doi:10.3969/j.issn.1000-436x.2013.05.021

可伸缩视频流的安全网络编码方案

刘西蒙[1]，刘光军[1]，马建峰[2]，熊金波[2]
(1. 西安电子科技大学 通信工程学院，陕西 西安 710071；2. 西安电子科技大学 计算机学院，陕西 西安 710071)

摘 要：为了使可伸缩视频流在异构网络中达到分层安全等级的目的，运用随机函数来随机化视频流各层中的部分数据流，并结合网络编码来抵御已知的明文攻击。此外，对网络编码器进行了研究，设计有序随机线性网络编码器用于可伸缩视频的传输，可以用很少的随机化操作来达到可扩展的安全等级，并降低通信开销。分析表明，所提方案可有效增加网络的吞吐率。

关键词：安全；网络编码；可伸缩视频编码；随机线性网络编码；散列函数
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2013)05-0184-08

Secure network coding scheme for scalable video streaming

LIU Xi-meng[1], LIU Guang-jun[1], MA Jian-feng[2], XIONG Jin-bo[2]
(1. School of Telecommunication Engineering, Xidian University, Xi'an 710071, China;
2. School of Computer Science and Technology , Xidian University, Xi'an 710071, China)

Abstract: With the purpose to achieve hierarchical security levels for scalable video streaming in heterogeneous networks, random function was used to randomize parts of the video streaming in each layer. Network coding scheme was also used to resist known-plaintext attacks. Moreover, network encoder was studied. Ordered random linear network encoder was designed for scalable video transmission. It could achieve scalability in security levels with few random operations and reduce communication overhead. Analysis shows that the scheme could effectively increase the network throughput.

Key words: security; network coding; scalable video coding; random linear network coding; hash function

1 引言

近年来，可伸缩视频编码是解决视频应用环境中存在的终端用户多样性和网络异构性的有力工具。由于其可以提供不同等级需求的服务并易于实现，可伸缩视频编码被视为在无线网络环境下一种很有前景的方案。但是，在异构网络中，为可伸缩视频编码不同的层提供一种可扩展安全等级的编码仍是巨大的挑战。

尽管安全可扩展的视频流可运用传统密码学的方法在不同的视频层上相互独立地实现。然而，这样的方案是低效的，并且当数据流的数目增加时，扩展性并不是很好。虽然现在有很多关于多媒体应用中可扩展加密方案[1~3]的研究，但是如何在异构网络中保证不同授权的用户有效地获得可变质量的视频仍是一个问题。

由于网络编码可以极大地提升网络吞吐量[4]，并可以提升网络的纠错能力[5]和安全性[6~8]，近年来

收稿日期：2012-07-04；**修回日期**：2012-10-27
基金项目：长江学者和创新团队发展计划基金资助项目(IRT1078)；国家自然科学广东省联合重点基金资助项目(U1135002)；国家科技部重大专项基金资助项目(2011ZX03005-002)；中央高校基本科研业务费基金资助项目(JY10000903001)；国家自然科学基金资助项目(60832001)；陕西省自然科学基础研究计划基金资助项目(2011JQ8042)；福建省自然科学基金资助项目(2011J01339)
Foundation Items: The Program for Changjiang Scholars and Innovative Research Team in University (IRT1078); The Key Program of NSFC-Guangdong Union Foundation (U1135002); The Major National S&T Program (2011ZX03005-002); The Fundamental Research Funds for the Central Universities (JY10000903001); The National Natural Science Foundation of China (60832001); The Natural Science Basic Research Program of Shaanxi Province (2011JQ8042); The Natural Science Foundation of Fujian Province (2011J01339)

受到学术界的广泛关注。随机线性网络编码(RLNC, random linear network coding)将中继节点的输入分组通过随机线性组合结合起来，当接收节点获得足够的线性编码数据分组后，通过运算就可以得到原始的信息分组。这样的特性使得随机线性网络编码非常适用于不稳定的网络[9, 10]。

截至目前，虽然有许多在网络中运用网络编码来解决可伸缩视频的传输方案[11~13]，但是这些方案主要关注于应用网络编码。值得注意的是，Tran 等[14]提出了一些近似的算法可以使优先的高的接收者达到其最大的输出。

在实际的应用中，分层安全对于可伸缩视频编码是非常重要的。特别是在异构网络中，它可以抵御未授权的接入并可以保护视频数据。相比于传统的数据加密，多媒体比特流通常包含较少的冗余。网络编码可以将不同的信息混合，因此，可以运用网络编码所提供的安全来解决可伸缩视频编码的安全性。

现有运用网络编码来提供安全可扩展的视频编码方案十分有限。Lima 等[15]结合传统密码学的方法提出了一种对于多分辨率的安全网络编码方案，这种方案可以抵御已知的明文攻击(KPA, known-plaintext attack)。文献[16]对文献[15]进行扩展，使得文献[16]中方案适合于异构网络中具有不同安全等级的接收者。但文献[16]中的方案会占用大量的带宽并会增加加密开销，这并不适于资源受限的网络。此外，2 种方案都不能抵御层间的 KPA。也就是说，若第 $i+1$ 层的视频信息提交给第 i 层的恶意接收者，这个恶意接收者就可以恢复出第 $i+1$ 层的编码矩阵。并且文献[15,16]中的方案都仅仅提出了一种确定性的层次编码方案，因此不能达到最大的吞吐量。为了解决这些问题，本文提供了相比文献[15,16]中的方案有更低加密开销、低分组丢失率，抵御更强 KPA 的安全可扩展的视频编码方案。

本文的一个首要贡献就是提出了一种有效的安全网络编码方案，在可伸缩视频流中运用分层安全来抵御 KPA。本文提出的方案有如下的特性：1)更强的安全性来抵御 KPA。运用安全散列函数来随机化每一层的前几个数据分组，使得可伸缩视频不仅可以完全地抵御窃听，而且提供更强的 KPA 安全。2)高有效性。本方案的主要开销包括有限域中的加法、乘法和散列函数的计算，这些都可以在现实中有效地进行运算。3)低通信开销。用安全散列函数来生成预编码矩阵，相比文献[15,16]中的方案，明显地降低了通信的开销。

本文的另一个贡献是在随机分组丢失网络中，设计了一种新的网络编码器——有序随机线性网络编码器(ORLNE, ordered random linear network encoder)，用来与源节点匹配并且使每一个接收节点尽可能地解码，可以使优先级高的接收者达到更高的吞吐量。这种网络编码节点更适合于可伸缩视频流且易于实现。

2　基本模型

本文仅考虑单源的无线网络，其中，源节点(也叫做流媒体服务的提供者)提供给异构终端节点可扩展的视频流，接收节点为需求不同服务质量的订阅者。

2.1　系统模型

一个视频数据被分割成图像组(GoP, group of pictures)的 1 个序列，每一个 GoP 编码成 L 层。其中，包括一个基本层和 $L-1$ 个增强层。高层的数据分组依赖于所有低层的数据分组。因此，要解码高层的数据分组必须正确地接收所有低层的数据分组(其中包括基本层的数据分组)。在源节点处，使用安全散列函数来进行安全源编码，以保证不同层的视频流具有不同的安全等级。在传输节点，使用本文所设计的 ORLNE，这样在传输节点可以有效地解决分层随机线性网络编码器(LRLNE, layered random linear network encoder)在接收节点效率低的问题。在接收节点进行可分级译码，只有当用户被授权具有该层以及所有低层的密钥时，才可以恢复源节点所发送的视频流。考虑在实际的网络中，不同用户对图像分辨率有不同的需求。如果一个用户需要更清晰的视频，用户可以向认证中心申请获得更高层级的密钥。当认证中心通过了用户的请求，那么认证中心向用户分发更高层级的密钥，用户就可以获得更加清晰的视频流。例如，在图 1 中，接收终端 1 只被授权获得基本层和 $L-2$ 个加强层的图像，当接收终端 1 向认证中心请求获得更加清晰的视频时，认证中心给用户终端 1 分配 $L-1$ 层的秘密钥。用户终端 1 被授权 $L-1$ 层的秘密钥时候，当收到数据时，就可以用 $L-1$ 层的秘密钥来恢复第 $L-1$ 增强层的信息，从而获得更加清晰的视频数据。

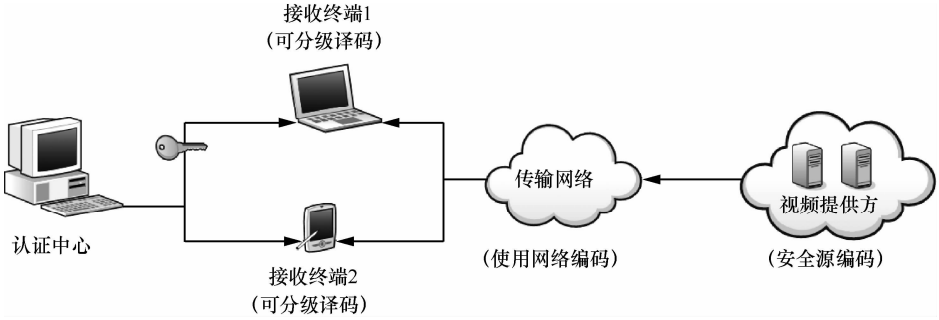


图 1 系统模型

2.2 敌手模型

在开放网络中，为了保证敏感数据的安全性，数据在发布之前应受到保护。网络中总存在被动的窃听者，其目的在于窃听从源节点到接收节点之间的通信，从而获得源节点的有用信息。窃听者尽自己的最大努力，尽可能多地恢复出高质量多播视频流。在这里，仅仅考虑计算能力有界的敌手。敌手有着最大的窃听能力并且知道编码译码的方案(但是不能知道秘密钥)。

2.3 记号

在有限域 $F_q(q=2^k)$ 中，每一层分成 l_i 个向量，每一个向量包含 n 个数据符号。令 $m_j=\sum_{i=1}^{j} l_i$ $(j=1,2,\cdots,L)$。为了简化起见，假定每一个 GoP 单独进行一次网络编码传输，每一层分发唯一的密钥，第 l 层的密钥记作 k_l。如果接收节点具备第 $1,2,\cdots,l$ 层的密钥，那么接收节点就可以获得第 l 层的视频。

在下文中，数据符号记作小写字母，行向量记作 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$，向量或矩阵的转置用上标符号“T”来表示。

3 安全可扩展的网络编码模型

本节主要强调安全可扩展的网络编码方案并阐述其性质。不失一般性，源节点将 GoP 多播给异构的节点，笔者提出的方案必须经历以下 3 个阶段：安全源编码、网络编码(中继节点)和接收节点译码。

3.1 安全源编码

这个阶段包含分组内随机化(IPR)和分层编码(HC)。

1) IPR。分组内随机化指的是在一个数据分组内用一个随机的序列数据符号，假定 IPR 仅仅随机化 $l(l=1,2,\cdots,L)$ 层中前面连续的 t_l 个数据分组。

源节点运用密码学中的安全散列函数 $h:K\times\{0,1\}^*\to F_q\setminus\{0\}$ 来生成随机的符号，其中，用 K 表示秘密钥空间。在这个阶段中，本文使用文献[17,18]中构造的散列函数作为一个伪随机数发生器。

用 id 来表示不同的 GoP，每个 GoP 可以看成 $m=m_l$ 个向量。将向量依据重要程度降序排列。对于第 i 个向量 $\boldsymbol{v}_i=(v_{i,1},v_{i,2},\cdots,v_{i,n})$，源节点运用一次一密的思想，使 h、id 与密钥用如下的方式将 $\boldsymbol{v}_i$ 随机化成。

$$\begin{aligned}&\boldsymbol{w}_i=(w_{i,1},w_{i,2},\cdots,w_{i,n}),\\&i=m_{l-1}+1,m_{l-1}+2,\cdots,m_{l-1}+t_l\end{aligned}$$

$$\begin{cases}w_{i,1}=v_{i,1}+h(\boldsymbol{k}_{l,1},v_{i,2},id)=v_{i,1}+h_{i,1}\\w_{i,2}=v_{i,2}+h(\boldsymbol{k}_{l,2},v_{i,3},id)=v_{i,2}+h_{i,2}\\\quad\vdots\\w_{i,n-1}=v_{i,n-1}+h(\boldsymbol{k}_{l,n-1},v_{i,n},id)=v_{i,n-1}+h_{i,n-1}\\w_{i,n}=v_{i,n}+h(\boldsymbol{k}_{l,n},v_{i,1},v_{i,2},\cdots,v_{i,n-1},id)=v_{i,n}+h_{i,n}\end{cases}\tag{1}$$

在这个过程后，GoP 就用一个 $m\times n$ 的矩阵 $\boldsymbol{G}_1=(\boldsymbol{w}_1^{\mathrm{T}},\boldsymbol{w}_2^{\mathrm{T}},\cdots,\boldsymbol{w}_n^{\mathrm{T}})^{\mathrm{T}}$ 来代替。其中，在 l 层中有 $\boldsymbol{w}_i=\boldsymbol{v}_i(i=m_{l-1}+t_l+1,m_{l-1}+t_l+2,\cdots,m_l)$。

2) 分层编码。分层编码(HC)用三角矩阵随机地组合 $\boldsymbol{G}_1$ 的行。

① 源节点通过 h 与图 2 中层密钥生成 $m\times n$ 的阶梯形矩阵 $\boldsymbol{A}$，另一种方法是通过 $a_{ij}=h(\boldsymbol{k}_{\boldsymbol{l}(i)},i,j)\in F_q(i\geqslant j)$ 来生成矩阵，其中，$\boldsymbol{l}(i)$ 为矩阵 $\boldsymbol{A}$ 的第 i 个行向量。

② 源节点用下面的公式计算载荷矩阵 $\boldsymbol{G}_2$。

$$\boldsymbol{G}_2=\boldsymbol{A}\cdot\boldsymbol{G}_1=(\boldsymbol{c}_1^{\mathrm{T}},\boldsymbol{c}_2^{\mathrm{T}},\cdots,\boldsymbol{c}_n^{\mathrm{T}})^{\mathrm{T}}\tag{2}$$

在完成 HC 后，矩阵将 $\boldsymbol{G}_2$ 的第 i 个向量 $\boldsymbol{c}_i$ 加上数据分组头封装成数据分组，其中，数据分组头中包含有全局编码向量 $\boldsymbol{e}_i$（$\boldsymbol{e}_i$ 代表单位矩阵的第 i 行）。源节点接着将这些编码好的数据分组运用适合于优先编码的 RLNC 方案进行传输。

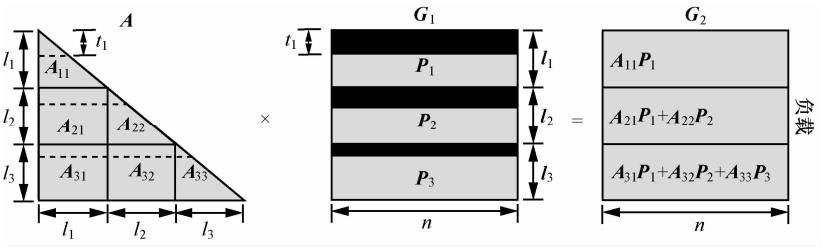


图 2　分层编码

3.2　网络编码(中继节点)

每一个中继节点在网络中担任一个网络编码器的职责。中继节点收到数据分组后，将其放到缓存器中，并辨别出每一个分组的全局编码向量中首个非 0 数据的位置。在文献[16]中，分层的网络中继节点中运用网络编码，当数据分组到达中继节点的时候，第 l 层的所有的数据分组仅仅与较低层的数据分组相互混合(也就是层 $1,2,\cdots,l-1$)。中继节点所做的操作为这些分组的随机线性组合，然后将组合后的数据分组发送给接收节点。

但网络中的数据分组经常会有传播时延与数据分组在缓存队列中随机时延。因此，编码节点与解码数据分组的同步是一个十分重要的问题。同步问题会导致在网络中使用 LRLNE 来接收节点时解码效率十分低。为了解决这个问题，本文设计了一种新的网络(中继)编码器叫做有序随机线性网络编码器，用此解码器来代替文献[16]中所提到的 LRLNE。ORLNE 的设计如下：每一个 ORLNE 节点依据收到的数据分组中全局编码向量的首个非 0 向量的位置，有序地存放在 ORLNE 的缓冲器中。每一个低优先级数据分组并不等待所有相同层的数据分组的到来，而是直接与已接收到的高优先级数据分组相混合，并机会式地向输出链路发送数据分组。这样做的目的是为了使相同层的数据分组相互独立。显然，如果在时刻 t 的中继节点缓存器中，数据分组 $\boldsymbol{x}_{t_1},\boldsymbol{x}_{t_2},\cdots,\boldsymbol{x}_{t_l}$ 以降序排列。那么中继节点将会实施有序的随机线性网络编码(ORLNC)操作，即数据分组 $\boldsymbol{x}_{t_i}$ 与数据分组 $\boldsymbol{x}_{t_1},\boldsymbol{x}_{t_2},\cdots,\boldsymbol{x}_{t_{i-1}}$ $(i=1,2,\cdots,l)$ 混合，产生并机会式地发送 l 个随机线性组合的数据分组。

例如，第 i 层的向量被编码成向量 $\boldsymbol{v}_{i_1},\boldsymbol{v}_{i_2},\cdots,\boldsymbol{v}_{i_{l_i}}$。第 i 层的接收节点已经接收到了第 $1,2,\cdots,i-1$ 层的数据分组，但仅收到了第 i 层的一部分数据 $\boldsymbol{c}_{i_1},\boldsymbol{c}_{i_2},\cdots,\boldsymbol{c}_{i_t}(t<l_i)$，如果使用 LRLNE 时，接收到的 $\boldsymbol{c}_{i_1},\boldsymbol{c}_{i_2},\cdots,\boldsymbol{c}_{i_t}$ 为源节点所有第 i 层数据分组 $\boldsymbol{v}_{i_1}$，$\boldsymbol{v}_{i_2},\cdots,\boldsymbol{v}_{i_{l_i}}$ 的随机线性组合。显然，除非收到 $\boldsymbol{v}_{i_1},\boldsymbol{v}_{i_2},\cdots,\boldsymbol{v}_{i_{l_i}}$ 的所有的线性组合，否则接收节点不能恢复 $\boldsymbol{c}_{i_t}(t=1,2,\cdots,l_t)$。因此，LRLNE 会使收到某一层数据分组要么可以完全恢复出数据，要么完全得不到这一层的数据。如果使用 ORLNE，ORLNE 将收到的前 $i-1$ 层数据与第 i 层的一部分数据 $\boldsymbol{c}_{i_1},\boldsymbol{c}_{i_2},\cdots,\boldsymbol{c}_{i_t}(t<l_i)$ 依据优先级顺序存储在缓存器中，ORLNE 进行 ORLNC 操作后，将产生的数据分组机会式地发送给下一级节点，当接收节点译码后，可以恢复出前 $i-1$ 层与 $\boldsymbol{c}_{i_t}(t=1,2,\cdots,l_t)$。ORLNE 应用在分组丢失较为严重的网络中，可以大大地提升网络的吞吐率。

3.3　在接收节点译码

只要一个中继节点通过 ORLNC 操作来生成 RLNC 数据分组，那么接收节点可以得到一个类似下三角矩阵的全局编码核，在每一个接收节点，那些接收到的全局编码向量可以构成下三角矩阵，使用高斯消去法，接收节点可以尽可能多地恢复数据。

事实上，ORLNE 保证了所有的授权接收者都可以尽可能多地解出更高优先级的数据分组。上述方案所采用的 RLNC 运算，接收到的数据分组仍然记作 $\boldsymbol{c}_{i_1},\boldsymbol{c}_{i_2},\cdots,\boldsymbol{c}_{i_t}$，并且按优先级降序进行排列。由于每一个数据分组 $\boldsymbol{c}_{i_k}(k=1,2,\cdots,t)$ 并没有与 $\boldsymbol{v}_{i_k}(k=t+1,t+2,\cdots,l_i)$ 相混合，源向量 $\boldsymbol{v}_{i_1},\boldsymbol{v}_{i_2},\cdots,\boldsymbol{v}_{i_t}$ 可以在接收节点译码。因此，相比于 LRLNE，运用 ORLNE 可以有效地提高吞吐量，接收节点可以在高延时网络中尽可能地译码。

4　安全性分析

假定源节点的压缩算法是最优的。压缩算法将原视频流中多余的比特流冗余去除。因此，每一个明文符号都可以看作是在 F_q 中均匀随机的。另一方面，笔者用安全散列函数生成不同的随机符号。只要对于

不同的输入，散列碰撞的概率不会超过$\frac{1}{q}$，那么方案的安全性就等同于一次一密的流密码。

假定窃听者的目的是取出编码矩阵的信息和编码数据分组中的原始数据，因此，HC 是对计算能力有界的窃听者是安全的。

定理 1 对于计算能力有界的窃听者，$\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_m$ 与 $\boldsymbol{A}$ 的互信息为 0[16]。

定理 2 对于计算能力有界的窃听者，$\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_m$ 与 $\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_m$ 的互信息为

$$\boldsymbol{I}(\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_m;\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_m)=(n(m-\sigma)-\frac{m(m+1)}{2}+\max\{\frac{m(m+1)}{2}-n(m-\sigma),0\})\log(q-1) \tag{3}$$

其中，$\sigma=\sum_{i=1}^{L}t_i$。

证明 仅需要将文献[16]中定理的 m 替换成 σ。本文提出的方案是层间 KPA 安全的，对于外部窃听者 KPA 安全的讨论是类似的。由于 $\boldsymbol{A}$ 可以在传输过程中重用，如果在一次的传输过程中第 $\theta+1$ 层的某些视频信息无意地传输给了第 θ 层的恶意接收者 R，R 可能会从泄漏的信息中提取出第 $\theta+1$ 层预编码系数的一些或者全部信息。

在这里，笔者考虑最坏的情况，R 获得了 $\theta+1$ 层的所有的视频信息，这个对于设计一个抵抗 KPA 安全方案是充分条件。

定理 3 当 $l_{\theta+1}(m_\theta+m_{\theta+1}+1)>2n(l_{\theta+1}-t_{\theta+1})$ 时，即使第 $\theta+1$ 层的明文已经暴露给计算能力有限的窃听者，窃听者可以恢复第 θ 层编码矩阵 $\boldsymbol{A}$ 的概率为 $\frac{1}{(q-1)^{n(t_{\theta+1}-l_{\theta+1})+\frac{1}{2}l_{\theta+1}(m_\theta+m_{\theta+1}+1)}}$。

证明 令 $\boldsymbol{A}=(\boldsymbol{a}_1^{\mathrm{T}},\boldsymbol{a}_2^{\mathrm{T}},\cdots,\boldsymbol{a}_n^{\mathrm{T}})$。假定信息 $\boldsymbol{v}_{m_\theta}$，$\boldsymbol{v}_{m_\theta+1},\cdots,\boldsymbol{v}_{m_{\theta+1}}$ 在一次传输中暴露给 R，如果 R 有能力解码 $\boldsymbol{c}_{m_\theta},\boldsymbol{c}_{m_\theta+1},\cdots,\boldsymbol{c}_{m_{\theta+1}}$，对于任意的 $k\in\{1,2,\cdots,n\}$，根据式(2)可以得到下面的等式。

当 $m_\theta+1\leqslant j<m_\theta+t_{\theta+1}$ 时，

$$\sum_{i=m_\theta+1}^{j}a_{ji}w_{i,k}+\sum_{i=1}^{m_\theta}a_{ji}w_{i,k}=c_{jk} \tag{4}$$

当 $m_\theta+t_{\theta+1}\leqslant j\leqslant m_{\theta+1}$ 时，

$$\sum_{i=m_\theta+1}^{m_\theta+t_{\theta+1}}a_{ji}w_{i,k}+\sum_{i=m_\theta+t_{\theta+1}+1}^{j}a_{ji}w_{i,k}+\sum_{i=1}^{m_\theta}a_{ji}w_{i,k}=c_{jk} \tag{5}$$

由于 R 可以恢复向量 $\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_{m_\theta}$，并且可以根据式(1)解码 $w_{1,k},w_{2,k},\cdots,w_{m_\theta,k}$ 与 $w_{m_\theta+j,k}=v_{m_\theta+j,k}$，$j=t_{\theta+1}+1,t_{\theta+1}+2,\cdots,l_{\theta+1}$。然后，通过联立式(4)与式(5)的 $nl_{\theta+1}$ 个方程，R 尝试提取出向量 $\boldsymbol{a}_{m_\theta+1},\boldsymbol{a}_{m_\theta+2},\cdots,\boldsymbol{a}_{m_{\theta+1}}$，其中，$\frac{l_{\theta+1}(m_\theta+m_{\theta+1}+1)}{2}$ 为未知量的个数。

然而，在式(1)中，$\Pr(w_{i,j})=\Pr(v_{i,j}+h_{i,j})=\Pr(h_{i,j})=\frac{1}{q}$ $(i=m_\theta+1,m_\theta+2,\cdots,t_{\theta+1};\ j=1,2,\cdots,n)$ 这就说明对于每一个 $h_{i,j}$ 在方程组中是未知的。显然系统中共有 $\frac{l_{\theta+1}(m_\theta+m_{\theta+1}+1)}{2}+nt_{\theta+1}$ 个未知量。由代数的定理可知，当且仅当 $\frac{l_{\theta+1}(m_\theta+m_{\theta+1}+1)}{2}+nt_{\theta+1}>nl_{\theta+1}$，也就是当 $l_{\theta+1}(m_\theta+m_{\theta+1}+1)>2n(l_{\theta+1}-t_{\theta+1})$ 时，R 恢复第 $\theta+1$ 层编码矩阵的概率为 $\frac{1}{(q-1)^{n(t_{\theta+1}-l_{\theta+1})+\frac{1}{2}l_{\theta+1}(m_\theta+m_{\theta+1}+1)}}$。

另一方面，需要注意的是随机数 $h_{i,j}$ 在不同的代之间是相互独立的，这样某一代的随机数并不能提供给其他代任何有用的信息。也就是说，即使在秘密钥升级阶段，窃听者可以恢复出多代的信息，窃听者也不能恢复出 $\boldsymbol{A}$。

事实上，本文提出了这个方案可以认为是对每一层提供不均等的安全保护。只要指定 $t_1,t_2,\cdots,t_L$，三角矩阵就可以提供不同的安全等级，通过保护每一层来抵御 KPA。

5 性能分析

本节主要对本文提出的方案来进行实用方面的考虑。通过分析表明，所提方案在计算开销和通信开销方面优于现有的方案。

5.1 计算开销

本文所提出的计算开销包含 3 个方面。在 F_q 下的加法运算、乘法运算以及散列函数的计算。

在源节点，所需要的计算仅仅为在 F_q 下乘法运算、加法运算与散列函数的计算。相比于乘加运算，散列函数运算要消耗更多的时间。正如第 3 节阐述的，在 F_q 中 IPR 的每一个阶段，在每一个 GoP 中需要进

行 σn 次散列计算，源节点用 h 通过 $\frac{m(m+1)}{2}$ 次散列计算来生成 $\boldsymbol{A}$。式(1)与式(2)在 HC 中需要执行 $\frac{mn(m+1)}{2}$ 次乘法运算与 $\frac{mn(m-1)}{2}$ 次加法运算，因此，HC 的计算复杂性为 $O(m^2n)$。在这里，源节点可以重复利用 $\boldsymbol{A}$，因此对 $\boldsymbol{A}$ 进行预计算可以极大地减小运算的开销。此外，源节点和接收节点都知道散列函数，所以在密钥分配以后就需要很少的加密操作。总之，本文设计方案的全部计算开销是易于实现的。

5.2　通信开销

本文所提出方案的通信开销包括全局编码向量。事实上，通信开销是十分小的。全局编码向量占数据分组的大小为 $\frac{m}{m+n}$。例如：当 $n=1\,024$, $m=30$ 时，通信的开销为 $\frac{30}{1024+30}\approx 2.85\%$，在文献[15,16]方案中的开销为 $\frac{60}{1\,024+60}\approx 5.54\%$。在密钥的分发阶段，$L$ 层的密钥仅仅分发 L 个密钥。每一个密钥在每一代不用升级，都可以重用，这样就进一步减小了通信的开销。

5.3　与其他方案的比较

本节给出了所提方案与已有方案的比较。

在文献[15,16]方案的每一个 GoP 中，源节点需要进行至少 $\frac{m(m+1)}{2}+l_1n$ 次加密操作。由于所提的方案中源节点可以重复利用 $\boldsymbol{A}$，开始通过 $\frac{m(m+1)}{2}$ 次散列计算来生成 $\boldsymbol{A}$，然后多次利用 $\boldsymbol{A}$，这样可以极大地减小开销。而在每一个 GoP 中需要进行 σn 次加密操作。此外，文献[15,16]中方案不能抵御层内的 KPA，相比之下，所提方案运用了散列函数来随机化各层中的首部分数据分组，可以有效地抵御层内 KPA。

用图 3 中的网络来仿真本文中所提出的方案，并且与文献[16]中的方案相比较。在图 3 中，S 为源节点，K_1、K_2、K_3 为中继节点，R_1、R_2、R_3 为 3 个被授予不同权限的接收者。假定视频分成 3 层，其中，第 1 层为基本层，第 2、3 层为增强层。服务节点 S 想要将视频流发送给 R_1、R_2、R_3，3 个接收者，R_1 被授权仅可以接收基层的视频，R_2 可以接收前 2 层的视频，R_3 可以接收前 3 层的视频。其中，网络中的每一条链路的随机分组丢失率为 p。源节点 S 运用本文所提出的安全源编码方案，经过源编码后，S 将编码过的数据分组分别发送给中继节点 K_1、K_2、K_3，中继节点接收到数据分组后，使用 ORLNC。经过中继节点编码后，将数据分组随机地发向接收端，接收端接收到数据后，通过数据分组头中所具有的全局编码向量的信息，先经过高斯消去法恢复源节点编码后的数据分组。不同的接收节点再根据自己被授权的密钥解出不同层的视频信息。需要注意的是，每一个增强层都以下层的数据为基础，如果下层的数据没有被完全恢复，即使解出了更高层的数据分组也不能得到与更高层对应的视频。

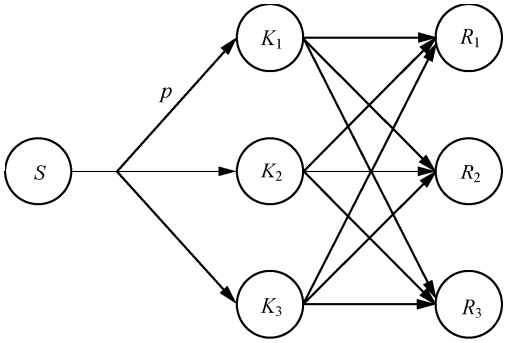
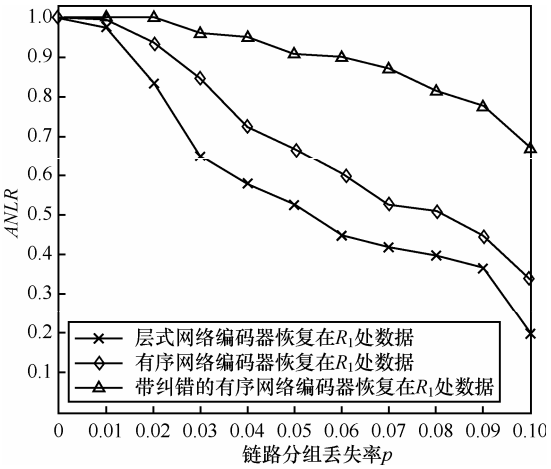


图 3　单源—多接收网络

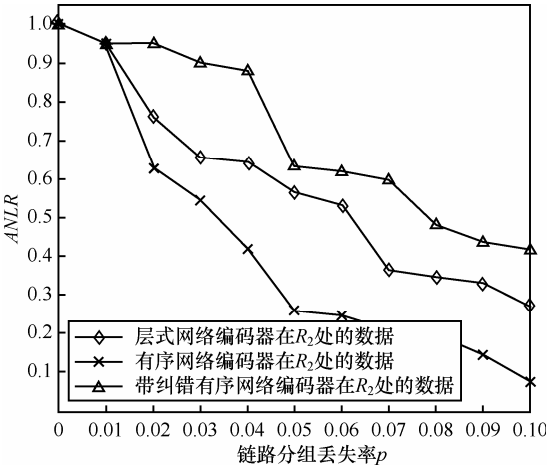
本文方案与文献[16]中方案的性能相比，参数选择 $m=60$，$n=1\,024$，$l_1=l_2=l_3=30$，并且 $q=2^8$。为了更有效地检测分组丢失率，假定 $\max flow\{S,\ R_i\}=20i(i=1,2,3)$。为了验证传输的有效性，本文引入平均层速率(ANLR)来对方案进行比较。ANLR 定义为层中可解码的数据分组的数量与该层总数据分组数目的比值，显然，ANLR 的上界为 1。

相比于文献[16]中的方案，本文在网络中引入了随机分组丢失模型后，分别仿真 ORLNE 与传统的 LRLNE，由于高分组丢失率对网络编码性能的影响十分显著，本文在仿真中模拟了每层中可纠错一个分组丢失的 ORLNE 加以对比，通过图 4 的仿真结果可以看出，ORLNE 相比于 LRLNE 节点，可以有效地增加网络的吞吐率。并且在接收节点 R_1 处，运用 ORLNE 的节点相比于使用 LRLNE 节点的改进明显，在 R_2 处，相比 R_1 改善效果更为明显。而在 R_3 处，使用 ORLNE 的节点改进方案的效果是最为明显的。这是由于使用传统的 RLNC 方案时，只要在网络中引起一个分组丢失，就会导致方程不可解，并且方程的规模越大，分组丢失引起的 ANLR 下降就越明显。当采用 ORLNE 节点

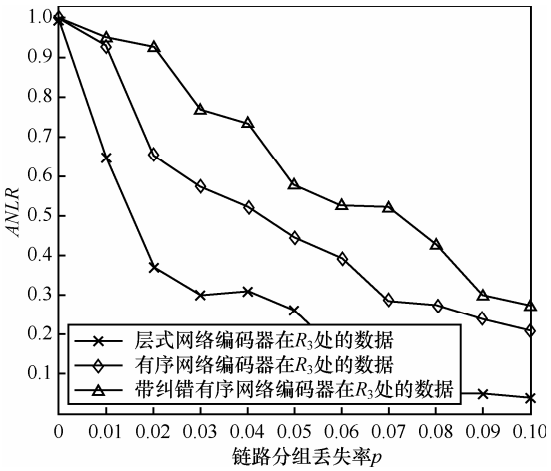
时，可以有效地改善原方案，并且当优先级越高时，效果就越明显。并且在仿真过程中引入纠错分组，在高分组丢失率时引入纠错分组可以显著地改善网络的性能。



(a)接收节点 R_1 处的含仿真结果



(b) 接收节点 R_2 处的含仿真结果



(c) 接收节点 R_3 处的含仿真结果

图 4　仿真结果

6　结束语

可伸缩视频编码是解决网络异构性和终端用户多样性的有力工具，网络编码理论改变了现有信息的传输方式，如何运用网络编码与可伸缩视频编码进行安全传输变成了一个重要的问题。

本文通过运用网络编码来实现安全可伸缩视频编码。基本思想就是在源编码的过程中，利用安全散列函数和随机线性组合的共同作用来实现安全性。通过网络编码技术来增加网络的吞吐量，并运用散列函数来提供更强的安全性来抵御 KPA。此外，设计的 ORLNE 相比于 LRLNE 可以更好地解决网络中链路的随机分组丢失。由于网络编码的使用会增加网络传输的开销，下一步研究工作的重点是设计一种方法在减小网络传输开销的同时保证网络中可伸缩视频流传输的安全性。

参考文献：

[1] LIAN S. Multimedia Content Encryption: Techniques and Applications[M]. Auerbach Publications, 2008.

[2] LIU F, KOENIG H. A survey of video encryption algorithms[J]. Computers & Security, 2010, 29(1):3-15.

[3] KULKARNI N, RAMAN B, GUPTA I. Multimedia encryption: a brief overview[J]. Recent Advances in Multimedia Signal Processing and Communications, 2009.417-449.

[4] LI S Y R, YEUNG R W, CAI N. Linear network coding[J]. IEEE Transactions on Information Theory, 2003, 49(2):371-381.

[5] ZHANG Z. Linear network error correction codes in packet networks[J]. IEEE Transactions on Information Theory, 2008, 54(1):209-218.

[6] CAI N, YEUNG R W. Secure network coding[A]. Proc of International Symposium in Information Theory[C]. Lausanne, Switzerland, 2002.

[7] CAI N, YEUNG R W. Secure network coding on a wiretap network[J]. IEEE Transactions on Information Theory, 2011, 57(1):424-435.

[8] 曹张华,唐元生. 基于网络编码保密通信[J].通信学报, 2010, 31(8): 188-194.
CAO Z H, TANG Y S. Secure communication based on network coding[J]. Journal on Communications, 2010,31(8):188-194.

[9] HO T, MEDARD M, KOETTER R, *et al*. A random linear network coding approach to multicast[J]. Information Theory IEEE Transactions, 2006, 52 (10):4413-4430.

[10] WIDMER J, LE BOUDEC J Y. Network coding for efficient

communication in extreme networks[A]. Proc of the 2005 ACM SIGCOMM Workshop on Delay-tolerant Networking[C]. New York, NY, USA, 2005. 284-291.

[11] WANG H, LIANG J, KUO C C J. Overview of robust video streaming with network coding[J]. Journal of Information Hiding and Multimedia Signal Processing, 2010, 2073:36-50.

[12] MACLAREN WALSH J, WEBER S. A concatenated network coding scheme for multimedia transmission[A]. Fourth Workshop on Network Coding, Theory,and Applications[C]. Hong Kong, China, 2008. 1-6.

[13] NGUYEN K, NGUYEN T, CHEUNG S C. Video streaming with network coding[J]. Journal of Signal Processing Systems, 2010, 59(3):319-333.

[14] TRAN T, NGUYEN T. Prioritized wireless transmissions using random linear codes[A]. IEEE International Symposium on Network Coding[C]. Toronto, 2010. 1-6.

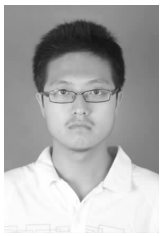
[15] LIMA L, BARROS J, MEDARD M, *et al.* Towards secure multiresolution network coding[A]. Networking and Information Theory[C]. Volos, Greece, 2009. 125-129.

[16] LIMA L, GHEORGHIU S, BARROS J, *et al*. Secure network coding for multi-resolution wireless video streaming[J]. IEEE Journal on Selected Areas in Communications, 2010, 28(3):377-388.

[17] MENEZES A J, VAN OORSCHOT P C, VANSTONE S A. Handbook of Applied Cryptography[M]. CRC Press, 1997.

[18] COPPERSMITH D, KRAWCZYK H, MANSOUR Y. The shrinking generator[A]. Advances in Cryptology- CRYPTO ’93 (LNCS 773)[C]. 1994. 22-39.

作者简介：



刘西蒙（1988-），男，陕西西安人，西安电子科技大学博士生，主要研究方向为公钥密码学与信息安全、安全网络编码及其应用。

刘光军（1980-），男，安徽六安人，西安电子科技大学博士生，主要研究方向为安全网络编码及其应用、密码学与信息安全。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学计算机学院院长、教授、博士生导师，主要研究方向为密码学、计算机网络与信息安全。

熊金波（1981-），男，湖南益阳人，西安电子科技大学博士生，主要研究方向为访问控制技术与结构化文档安全。