方案无需秘密信道传输密钥,同时网络容量的使用率达到$\frac{n-1}{n}$。而且,当网络编码的系数域足够大时,该保密通信方案使用随机网络编码实现安全通信的概率趋于1。

关键词 窃听者,网络编码,组播,网络安全,随机网络编码
中图法分类号 TP309 **文献标识码** A

Application of Network Coding in Wiretap Network

CAO Zhang-hua JI Xiao-dong LIU Min
(School of Electronic and Information, Nantong University, Nantong 226019, China)

Abstract Focusing on the issue of secure communication on a wiretap network where a wiretapper can eavesdrop a limited number of links, we proposed a secure communication scheme based on linear network coding. The key idea of our scheme is to combine the ability of network coding that allows intermediate nodes to mix information from different data flows with one time pad. Further, the presented scheme achieves secure communication without employing a secrecy channel and the utilization of network capacity is up to $\frac{n-1}{n}$. Moreover, we showed that if the efficient domain is large enough, the probability of achieving secure communication with random linear network coding tends to 1 in our scheme.

Keywords Wiretapper, Network coding, Multicast, Network security, Random network coding

1 引言

窃听信道或窃听网络中信息的安全传输是一个经典而又备受关注的问题。在传统的窃听信道模型中,窃听者分为窃听能力受限和窃听能力不受限两类,Ozarow-Wyner等在文献[3]中提出了窃听者窃听能力受限的窃听信道模型,并指出在该信道中,若信源发送一n长的分组,窃听者最多能窃听其中的μ个码元符号,则信源一次最多可以安全地发送$n-\mu$个码元。

网络编码这一数据传输技术出现后,Roneyheb和Cai等各自在文献[4]和文献[5]中将Ozarow-Wyner窃听信道模型网络化。文献[4,5]中考虑的窃听网络是信道容量为单位容量组播$G=(V,E)$,窃听者一次可以窃听数量有限的信道。显然,怎样在窃听网络中构造有效的网络编码来安全而尽可能多地传输信源消息分组是一个重要问题。

Cai和Yeung等在文献[5]中证明了对容量为n的组播网络$G=(V,E)$,当窃听者能窃听μ条信道时,存在合适的网络编码使得信源一次最多可以安全地传输$n-\mu$个消息数据组。但是,随着窃听者窃听能力的增强,该方案能安全传输的数据组急剧减少,当窃听者能窃听$n-1$条信道时,组播网络仅能安全有效地传输一个消息分组。

Roneyheb等在文献[4]中指出,在容量为n的窃听组播网络$G=(V,E)$中,使用(n,k)最大距离可分码传输信源消息时,只要窃听者能窃听到的信道数量μ不大于线性分组码的冗余位($\mu\leqslant n-k$),就可以构造合适的网络编码实现安全通信。Silva等在文献[6]中指出,结合最大秩距码(MRD)和网络编码的自身特征同样可以实现安全通信。文献[4,6]中方案能安全传输的数据组的个数也随着窃听者能力的增强而减少。

Lima等在文献[7]中提出了一种基于系数矩阵的对抗窃听攻击的方法。但是,该方法与传统的密码学方法一样,需要一个秘密信道来传输密钥。而且,当传输的消息较少时,充当明文的系数矩阵数量也较少,但其论文中并未讨论怎样对抗穷搜攻击;当传输的消息较多时,又会产生大量的冗余。

与抗窃听攻击相对应,构造对抗主动攻击的网络编码也受到了研究者的关注。主动攻击者不仅能窃听,而且能篡改

到稿日期:2012-12-05 返修日期:2013-03-25 本文受国家自然科学基金项目(61174065),江苏省高校自然科学研究面上项目(10KJB510020),南通大学项目(03080411)资助。

曹张华(1982-),男,博士,讲师,主要研究方向为网络编码与信息安全,E-mail:cryptocaozhanghua@126.com;吉晓东(1980-),男,博士,讲师,主要研究方向为网络编码、协作通信和认知无线电;刘 敏(1976-),男,博士,讲师,主要研究方向为网络编码、无线资源管理、空时信号处理。

网络中的数据组。Jaggi 和 Ho 等在文献[9,10]中分别构造了对抗主动攻击者的安全网络编码。文献[13]也构造了一种对抗主动攻击的通信方案，但未对安全性进行详细的证明。

受 Cai 和 Rouayheb 的启发，本文将网络编码和一次一密相结合，再利用对称密码算法，构造了一个保密通信方案，并证明了其安全性。而且，文中还证明了利用随机网络编码进行数据传输时，若充当母表的有限域足够大，则实现安全通信的概率趋于 1。

2 概念

2.1 网络模型和网络编码

有向无圈图 $G=(V,E)$ 表示单信源、多信宿组播网络，其中 V 是节点集，E 是信道集，s 为网络的信源，$V_D=\{t_1,\cdots,t_m\}$ 是信宿集。有向边 $e=(u,v)$ 表示从 u 到 v 的信道，其中，u 称为 e 的尾节点，v 称为 e 的头节点，分别记为 $u=T(e)$ 和 $v=H(e)$。组播网络的任一信道无噪无损，且容量均为单位容量。对任意的节点 $v\in V$，称 $\Gamma_I(v)=\{e\in E: H(e)=v\}$ 为节点 v 的入边集，$\Gamma_O(v)=\{e\in E: T(e)=v\}$ 为节点 v 的出边集。记信源 s 和信宿 t_i 之间的最大流为 $maxflow(s,t_i)$，且令 $n=\min\{maxflow(s,t_i): i=1,\cdots,m\}$，此即为网络容量。设字母表为有限域 F_q，信源 s 一次发送的 n 个消息记为 $x_1,\cdots,x_n\in F_{q^r}$。显然，$x_1,\cdots,x_n$ 可视为有限域 F_{q^r} 中的元。

线性网络编码这一数据传输技术允许网络中的节点对收到的数据进行线性组合并转发，具体定义如下，该定义引自文献[2]。

定义 1 有向无圈图 $G=(V,E)$ 表示一通信网络，F_q 为一有限域，G 中一个 n 维 F_q 取值的线性网络编码由 $k_{d,e}\in F_q$ $(H(d)=T(e))$ 和 n 维列向量 $\boldsymbol{f}_e(e\in E)$ 组成，且满足下列条件：

(1) $\boldsymbol{f}_e=\sum_{d\in\Gamma_I(T(e))}k_{d,e}\boldsymbol{f}_d, e\in\Gamma_O(H(d))$；

(2) $\boldsymbol{f}_e, e\in\Gamma_I(s)$ 构成 F_q^n 的一组基，称为虚拟信道的全局网络编码核。

对任意的信道 $e\in E$，向量 $\boldsymbol{f}_e$ 称为 e 的全局网络编码核，而 $k_{d,e}$ 称为局部网络编码核。

由上面的定义，可将信源 s 产生的 n 个消息用 $n\times r$ 的矩阵 $\boldsymbol{x}=(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_n)$ 来表示，具体如下：

$$\boldsymbol{x}^{\mathrm{T}}=\begin{pmatrix}\boldsymbol{x}_1\\ \boldsymbol{x}_2\\ \cdots\\ \boldsymbol{x}_n\end{pmatrix}=\begin{pmatrix}x_{11} & x_{12} & \cdots & x_{1r}\\ x_{21} & x_{22} & \cdots & x_{2r}\\ \cdots & \cdots & \cdots & \cdots\\ x_{n1} & x_{n2} & \cdots & x_{nr}\end{pmatrix} \tag{1}$$

式中，$x_{ij}\in F_q$。对任意的信道 $e\in E$，记 e 上传送的数据组为 $\boldsymbol{Y}(e)=\boldsymbol{x}\boldsymbol{f}_e$；对任意的集合 $B\subseteq E$，记 $\boldsymbol{Y}(B)=(\boldsymbol{Y}(e): e\in B)$，以 B 中的线性全局编码核为列向量构成的矩阵记为 $\boldsymbol{F}(B)=(\boldsymbol{f}_e: e\in B)$。

2.2 敌手模型

在组播网络 $G=(V,E)$ 中，窃听信道集构成的集合记为 $\overline{\boldsymbol{W}}=\{W_1,\cdots,W_{|\overline{W}|}\}$，且 $|W_i|\leqslant n-1$。窃听者一次只能窃听到 $\overline{\boldsymbol{W}}$ 中任一信道集 W_i 中的信道所传输的数据组，但窃听者一次只能选 $\overline{\boldsymbol{W}}$ 中一个信道集进行窃听。

窃听者知道网络中各信道的全局网络编码核，且能根据自己的条件和需求选择 $\overline{\boldsymbol{W}}$ 中的一信道集 W_i 进行窃听。窃听者的计算能力受限，不能解决数学中的困难问题，如大数分解、离散对数问题；也不能攻破当前通用的对称密码体制，如 AES 等。但是，窃听者熟知各种已有的密码体制和本文提出的安全通信方案的加解密方法。

2.3 安全性定义

在窃听组播网络 $G=(V,E)$ 中，可被窃听集为 $\overline{\boldsymbol{W}}=\{W_1,\cdots,W_{|\overline{W}|}\}$，信源发送的消息为 $\boldsymbol{X}_1,\cdots,\boldsymbol{X}_n$，窃听者能窃听的数据为 $\boldsymbol{Y}(W_i)$。若对 $j=1,2,\cdots,m$ 有网络编码使得：

$$H(\boldsymbol{X}_1,\cdots,\boldsymbol{X}_n|\boldsymbol{Y}(\Gamma_I(t_j)))=0 \tag{2}$$

则此网络编码是有效的。若有网络编码使得：

$$H(\boldsymbol{X}_1,\cdots,\boldsymbol{X}_n|\boldsymbol{Y}(W_i))=H(\boldsymbol{X}_1,\cdots,\boldsymbol{X}_n) \tag{3}$$

则称此网络编码是信息论意义上安全的，即是完善保密的。

3 安全网络编码

3.1 网络编码与一次一密

在经典的由密码学方法实现安全通信的方案中，消息发送者 Alice 和消息接收者 Bob 之间先通过秘密信道或公钥基础设施获得对称密码体制的加解密密钥。在这样的保密通信方案中，建立秘密信道或使用公钥基础设施分配密钥都需要付出巨大的代价或占用大量资源。

网络编码的出现为实现安全通信提供了免费资源。网络编码不仅允许网络中的节点存储、转发接收到的消息数据，而且还能对接收到的数据进行编码，例如，用线性网络编码传输数据时，网络中的节点 v 收到消息数据组 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 后，对 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 进行编码。即选取系数 a,b，将编码所得分组 $a\boldsymbol{x}+b\boldsymbol{y}$ 作为一信道的输出数据组。若 a,b 是非零，且 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的选取服从均匀分布，由一次一密可知，窃听者即使获得 $a\boldsymbol{x}+b\boldsymbol{y}$，也无法译出消息 $\boldsymbol{x}$ 或 $\boldsymbol{y}$。

3.2 编码和解码

本文提出的安全通信方案如下。在组播 $G=(V,E)$ 中，由密钥生成器生成一个密钥 $\boldsymbol{k}$，调用 AES 加密数据组 $\boldsymbol{x}_1,\cdots,\boldsymbol{x}_{n-1}$，得密文 $\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1}$。密钥 $\boldsymbol{k}$ 的长度将远小于密文长度，将密钥 $\boldsymbol{k}$ 后面加一个向量 $(1,0,\cdots,0)$，得到一个和密文长度相等的数据组 $\boldsymbol{k}'$。接着信源生成满足一定条件的网络编码，最后将 $\boldsymbol{k}',\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1}$ 作为消息分组传输出去。信宿接收到数据后，由网络编码解出 $\boldsymbol{k}',\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1}$，再由 AES 解密出信源消息 $\boldsymbol{x}_1,\cdots,\boldsymbol{x}_{n-1}$，并销毁密钥 $\boldsymbol{k}$。在此安全通信方案中，网络编码不只是提高网络信息传输率，还保证了密钥不被窃听，从而不必调用秘密信道传输密钥。下面给出具体的编码和解码算法。

信源节点的编码算法：

①由密钥生成器生成一个密钥 $\boldsymbol{k}$；

②调用 AES 算法，对信源消息 $\boldsymbol{x}_1,\cdots,\boldsymbol{x}_{n-1}$ 进行加密，得到密文 $\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1}$；

③在密钥 $\boldsymbol{k}$ 后面加一个适当的向量 $(1,0,\cdots,0)$，得到 $\boldsymbol{k}'$，使得 $\boldsymbol{k}'$ 和密文长度相等。信源要传输的消息数据组如下：

$$\begin{pmatrix} \boldsymbol{k}' \\ \boldsymbol{c}_1 \\ \vdots \\ \boldsymbol{c}_{n-1} \end{pmatrix} = \begin{pmatrix} k_1' & k_2' & \cdots & k_r' \\ c_{11} & c_{12} & \cdots & c_{1r} \\ \cdots & \cdots & \cdots & \cdots \\ c_{n-1,1} & c_{n-1,2} & \cdots & c_{n-1,r} \end{pmatrix} \tag{4}$$

④各信道对应的全局网络编码核是 n 长向量，对任意的 $e_1,\cdots,e_{n-1}\in E$，要求对应的全局网络编码核 $f_{e_1},\cdots,f_{e_{n-1}}$ 和向量 $\varepsilon_1=(1,0,\cdots,0)^{\mathrm{T}}$ 是线性无关的，而且 $\mathrm{rank}\boldsymbol{F}(\Gamma_I(t_j))=n$，然后将局部网络编码核发送到网络中的各节点。

信宿节点 $t_1,\cdots,t_m$ 的解码算法：

①根据接收到的数据组恢复出 $\boldsymbol{k}',\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1}$，并恢复出密钥 $\boldsymbol{k}$；

②调用 AES 算法，用密钥 $\boldsymbol{k}$ 解密 $\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1}$，得到信源消息 $\boldsymbol{x}_1,\cdots,\boldsymbol{x}_{n-1}$，并销毁密钥 $\boldsymbol{k}$。

在上述算法中，中间节点只是按照给定的局部网络编码核对接收到的数据组进行网络编码。

3.3 安全性分析

在组播窃听网络 $G=(V,E)$ 中，对任意的 $W_i\in\overline{W}$，有 $\boldsymbol{Y}(W_i)=(\boldsymbol{k}',\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1})\boldsymbol{F}(W_i)$。窃听者的目标是从窃听到的数据组中获得 $\boldsymbol{x}_1,\cdots,\boldsymbol{x}_{n-1}$ 的全部或若干个。因为窃听者无法破译 AES 算法，所以窃听者想获得的数据只能是密钥 $\boldsymbol{k}$。然而，网络编码允许密文 $\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1}$ 和 $\boldsymbol{k}'$ 混合，这样就掩藏了密钥 $\boldsymbol{k}$。对任意的 $W_i\in\overline{W}$，记 $\boldsymbol{F}(W_i)$ 的第一行为 $\boldsymbol{F}_1(W_i)$，剩余的 $n-1$ 行构成的矩阵为 $\boldsymbol{F}_2(W_i)$，从而有：

$$\boldsymbol{Y}(W_i)=\boldsymbol{k}'\boldsymbol{F}_1(W_i)+(\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1})\boldsymbol{F}_2(W_i) \tag{5}$$

下面首先给出一个引理。

引理 1 在组播通信网络 $G=(V,E)$ 中，可被窃听集为 $\overline{W}=\{W_1,\cdots,W_{|\overline{W}|}\}$，且 $|W_i|\leqslant n-1$。信源发出的消息为 $\boldsymbol{k}'$，$\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1}$。若对任意的 $W_i\in\overline{W}$ 有 $\mathrm{rank}\boldsymbol{F}_2(W_i)=\mathrm{rank}\boldsymbol{F}(W_i)$，且 $\boldsymbol{Y}_2(W_i)$ 服从均匀分布，则窃听者不能获得关于密钥 $\boldsymbol{k}$ 的任何信息。

证明：记 $\mathrm{rank}\boldsymbol{F}_2(W_i)=\mathrm{rank}\boldsymbol{F}(W_i)=\lambda_i$，则矩阵 $\boldsymbol{F}_2(W_i)$ 和 $\boldsymbol{F}(W_i)$ 的行向量空间相同。F_q 是 F_{q^r} 的子域，则 $\boldsymbol{F}_2(W_i)$ 和 $\boldsymbol{F}(W_i)$ 的行向量空间也是 F_{q^r} 上的 λ_i 维向量空间。由 $\boldsymbol{Y}_2(W_i)$ 服从均匀分布可知对任意的 $\boldsymbol{y}_2$ 有：

$$\Pr\{\boldsymbol{Y}_2(W_i)=\boldsymbol{y}_2\}=(q^r)^{-\lambda_i} \tag{6}$$

另一方面有：

$$\Pr\{\boldsymbol{Y}(W_i)=\boldsymbol{y}\mid\boldsymbol{Y}_1(W_i)=\boldsymbol{k}'\}=\Pr\{\boldsymbol{Y}_2(W_i)=\boldsymbol{y}-\boldsymbol{k}'\}=(q^r)^{-\lambda_i} \tag{7}$$

从而有：

$$\begin{aligned}&\Pr\{\boldsymbol{Y}(W_i)=\boldsymbol{y}\}\\&=\sum_{\boldsymbol{k}'}\Pr\{\boldsymbol{Y}(W_i)=\boldsymbol{y}\mid\boldsymbol{Y}_1(W_i)=\boldsymbol{k}'\}\Pr\{\boldsymbol{Y}_1(W_i)=\boldsymbol{k}'\}\\&=(q^r)^{-\lambda_i}\sum_{\boldsymbol{k}'}\Pr\{\boldsymbol{Y}_1(W_i)=\boldsymbol{k}'\}\\&=(q^r)^{-\lambda_i}\end{aligned} \tag{8}$$

下面考虑明文和密钥之间的统计相关性。

$$\begin{aligned}&\Pr\{\boldsymbol{Y}(W_i)=\boldsymbol{y},\boldsymbol{K}'=\boldsymbol{k}'\}\\&=\Pr\{\boldsymbol{Y}_2(W_i)=\boldsymbol{y}-\boldsymbol{k}'\boldsymbol{F}_1(W_i)\}\Pr\{\boldsymbol{K}'=\boldsymbol{k}'\}\\&=(q^r)^{-\lambda_i}\Pr\{\boldsymbol{K}'=\boldsymbol{k}'\}\\&=\Pr\{\boldsymbol{Y}(W_i)=\boldsymbol{y}\}\Pr\{\boldsymbol{K}'=\boldsymbol{k}'\}\end{aligned} \tag{9}$$

所以对任意的 $W_i\in\overline{W}$，有 $\boldsymbol{Y}(W_i)$ 和 $\boldsymbol{k}'$ 相互统计独立，即 $I(\boldsymbol{k}';\boldsymbol{Y}(W_i))=0$，则窃听者从窃听得到的数据 $\boldsymbol{Y}(W_i)$ 中得不到任何关于密钥 $\boldsymbol{k}$ 的信息。

加密后的密文可以看成是随机均匀产生的，因此引理 1 中假设 $\boldsymbol{Y}_2(W_i)$ 服从均匀分布是合理的。

定理 1 在组播通信网络 $G=(V,E)$ 中，对任意的 $W_i\in\overline{W}$，设 $f_1(W_i),\cdots,f_{\lambda_i}(W_i)$ 为 $\{f_e:e\in W_i\}$ 的最大线性无关组。若 $\boldsymbol{\varepsilon},f_1(W_i),\cdots,f_{\lambda_i}(W_i)$ 为线性无关向量组，且 $\boldsymbol{Y}_2(W_i)=(\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1})\boldsymbol{F}_2(W_i)$ 服从均匀分布，则窃听者不能获得关于密钥 $\boldsymbol{k}$ 的任何信息。

为了证明最终的结论，我们还需要下面的引理。

引理 2 在单信源、多信宿的组播网络 $G=(V,E)$ 中，若 $q>|\overline{W}|$，则对任意的 $W_i\in\overline{W}$，存在 n 维向量 $\boldsymbol{\eta}$，使得 $\boldsymbol{\eta},f_1(W_i),\cdots,f_{\lambda_i}(W_i)$ 线性无关。

证明：由于对任意 $W_i\in\overline{W}$，有 $\mathrm{rank}\boldsymbol{F}(W_i)<n$，因此有：

$$\begin{aligned}&|(F_q)^n\setminus\bigcup_{i=1}^{|\overline{W}|}\langle f_1(W_i),\cdots,f_{\lambda_i}(W_i)\rangle|\\&\geqslant q^n-\sum_{i=1}^{|\overline{W}|}|\langle f_1(W_i),\cdots,f_{\lambda_i}(W_i)\rangle|\\&\geqslant q^{n-1}(q-|\overline{W}|)\end{aligned} \tag{10}$$

又因为 $q>|\overline{W}|$，从而对任意的 $W_i\in\overline{W}$，可以找到非零向量 $\boldsymbol{\eta}\in(F_q)^n$，使得 $\boldsymbol{\eta},f_1(W_i),\cdots,f_{\lambda_i}(W_i)$ 线性无关。

文献[11]中证明了存在多项式时间算法找出合适的网络编码实现组播网络的有效通信。这样，我们可以获得如下的结论。

定理 2 在单信源、多信宿组播网络 $G=(V,E)$ 中，$\overline{W}=\{W_1,\cdots,W_{|\overline{W}|}\}$ 为可被窃听信道集构成的集合。分组 $\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1}$ 为消息数据 $\boldsymbol{x}_1,\cdots,\boldsymbol{x}_{n-1}$ 的密文，且服从均匀分布。若 $q>\max\{|V_D|,|\overline{W}|\}$，则 3.2 节中的通信方案是安全有效的。

证明：有效性显然。由引理 2 知，对所有的 $W_i\in\overline{W}$，存在 n 维向量 $\boldsymbol{\eta}$，使得 $\boldsymbol{\eta},f_1(W_i),\cdots,f_{\lambda_i}(W_i)$ 线性无关。将 $\boldsymbol{\eta}$ 扩充为向量空间 $(F_q)^n$ 的一组基向量 $\boldsymbol{\eta},\xi_2,\cdots,\xi_n$，再令 $\boldsymbol{Q}=(\boldsymbol{\eta},\xi_2,\cdots,\xi_n)^{-1}$，对任意的 $e\in E$，记 $f_e'=\boldsymbol{Q}f_e$，则对任意的 $W_i\in\overline{W}$ 有：

$$\boldsymbol{Q}(\boldsymbol{\eta},f_1(W_i),\cdots,f_{\lambda_i}(W_i))=(\boldsymbol{\varepsilon}_1,f_1'(W_i),\cdots,f_{\lambda_i}'(W_i)) \tag{11}$$

因为 $\boldsymbol{Q}$ 可逆，则 $\boldsymbol{\varepsilon}_1,f_1'(W_i),\cdots,f_{\lambda_i}'(W_i)$ 线性无关。而 $(\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1})$ 服从均匀分布，则 $(\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1})\boldsymbol{Q}\boldsymbol{F}_2(W_i)$ 也服从均匀分布。由定理 1 可知，网络编码 $\{f_e':e\in E\}$ 可使得窃听者不能获得关于密钥 $\boldsymbol{k}$ 的任何信息。又因为所用的密码算法 AES 是安全的，所以窃听者不能从密文 $\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{n-1}$ 中破译出被加密的信源消息 $\boldsymbol{x}_1,\cdots,\boldsymbol{x}_{n-1}$。因此，3.2 节中的通信方案能在组播网络中实现安全通信。

4 安全随机网络编码

使用随机线性网络编码传输数据组时，局部网络编码核在有限域 F_q 中随机选取。下面将证明，用随机线性网络编码进行通信，当有限域 F_q 足够大时，本文给出的方案实现安全通信的概率趋于 1。

首先给出 Schwartz-Zippel 引理。

引理 3 设 $Q(x_1,\cdots,x_N)\in F[x_1,\cdots,x_N]$ 是一个总次数为 δ 的多变量多项式。固定有限集合 $R\subseteq F$，设 $r_1,\cdots,r_N$ 独立、均匀地从集合 R 中选取。则有：

$$\Pr\{Q(r_1,\cdots,r_N)=0 \mid Q(x_1,\cdots,x_N)\neq 0\}\leqslant\frac{\delta}{|R|} \tag{12}$$

由引理 1 可知，对于单信源、多信宿的组播窃听网络 $G=(V,E)$，对任意的 $W_i\in\overline{W}$，只需 $\boldsymbol{F}_2(W_i)$ 中有 $\mathrm{rank}\boldsymbol{F}(W_i)$ 阶子式就能实现保密通信。

定理 3 在单信源、多信宿的组播网络 $G=(V,E)$ 中，可被窃听信道集构成的集合为 $\overline{W}=\{W_1,\cdots,W_{|\overline{W}|}\}$，且 $|W_i|\leqslant n-1$。在组播中进行随机网络编码，则对任意的 W_i，有 $\Pr\{\mathrm{rank}\boldsymbol{F}(W_i)=\mathrm{rank}\boldsymbol{F}_2(W_i)\}\geqslant 1-\frac{\omega(n-1)}{q}$。其中，$\omega$ 表示从信源到信宿的所有路长的最大值，且有限域 F_q 的基数 $q>\omega(n-1)$。

证明：用随机网络编码进行数据传输时，局部网络编码核随机地选自 F_q。因为对任意 $W_i\in\overline{W}$，有 $\mathrm{rank}\boldsymbol{F}(W_i)\leqslant n-1$，则由引理 3 可知矩阵 $\boldsymbol{F}_2(W_i)$ 中存在 $\mathrm{rank}\boldsymbol{F}(W_i)$ 阶非零行列式的概率为：

$$\Pr\{\mathrm{rank}\boldsymbol{F}(W_i)=\mathrm{rank}\boldsymbol{F}_2(W_i)\}\geqslant 1-\left(\frac{\mathrm{rank}\boldsymbol{F}(W_i)\cdot\omega}{q}\right)^{C_{n-1}^{\mathrm{rank}\boldsymbol{F}(W_i)}} \tag{13}$$

因为 $\mathrm{rank}\boldsymbol{F}(W_i)\leqslant n-1$，从而有：

$$\Pr\{\mathrm{rank}\boldsymbol{F}(W_i)=\mathrm{rank}\boldsymbol{F}_2(W_i)\}\geqslant 1-\frac{\omega(n-1)}{q} \tag{14}$$

由定理 2，在单信源、多信宿组播网络 $G=(V,E)$ 中使用随机线性网络编码传输数据时，窃听者无法获得任何密钥信息的概率不小于 $\left(1-\frac{\omega(n-1)}{q}\right)^{C_{|E|}^{n-1}}$。显然，当 q 趋于无穷大时，实现安全通信的概率趋于 1。

5 性能分析与比较

在窃听者窃听能力受限的网络中，现有安全通信方案主要有基于网络编码这一免费资源和信道编码技术这两大类。在这两类方案中，窃听者的窃听能力和网络容量的利用率是一个矛盾。文献[4-6]中的窃听者能窃听到 $n-1$ 条信道时，网络容量的利用率为 $\frac{1}{n}$。同样条件下，本文提出的安全通信方案对网络容量的利用率为 $\frac{n-1}{n}$。

文献[7]改进传统的密码学方法，减小了加密数据量，但是他们的方案需要使用秘密信道传送密钥，没有脱离传统密码学方法的窠臼。而且该方法中引入的加密系数产生了额外的冗余，同时论文中也没有讨论在减少加密数据量时怎样对抗穷搜攻击。若通过增大系数域来增大明文空间，这既会增大构建网络编码的复杂度，又会降低网络容量的利用率。本文提出的保密通信方案没有使用秘密信道，节省了网络资源。文献[8]中的网络容量利用率最多只有 $\frac{1}{2}$，这对于网络容量是一个巨大的浪费。

文献[13]中要求编码系数域 F_q 中的 q 是一个大素数，这既增加了网络编码的复杂度，又产生大量的冗余。文献[14]中多了事先探测安全途径这一步骤，每次通信需要检测网络中的链路是否被偷听，然后再设计相应的网络编码，而文中没有说明怎样保证窃听者在探测阶段和数据传输阶段窃听的是同样的信道。文献[13,14]中没有对他们所提出的方案给出详细的证明。

上述文献均没有考虑使用随机网络编码实现安全通信的概率，但本文考虑了这一问题。结论表明充当字母表的有限域足够大时，随机网络编码实现安全通信的概率趋于 1，这也为寻找安全网络编码提供了依据，同时为构造安全网络编码的随机算法奠定了基础。

结束语 构造基于网络编码的抗窃听攻击保密通信方案是当前的一个热点问题。本文给出了一个网络容量利用率高同时又能实现保密通信的方案，并对方案进行了详细分析，论证了该方案的安全性。而且还证明了当系数域足够大时，使用随机网络编码实现安全通信的概率趋于 1。

参 考 文 献

[1] Ahlswede R, Cai N, Li S Y R, et al. Network Information Flow [J]. IEEE Trans. Inf. Theory, 2000, 46(4): 1204-1216

[2] Li S Y R, Cai N. Linear Network Coding[J]. IEEE Trans. Inf. Theory, 2003, 49(2): 371-381

[3] Ozarow L H, Wyner A D. The wire-tap channel II [J]. Bell Syst Tech. J, 1984, 63: 2135-2157

[4] Rouayheb S E, Soljanin E, Sprintson A, et al. Secure Network Coding for Wiretap Networks of Type II [J]. IEEE Trans. Inf. Theory, 2012, 58(3): 1361-1371

[5] Cai N, Yeung R W. Secure network coding on a wiretap network [J]. IEEE Trans. Inf. Theory, 2011, 57(1): 424-435

[6] Silva D, Kschischang F R. Universial Secure Network Coding via Rank-Metric Codes [J]. IEEE Trans. Inf. Theory, 2011, 57(2): 1124-1135

[7] Lima L, Gheorghiu S, Barros J, et al. Secure Network Coding for Multi-Resolution Wireless Video Streaming [J]. IEEE Selected areas in Comm, 2010, 28(3): 377-388

[8] Yan Z, Xu C Q, Wang F. A Novel Scheme for Secure Network Coding Using One-time Pad [C]// Conf on Networks Security, Wireless Comm and Trusted Computing. 2009: 92-98

[9] Jaggi S, Langberg M, Katti S, et al. Resilient Network Coding in the Presence of Byzantine Adversaries [J]. IEEE Trans. Inf. Theory, 2008, 54(6): 2596-2603

[10] Ho T, Leong B, Koetter R, et al. Byzantine Modification Detection in Multicast Networks with Random Network Coding [J]. IEEE Trans. Inf. Theory, 2008, 54(6): 2798-2803

[11] Jaggi S, Sanders P, Chou P A, et al. Polynomial time algorithms for multicast network code construction [J]. IEEE Trans. Inf. Theory, 2005, 51(6): 1973-1982

[12] Cui T, Hot T, Kliewer J. On Secure Network Coding with Nonuniform or Restricted Wiretap Set [J]. IEEE Trans. on Inf. Theory, 2013, 59(1): 166-176

[13] 徐光宪，付晓. 抗万能攻击的安全网络编码[J]. 计算机科学，2012, 39(8): 88-91

[14] 朱联祥，朱艳艳，曹铮. 搭线窃听下网络安全路径及安全网络编码的研究[J]. 重庆邮电大学学报，2012, 24(1): 39-44

[15] 俞立峰，杨琼，于娟. 防窃听攻击的安全网络编码[J]. 计算机应用研究，2012, 29(3): 813-818