Security-An Intrinsic Property of Network Coding

CAO Zhanghua[1], TANG Yuansheng[1]
1. School of Mathematical Science, Yangzhou University, Yangzhou, China 225002
1. Caozhanghua@gamil.com

Abstract: Network coding allows immediate nodes to mix information from different data flows. Building on this observation, two secure communication protocols are proposed for a communication system on wiretap multicast networks. The first approach relies on linear network coding completely and enables the multicast network to have perfect secrecy without keys, which is the essential distinction from cryptographic methods. Another way of achieving security over wiretap multicast network via encrypting part of source messages. Comparing with other approaches, no network capacity is lost by our methods.

Keywords: network coding; information security; multicast; capacity; wiretap networks

安全性－网络编码的一种固有性质

曹张华[1]，唐元生[1]
1. 扬州大学数学科学学院，扬州，中国，225002
1. Caozhanghua@gamil.com

【摘要】注意到应用网络编码进行通信时，网络中的消息数据被混合。通过分析这一事实，对组播窃听通信网络，我们在文中给出了两种基于网络编码的保密通信方案。其中，方案一是完全利用网络编码来实现完善保密通信的，即信源消息数据在传输过程中未使用密钥加密，这是与密码学方法的一个根本区别；方案二是结合网络编码和密码学方法实现保密通信的，其安全性由网络编码和密码学方法共同保证。与已有的方法相比，可以看到，文中的方法在实现保密通信的同时，完全有效的利用了网络容量，这是一个显著优势。

【关键词】网络编码；信息安全；组播；容量；窃听网络

1 引言

网络编码理论是由 R. Ahlswede 等在[1]中首次提出的，其核心思想是允许网络中的中继节点对接收到的消息数据进行编码和解码，他们证明了网络编码可以减小网络的冗余容量，提高信息传输效率。随后的研究表明网络编码和信息安全有着密切的联系。最近两年对网络编码的安全性研究受到越来越多的关注。以往考虑通信安全这一问题时，常用的方法是对信源消息数据进行编码和加密，然后经信道传输给信宿。因此，数据的保密是用密码学的方法在通信协议的更高层实现的。但是，网络编码理论的出现改变了这种现状，因为网络中的节点将不同的数据进行混合，掩盖了原来的真实数据，为通信提供了某种安全保证。基于网络编码的安全通信是本文要考虑的问题。

网络编码理论出现后，N. Cai 和 R. W. Yeung 在[2]中首次考虑了窃听网络的的信息安全这一问题；Rouayheb 和 Soljanin 在[3]中说明了窃听网络的网络编码安全性问题是第二类 Ozarow-Wyner 窃听信道问题的推广，在他们的模型中，是用基于最大距离可分码构造出的陪集码对信源消息进行编码，将码字的所有分量作为信源消息经各信道同时发送，只能用基于特殊的码构造出的码来编码信源消息数据显然限制了他们提出的方法的应用；Silva 和 Kschischang 在[4]中提出的用最大秩距码来实现窃听网络安全通信的方法可以看作是[3]的特例，在他们的方法中，网络编码对安全性无影响。同时他们的方法也存在[3]中方法的同样的弊端。[2][3][4]中方法的共同缺点是以牺牲网络容量，降低信息传输率为代价来实现安全通信的；[7]中通过加密一组虚拟线性全局网络编码核来为安全性提供保证，他们方法的一个缺陷就是字母表必须足够的大；[8][9]讨论了网络在遭遇拜占庭攻击时用网络编码实现安全通信的方法。

文章的思想源于这样的事实，当多个信源消息数据组在网络中传输时，应用网络编码，网络中的节点能对消息数据进行不加冗余的编码，将信源消息数据相互混合，使得通信网络中传输的数据不是原始信源消息数据。以线性网络编码为例，当一个节点 v 接收到消息数据组 x 和 y 后，将其混合为数据组 $x+y$ 再发送。若数据组 x 和 y 是随机，均匀，独立产生的，且 x

资助信息：教育部科学技术研究重点项目(208045)；国家自然科学基金项目(60473018)；江苏省自然科学基金(BK2008208)；

978-1-935068-01-3 © 2009 SciRes.

和 y 所在的空间相同，则窃听者只获得 $x+y$ 是无法破译出 x 和 y 的任何信息的；另一方面，若 y 所在的空间包含 x 所在的空间，这时只需对消息数据 y 进行加密，得到密文 c，这儿所用密码体制的明文空间与密文空间是相同的，密文 c 是随机，均匀产生的，且密文 c 的产生与 x 无关，则窃听者获得数据 $x+c$ 还是不能得到信源消息的任何信息，这样就实现了安全通信。

由上述的分析，我们为有窃听者的组播通信网络提供了两种保密通信方案。与已有的方案相比，我们的方案一个显而易见的优势是完全有效的利用了网络的容量。其中方案一实现保密通信未使用密钥，这是与密码学方法的一个根本区别，省略了对数据加密和解密者两个步骤；方案二是一种次优选择，由上一节的分析可知，结合网络编码，只需对部分信源消息数据进行加密，也可达到安全通信的目的，这也节省了许多资源。

本文余下内容是如下安排的：第二部分给出了一些基本概念，并介绍了 N. Cai 等引入的窃听网络(CSWN)；第三部分提供了两种基于网络编码的保密通信方案；最后一部分对文章作了总结。

2 基本概念

本文中主要考虑组播网络中的安全通信问题。下面首先给出组播通信网络的一些基本概念。

只有一个信源多个信宿，并且所有信宿都能恢复出信源消息的通信网络称为组播通信网络。组播通信网络可用有向无圈多重图 $G=(V,E)$ 来表示，V 是节点集，E 是边（信道）集，s 表示信源，$V_D=\{t_1,\cdots,t_\mu\}$ 表示信宿集。对节点 $u,v\in V$，若存在从 u 到 v 的信道，则用有向边 (u,v) 表示此信道，对 $e=(u,v)\in E$，u 称为 e 的尾节点，v 称为 e 的头节点，分别记为 $u=T(e)$，$v=H(e)$，为了讨论的方便，本文中设各信道的容量为单位容量，且无噪无损。对节点 $v\in V$，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。将信源 s 和信宿 $t_i(i=1,\cdots,\mu)$ 之间的最大流记为 $MF(s,t_i)$，记 $n=\min\{MF(s,t_i):i=1,\cdots,\mu\}$。向量组 $\alpha_1,\cdots,\alpha_k$ 的生成的向量空间记为 $\langle\alpha_1,\cdots,\alpha_k\rangle$。设信源发送的消息为有限域 $F=GF(q)$ 上的 r 维向量，即为 $GF(q^r)$ 中的元，其中 r 为一正整数，q 为某一素数的幂，下面将 $F=GF(q)$ 记为 F_q。信源 s 一次所发送的 n 条消息用随机变量集 $\{X_1,\cdots,X_n\}$ 表示，其中 $X_i(i=1,\cdots,n)$ 独立同分布，且均在 F_{q^r} 上服从均匀分布。

因为下文中只考虑线性网络编码，这里先给出网络编码的一些基本概念。下面关于线性网络编码的一些基本概念引自 R. W. Yeung 。

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，称为虚拟信道编码核。

对任意的信道 $e\in E$, f_e 称为 e 的全局编码核。

由上面的定义，可将信源 s 产生的 n 个消息用 n 维的向量 $\boldsymbol{x}=(x_1,\cdots,x_n)$ 来表示，其中 $\boldsymbol{x}$ 的分量 x_i 为 F_{q^r} 中的元，从而信道 e 上传送的数据包为 $\boldsymbol{x}\boldsymbol{f}_e$，将其记为 $\boldsymbol{Y}(e)$。对集合 $B\subseteq E$，记 $\boldsymbol{Y}(B)=(\boldsymbol{Y}(e):e\in B)$，以 $B\subseteq E$ 中的线性全局编码核为列向量构成的矩阵记为 $\boldsymbol{F}(B)=(\boldsymbol{f}_e:e\in B)$。下文中，对任意的信源消息向量 $\boldsymbol{x}=(x_1,\cdots,x_n)\in(F_{q^r})^n$，设 $\Pr\{\boldsymbol{X}=\boldsymbol{x}\}>0$

N. Cai 和 R. W. Yeung 在[5][6]中将第二类窃听网络推广成了可被窃听的通信网络(CSWN)，一 CSWN 由通信网络和可被窃听集 $\overline{\mathrm{A}}=\{A_1,\cdots,A_W\}$ 构成。窃听者可以窃听到 $\overline{\mathrm{A}}$ 中任一信道集 A_i 中所有信道所传输的消息，但只能任选 $\overline{\mathrm{A}}$ 中一个信道集进行窃听。在 CSWN 中，消息发送者知道 $\overline{\mathrm{A}}$，但不知道窃听者会窃听哪一个信道集中的信道；窃听者知道网络中的网络编码协议，且能根据自己的需求选择 $\overline{\mathrm{A}}$ 中的一信道集 A_i 进行窃听。由信息论的基本结论可知，在组播窃听网络中能实现安全通信当且仅当下列两条件被满足。

$$H(\boldsymbol{X}\mid\boldsymbol{Z}(t_i))=0, i=1,\cdots,\mu \qquad (1)$$

$$H(\boldsymbol{X}\mid\boldsymbol{Y}(A_j))=H(\boldsymbol{X}), j=1,\cdots,W \qquad (2)$$

因为我们要讨论的是组播窃听网络的保密通信问题，所以不妨设条件(1)是自然成立的。

条件(2)可用密码学的术语来进行等价的描述。令 $(\mathrm{M},\mathrm{K},\mathrm{C},\mathrm{e}(\ ),\mathrm{d}(\ ))$ 为一密码体制，其中 M 为明文集，K 是密钥集，C 是密文集，e( ) 和 d( ) 分别为加密和解密函数。任一消息明文 $m\in\mathrm{M}$ 产生的概率为 $p_m>0$，任一密钥 $k\in\mathrm{K}$ 使用的概率为 $q_k>0$，由此可知对任意的密文 $c\in\mathrm{C}$，有 $r_c=\sum_{\mathrm{e}(m,k)=c}p_mq_k>0$。

定义 2: 若对任意的消息明文 $m\in\mathrm{M}$ 有 $p_m=\left(\frac{p_m}{r_c}\right)\sum_{\mathrm{e}(m,k)=c}q_k$，则称密码体制 $(\mathrm{M},\mathrm{K},\mathrm{C},\mathrm{e}(\ ),\mathrm{d}(\ ))$ 是完善保密的。

3 保密通信方案

在组播窃听网络中，对任意的 $A_i \in \overline{\mathrm{A}}, i=1,\cdots,W$，有 $\boldsymbol{Y}(A_i)=\boldsymbol{X}\boldsymbol{F}(A_i)$。窃听者就是想从窃听而得的数据 $\boldsymbol{Y}(A_i)$ 中获得有关信源消息数据 $\boldsymbol{X}$ 的信息。从数学角度来分析，窃听者就是在知道矩阵 $\boldsymbol{F}(A_i)$ 和 $\boldsymbol{Y}(A_i)$ 的条件下，想要确定向量 $\boldsymbol{X}$ 的若干或全部分量值。而为了阻止窃听者获得有用信息，直观上看，首先矩阵 $\boldsymbol{F}(A_i)$ 必须不是满秩矩阵；其次，在用 Gauss 消元法解方程 $\boldsymbol{Y}(A_i)=\boldsymbol{X}\boldsymbol{F}(A_i)$ 过程中，$\boldsymbol{F}(A_i)$ 任意一列均至少有两个非零元。当这两个条件满足时，要确定 $\boldsymbol{X}$ 的任一分量值都是有难度的。下面介绍的保密通信方法就是对这一分析通过不同的方法进行刻画而得到的。首先看方案一。

3.1 基于网络编码的保密通信方案一

受到[5][6]的启发，设 $\{\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\}$ 为 $\{\boldsymbol{f}_e : e\in A_i\}$ 的最大线性独立集，$\boldsymbol{\varepsilon}_i\,(1\le i\le n)$ 是第 i 个分量为1，其余分量均为0的列向量。

对任意的 $i\in\{1,\cdots,W\}$，存在整数 $n_i\,(1\le n_i\le n-1)$，使 $\{\boldsymbol{\varepsilon}_1,\cdots,\boldsymbol{\varepsilon}_{n_i},\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\}$ 和 $\{\boldsymbol{\varepsilon}_{n_i+1},\cdots,\boldsymbol{\varepsilon}_n,\boldsymbol{f}_1(A_i),\ \cdots,\boldsymbol{f}_{\lambda_i}(A_i)\}$ 均为线性独立集。

(3)

则条件(3)是对上文中直观描述的数学化的刻画，显然，条件(3)是符合上文直观描述中的两个条件的。下面将从理论上来证明在一定条件下，条件(3)是实现保密通信的充分条件。

对任一 $i\in\{1,\cdots,W\}$，记 $\boldsymbol{F}(A_i)$ 的前 n_i 行构成的矩阵为 $\boldsymbol{F}_1(A_i)$，而 $\boldsymbol{F}(A_i)$ 剩余的后 $n-n_i$ 行构成的矩阵为 $\boldsymbol{F}_2(A_i)$；$\boldsymbol{Y}(A_i)=\boldsymbol{X}\boldsymbol{F}(A_i)=(X_1,\cdots,X_{n_i},X_{n_i+1},\cdots,X_n)\left(\boldsymbol{F}_1(A_i)^T\ \boldsymbol{F}_2(A_i)^T\right)^T$，记 $\boldsymbol{Y}_1(A_i)=(X_1,\cdots,X_{n_i})\boldsymbol{F}_1(A_i)$，$\boldsymbol{Y}_2(A_i)=(X_{n_i+1},\cdots,X_n)\boldsymbol{F}_2(A_i)$。则 $\boldsymbol{Y}(A_i)=\boldsymbol{Y}_1(A_i)+\boldsymbol{Y}_2(A_i)$，此处视 $\boldsymbol{F}(A_i),\boldsymbol{F}_1(A_i),\boldsymbol{F}_2(A_i)$ 为线性变换，分别将 n 维，n_i 维，$n-n_i$ 维向量映为 $\boldsymbol{Y}(A_i),\boldsymbol{Y}_1(A_i),\boldsymbol{Y}_2(A_i)$，记 $\boldsymbol{F}(A_i),\boldsymbol{F}_1(A_i),\boldsymbol{F}_2(A_i)$ 的象空间分别为 L,L_1,L_2，显然 $L_1\subseteq L,L_2\subseteq L$。下面首先给出一个重要的引理。

引理 1：在组播窃听网络 $G=(V,E)$ 中，$\boldsymbol{X}=(X_1,\cdots,X_n)$ 为信源输出消息数据构成的随机向量，若 $rank\boldsymbol{F}_1(A_i)=rank\boldsymbol{F}_2(A_i)=rank\boldsymbol{F}(A_i),i=1,\cdots,W$，且 $\boldsymbol{Y}(A_i),\boldsymbol{Y}_1(A_i),\boldsymbol{Y}_2(A_i)$ 均服从均匀分布，则能实现完善保密通信。

证明：因为 $rankF_1(A_i)=rankF_2(A_i)=rankF(A_i)=\lambda_i$，则 $\Pr\{Y(A_i)=y\}=\Pr\{Y_1(A_i)=y_1\}=\Pr\{Y_2(A_i)=y_2\}=(q^r)^{-\lambda_i}$。由 $y=y_1+y_2$，将 $y\in L$ 看成是用密钥 y_1 加密明文 y_2 而得的密文，易知 $r_y=\sum_{y_1+y_2=y}p_{y_2}q_{y_1}=(q^r)^{-\lambda_i}$，从而有 $\left(\frac{p_{y_2}}{r_y}\right)\sum_{y_1+y_2=y}q_{y_1}=\left(\frac{p_{y_2}}{(q^r)^{-\lambda_i}}\right)q_{y_1}=p_{y_2}$ 成立，所以 $I(Y_2(A_i);Y(A_i))=0$，同理可知 $I(Y_1(A_i);Y(A_i))=0$。而 $(X_1,\cdots,X_{n_i})\to Y_1(A_i)\to Y(A_i)$ 和 $(X_{n_i+1},\cdots,X_n)\to Y_2(A_i)\to Y(A_i)$ 均为 Markov 链，所以 $I(X_1,\cdots,X_{n_i};Y(A_i))=0$，$I(X_{n_i+1},\cdots,X_n;Y(A_i))=0$，从而有 $I(X;Y(A_i))=I(X_1,\cdots,X_{n_i};Y(A_i))+I(X_{n_i+1},\cdots,X_n;Y(A_i))=0$。则能在组播窃听网络中实现完善保密通信。

由此引理1可得出如下的结论。

定理 1：若条件(3)被满足，且随机变量 $\boldsymbol{Y}(A_i),\boldsymbol{Y}_1(A_i),\boldsymbol{Y}_2(A_i)$ 均服从均匀分布，则能在组播窃听网络中实现完善保密通信。

证明：只需注意到 $rank\boldsymbol{F}_1(A_i)=rank\boldsymbol{F}_2(A_i)=rank\boldsymbol{F}(A_i),i=1,\cdots,W$ 和条件(3)等价。

下面先给出[10]中的一个结论。该结论表明存在多项式时间算法来找出合适的网络编码实现组播网络的通信。

引理 2：在单信源，多信宿的组播网络 $G=(V,E)$ 中，与上文一样记 $\min\{MF(s,t_i):i=1,\cdots,v\}=n$，若 $q>|V_D|$，则存在多项式时间算法找出 F_q 取值的 n 维线性网络编码，使得组播网络中信源和任一信宿之间的信息传输率为 n。

为了证明最终的结论，我们还需要下面的引理。

引理 3：若 $q>|\overline{\mathrm{A}}|+1$，且 $\min\{n_i,n-n_i\}\ge\lambda_i,i=1,\cdots,W$，则存在 n 维线性无关的向量 $\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_n$，使得 $\{\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_{n_i},\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\}$ 和 $\{\boldsymbol{\eta}_{n_i+1},\cdots,\boldsymbol{\eta}_n,\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\},i=1,\cdots,W$ 均为线性独立集。

证明：由题意，对任意 A_i，有 $n_i+\lambda_i\le n$，及 $n-n_i+\lambda_i\le n$。又因为 $q>|\overline{\mathrm{A}}|+1$，则容易取到非零的向量 $\boldsymbol{\eta}_1$，使得 $\{\boldsymbol{\eta}_1,\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\}$ 为线性无关集，其中 $i=1,\cdots,W$。继续下去，当 $1\le j\le n-1$ 时，若 $n_i\le j$，则 $\{\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_{n_i},\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\}$ 是线性无关集。下面只需证明存在 n 维向量 $\boldsymbol{\eta}_{j+1}$ 满足：

978-1-935068-01-3 © 2009 SciRes.

$\{\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_j,\boldsymbol{\eta}_{j+1},\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\},j<n_i$ ，$\{\boldsymbol{\eta}_{n_i+1},\cdots,\boldsymbol{\eta}_j,\boldsymbol{\eta}_{j+1},\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\},j\geq n_i$，和 $\{\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_{j+1}\}$ 是线性无关集。注意到，对 $1\leq j\leq n-1$，由 $n_i+\lambda_i\leq n$ 及 $n-n_i+\lambda_i\leq n$，有：

$$\begin{aligned}&\Big|(F_q)^n\Big/\bigcup_{i=1,j<n_i}^{|\overline{\mathrm{A}}|}\langle\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_j,\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\rangle\\&\bigcup\bigcup_{i=1,j\geq n_i}^{|\overline{\mathrm{A}}|}\langle\boldsymbol{\eta}_{n_i+1},\cdots,\boldsymbol{\eta}_j,\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\rangle\\&\cup\langle\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_j\rangle\Big|\\&\geq q^l-q^{l-1}-\sum_{i=1,j<n_i}^{|\overline{\mathrm{A}}|}q^{j+\lambda_i}-\sum_{i=1,j\geq n_i}^{|\overline{\mathrm{A}}|}q^{j+\lambda_i-n_i}\\&\geq q^{l-1}\left(q-|\overline{\mathrm{A}}|-1\right)\end{aligned}$$

由 $q>|\overline{\mathrm{A}}|+1$ 可知，此引理的结论成立。

定理 2：在单信源多信宿的组播网络 $G=(V,E)$ 中，$\overline{\mathrm{A}}$ 为可被窃听的信道集构成的集合。信源消息向量 $\boldsymbol{X}$ 中的任一分量 X_i 均在 F_{q^r} 上服从均匀分布，则当 $q>\max\{|V_D|,|\overline{\mathrm{A}}|+1\}$，且 $\min\{n_i,n-n_i\}\geq\lambda_i,i=1,\cdots,W$ 时，能实现完善保密通信。

证明：由引理 2，当 $q>|V_D|$ 时，能用线性网络编码实现组播网络通信。由引理 3，存在 n 维线性无关的向量组 $\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_n$，使得 $\{\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_{n_i},\ \boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\}$ 和 $\{\boldsymbol{\eta}_{n_i+1},\cdots,\boldsymbol{\eta}_n,\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\}$ 均为线性独立集对所有 $A_i\in\overline{\mathrm{A}}$ 成立。设 $\boldsymbol{Q}=(\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_n)^{-1}$ 为 $(F_q)^n\to(F_q)^n$ 的某一线性变换所对应的矩阵，对任意的 $e\in E$，记 $\boldsymbol{f}'_e=\boldsymbol{Q}\boldsymbol{f}_e$。则有

$$\begin{aligned}&\boldsymbol{Q}(\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_{n_i},\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i))\\&=(\boldsymbol{\varepsilon}_1,\cdots,\boldsymbol{\varepsilon}_{n_i},\boldsymbol{f}'_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}{}'(A_i)),\\&\boldsymbol{Q}(\boldsymbol{\eta}_{n_i+1},\cdots,\boldsymbol{\eta}_n,\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i))\\&=(\boldsymbol{\varepsilon}_{n_i+1},\cdots,\boldsymbol{\varepsilon}_n,\boldsymbol{f}'_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}{}'(A_i))。\end{aligned}$$

因为 $\boldsymbol{Q}$ 可逆，则 $\{\boldsymbol{\varepsilon}_1,\cdots,\boldsymbol{\varepsilon}_{n_i},\boldsymbol{f}'_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}{}'(A_i)\}$ 和 $\{\boldsymbol{\varepsilon}_{n_i+1},\cdots,\boldsymbol{\varepsilon}_n,\boldsymbol{f}'_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}{}'(A_i)\}$ 是线性独立集。而随机变量 $\boldsymbol{Y}'(A_i)=\boldsymbol{X}\boldsymbol{Q}\boldsymbol{F}(A_i),\boldsymbol{Y}'_1(A_i)=(X_1,\cdots,X_{n_i})\boldsymbol{Q}\boldsymbol{F}_1(A_i)$，和 $\boldsymbol{Y}'_2(A_i)=(X_{n_i+1},\cdots,X_n)\boldsymbol{Q}\boldsymbol{F}_2(A_i)$ 都是服从均匀分布的，由定理 1，结论得证。

由定理 2 的证明可知 $\boldsymbol{X}=(X_1,\cdots,X_n)$ 中的任一分量服从均匀分布不是必须的。实际上只要 $\boldsymbol{Y}'(A_i),\boldsymbol{Y}'_1(A_i)$ 和 $\boldsymbol{Y}'_2(A_i)$ 服从均匀分布即可。

这里给出的组播通信网络中的保密通信方案，显著优点是无需对信源消息数据进行加密就能实现完善保密通信，这是一个让人感到以外的结论。同时我们的方法与[3][4][5]的方法相比，既没有引入随机数据，也没有要求用某种特殊的码对信源消息数据进行编码。这使得我们的方法更具一般性。

3.2 一个例子

这一部分举一个例子来说明上面结论的应用，同时通过对例子的分析引入组播窃听网络的保密通信方案二。

在如图 1 所示的组播窃听网络中，s 为信源，t_1,t_2 为信宿，其余节点是中继节点。窃听者可窃听 $\{(v_1,t_1),(v_2,w_1),(v_3,w_2),(v_4,t_2)\}$ 中的任一信道。设字母表为 $F_5=Z_5$，信源 s 发送的消息数据 x_1,x_2,x_3 是随机均匀独立产生的，且均在 F_{5^r} 上服从均匀分布。对网络进行如下的网络编码：信道 $(s,u_1),(u_1,v_i),i=1,2,3$ 传输的消息数据为 x_1；信道 $(s,u_2),(u_2,v_i),i=1,2,3,4$ 传输的消息数据为 x_2；信道 $(s,u_3),(u_3,v_i),i=2,3,4$ 传输的消息数据为 x_3。记消息向量为 (x_1,x_2,x_3)，信道 (v_1,t_1) 和 (v_4,t_2) 全局编码核分别为 $(1,1,0)^T$ 和 $(0,1,1)^T$；信道 $(v_2,w_1),(w_1,t_1),(w_1,t_2)$ 的全局编码核为 $(1,0,1)^T$；信道 $(v_3,w_2),(w_2,t_1),(w_2,t_2)$ 的全局编码核为 $(1,1,3)^T$。此时，$\Gamma_I(t_1)$ 和 $\Gamma_I(t_2)$ 的全局编码核对应的矩阵分别为：$\boldsymbol{M}_1=\begin{pmatrix}1&0&1\\1&1&3\end{pmatrix}$ 和 $\boldsymbol{M}_2=\begin{pmatrix}0&1&1\\1&1&3\end{pmatrix}$，因为 $\det\boldsymbol{M}_1$ 和 $\det\boldsymbol{M}_2$ 均不为零，所以此处给出的网络编码能实现组播网络的通信。由定理 1 可知窃听者仅能

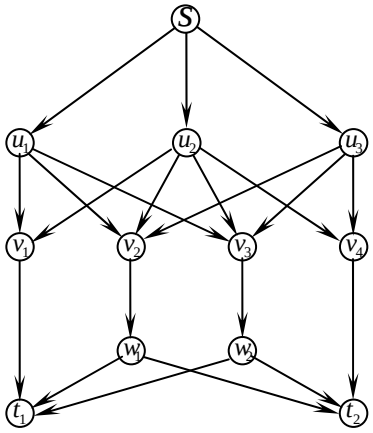

Fig.1 An example of multicast CSWN

图1 组播窃听网络

窃听得 $\{(v_1,t_1),(v_2,w_1),(v_3,w_2),(v_4,t_2)\}$ 中得某一信道是无法得到任何有用的信源信息的，即此时上述网络编码能实现组播网络的完善保密通信。

仍然考虑上述的通信网络，当窃听者可窃听 $\{(v_1,t_1)\ ,(v_2,w_1),(v_3,w_2)(v_4,t_2)\}$ 中任意两信道时，网络显然不是完善保密的。这时只需对信源消息数据 x_1 和 x_2 进行加密，此处要求所用的密码体制的明文空间和密文空间是相同的，对 x_1 和 x_2 进行加密，分别得密文 c_1 和 c_2，密文 c_1 和 c_2 是相互独立，均匀产生的。此时可以证明窃听者无法获得信源消息数据 x_3 的任何信息。而窃听者从可能获得的密文中也无法有效的得到信源消息数据的信息，所以此时可以进行保密通信。下面给出具体的方案。

3.3 基于网络编码的保密通信方案二

对如上定义的组播窃听网络，$\overline{\mathrm{A}}=\{A_1,\cdots,A_W\}$ 为窃听集。当出现 3.2 中的例子中出现的利用网络编码只能保密部分信源消息数据的情况时，可采用密码学的方法对另外的消息数据进行加密，从而达到保密通信的目的。这里需要几个假设，首先所用密码体制明文空间和密文空间相同，其次所使用的密码体制是安全的，第三点是网络编码对密码体制的安全性是没有影响的。

引理 4：对任意的可被窃听集 $A_i\in\overline{\mathrm{A}}$，若存在 σ_i 满足 $\lambda_i\le\sigma_i\le n-1$，其中 $i=1,\cdots,W$，应用密码学方法对 $x_1,\cdots,x_{\sigma_i}$ 进行加密，加密后所得的密文分别为 $c_1,\cdots,c_{\sigma_i}$。对所有的 $A_i\in\overline{\mathrm{A}}$ 有 $\{\varepsilon_{\sigma_i+1},\cdots,\varepsilon_n,\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\}$ 为线性无关集，且 $(c_1,\cdots,c_{\sigma_i})F_1(A_i)$ 服从均匀分布。则窃听者不能获得关于信源消息数据的任何有用信息。

引理 4 的证明与引理 1 的证明相似，也可以看作引理 1 的推论。此结论实际上就是通过用对部分信源消息数据加密而得的密文混合未被加密的明文，达到阻止窃听者获得未被加密的明文的目的。而窃听者是否获得密文是无关紧要的，即使窃听者获得密文，所采用的安全密码体制也能确保窃听者不能获得有用信息。

下面的引理与 N. Cai [5] 中的引理相似。

引理 5：当 $q>\left|\overline{\mathrm{A}}\right|$ 时，对任意的可被窃听集 $A_i\in\overline{\mathrm{A}}$，存在 σ_i 满足 $\lambda_i\le\sigma_i\le n-1$，及 F_q 取值的 n 维向量 $\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_{n-\sigma_i}$ 使得 $\{\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_{n-\sigma_i},\boldsymbol{f}_1(A_i),\cdots,\boldsymbol{f}_{\lambda_i}(A_i)\}$ 为线性无关集。

引理 2 的证明方法与引理 3 的类似。

由上面的两个引理我们给出下面的主要结论。

定理 3：对组播窃听网络，$\overline{\mathrm{A}}=\{A_1,\cdots,A_W\}$ 为窃听集。若对任意的可被窃听集 $A_i\in\overline{\mathrm{A}}$，存在 σ_i 满足 $\lambda_i\le\sigma_i\le n-1(i=1,\cdots,W)$，应用密码学方法对 $x_1,\cdots,x_{\sigma_i}$ 进行加密，加密后所得的密文分别为 $c_1,\cdots,c_{\sigma_i}$，且与 $(c_1,\cdots,c_{\sigma_i})$ 对应的随机向量服从均匀分布。则当 $q>\max\{|V_D|,\left|\overline{\mathrm{A}}\right|\}$ 时，能在网络中实现保密通信。

定理 3 的证明可直接由引理 4，引理 5 得到的。

这一部分简要的给出了组播窃听网络实现保密通信的一种方法。在无法完全用网络编码的方法对抗窃听者，实现保密通信时，结合密码学方法实现保密通信还是能节省大量的计算资源的，而且使得保密通信的方法更加的多元化，选择范围更广。

4 结论

网络编码极大的减小了网络的冗余容量，提高了信息传输率，而网络容量和信息率是信息论中的两个贯穿始终的问题，所以网络编码理论是对现有通信模式有着极大的冲击。文中讨论的基于网络编码的安全通信可以看作是网络编码理论的一个应用。

对可被窃听的组播通信网络的通信安全问题，文中给出了两中解决方案。方案一指出，在一定的条件下，若窃听者可窃听的信道数量受到限制，则可构造适当的网络编码实现完善保密。方案二是结合网络编码和密码学的方法达到安全通信的目的。与[3][4][5]相比，我们的方法极大的提高了网络容量的有效利用。方案一未使用密码学方法对任何数据进行加密，方法二也只需对一部分信源消息数据加密，显然，这两种方法都节约了许多的计算资源。

最近两年，对网络编码的安全性的研究是一个热点问题，有许多的问题待解决。譬如，对于一般的窃听通信网络，能用网络编码实现通信时，能实现基于网络编码的安全通信吗？用随机网络编码的方法实现本文保密通信方案一的概率是多大？对于主动的攻击模式有那些方法可以提高通信效率？

References (参考文献)

[1] R. Ahlswede, N. Cai, S.Y-R. Li, and R. W Yeung. Network information flow [J]. IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204−1216, July 2000.

[2] N. Cai, and R. W Yeung. Secure network coding [C]. in Proc. IEEE Int. Symp. Information Theory, Lausanne, Switzerland, Jun. 30-July. 5, 2002, p. 323.

[3] S. Y. E. Rouayheb and E. Soljanin. On wiretap network II [C]. in Proc. IEEE Int. Symp. Information Theory, Nice, France, Jun. 24-29, 2007, pp 551−555.

[4] D. Silva and F. R. Kschischang. Universal secure network coding via Rank-Metric codes [EB]. pp. 1−22 Available: http://arxiv.org/abs/0809 3546v1 [cs. IT] Sep 2008.

[5] N. Cai, and R. W. Yeung. Secure network coding [OL]. 1−23 Submitted for publication. 2008.

[6] N. Cai, and R. W. Yeung. A security condition for multi-source linear network coding [C]. in Proc. IEEE Int. Symp. Information Theory. pp 561−565, Nice, France, Jun. 24-Jun 29, 2007.

978-1-935068-01-3 © 2009 SciRes.

[7] J. P. Vilela, L. lima and J. Barros. Lightweight security for network coding [C]. IEEE. Inter. Con. on Communications, pp 1750−1754. 2008.

[8] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. R. Karger. Byzantine modification detection in multicast networks with random network coding [J]. IEEE Trans. Inf. Theory, vol. 54, no. 6, pp 2798−2803, Jun 2008.

[9] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Medard, and M. Effros. Resilient network coding in the presence of byzantine adbersaries [J]. IEEE Trans. Inf. Theory, vol 54, no 6, pp 2596−2603, Jun 2008.

[10] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, and L. Tolhuizen, Polynomial time algorithms for multicast network code construction [J]. IEEE Trans. Inf. Theory, vol. 51, no. 6, pp. 1973−1982, Jun. 2005.