基于同步卫星通信网络的弱安全网络编码

刘 琼,潘 进,刘 炯
(西安通信学院,陕西 西安 710106)

摘 要:卫星通信能够克服地面组播通信中用户频繁变动带来的不足,但其使用无线传输媒介传递信息,会导致信息泄露。针对其星间链路上存在被窃听的威胁,构造了一种防窃听的弱安全网络编码方案。该方案中,利用阈值方案达到信源与信宿共享密钥的目的,数据传输过程中,信源首先对数据进行加密,然后再利用网络编码技术对信息进行编码并传输。由于窃听者不知道加密矩阵,因此其无法得到关于信源任何有意义的信息。本方案能够防止窃听者窃听到星间链路上传输的信息,达到了弱安全的要求,同时利用网络编码技术,提高了网络容量的利用率。

关键词:同步卫星;网络编码;门限方案;弱安全
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)07-0143-04

Weakly Secure Network Coding Based on Synchronous Satellite Communication Networks

LIU Qiong, PAN Jin, LIU Jiong
(Xi'an Communications Institute, Xi'an 710106)

Abstract: Satellite communication can overcome the defect that users frequent changing brings about in multicast communication. But using wireless transmission medium to transmit information causes it easy to be wiretapped and lead to information disclosure. For there exist the threat of eavesdropping in the inter-satellite links, it constructed an anti-eavesdropping network coding scheme which can reach weak security. In the scheme, it uses the threshold scheme to achieve a key share between the source and the sinks before transmit the information. When transmitting the information, the source encrypted the data then used network coding techniques to encode and transmit. This program can prevent eavesdroppers listening to the information from the inter-satellite links, reach weak security while improve network capacity utilization by using the network coding technology.

Key words: satellite communication; network coding; threshold scheme; weak security

0 引 言

网络编码的思想是由 R. W. Yeung 和 Z. Zhang 在文献[1]中明确提出的,其改变了传统网络中中间节点单一的存储-转发功能,使之能够对收到的信息进行编码。2000 年,Rudolf Ahlswede、蔡宁、李硕彦和杨伟豪在文献[2]中证明使用网络编码技术能够使网络的传输容量达到网络容量的最大值。Cai 和 Yeung[3] 首先针对能窃听网络中窃听者能力有限,只能窃听到有限条信道,设计了一种基于信息论安全的网络编码方案,并且给出了具体的编码方法。Bhattad 和 Narayanan[4] 首次构造了一种弱安全的网络编码体制,当窃听者窃听到信道的最小割小于网络的最大流时,窃听者无法得到关于信源任何有意义的消息。当窃听者的计算能力有限时,Jain[5] 利用单向函数设计了一种基于弱安全的网络编码体制。Vilela[6] 在密钥共享的基础上,用加密部分编码系数的方法给出了一种弱安全的编码方法。文献[7]基于广义攻击模型和 all-or-nothing 变换,构造了广义组合网络上的安全网络编码,其安全性由网络容量和窃听集的最小割共同决定。文献[8]针对随机网络编码传输文件时的安全问题,给出了一种弱安全的网络编码。文献[9]中通过分析应用网络编码进行通信时,网络中的消息数据被混合这一事实,给出了 2 种基于网络编码的保密通信方案。文献[10]主要研究搭线窃听网络中如何设计线性网络编码使得在有窃听者可以偷听网络中任意的一些边的情况下,网络依然是完善保密的。文献[11]针对无线传感器网络中存在的安全性,利用网络编码技术,基于密码学中的椭圆曲线加密算法,给出了一种改进的方案。文献[12]则针对目前 P2P 流媒体直播系统不能充分利用网络资源的问题,提出了一种基于网络编码的流媒体直播方案。

收稿日期:2011-11-29;**修回日期**:2012-03-02
基金项目:全军军事学研究生课题(2010JY0419-239)
作者简介:刘 琼(1985-),女,硕士研究生,研究方向为网络安全与对抗;潘 进,博士,教授,研究方向为网络安全与对抗。

卫星采用广播的方式，通过无线传输媒介传递信息，会导致卫星网络没有可信域，在星间链路上存在被窃听的威胁，这种威胁虽然不会导致网络系统中的信息被篡改，也不会影响网络正常的运行，但是，可能会造成严重的失泄密。文中针对卫星通信过程中信息易被窃听的特点，基于密码学中的门限方案构造了一种弱安全的网络编码方案。本方案中，利用信源与信宿对数据进行加解密，减少了卫星计算能力有限的不足，而星上采用简单的网络编码，以牺牲少量的计算开销来提高网络的利用率。

1 基本概念及攻击模型

1.1 基本概念

1.1.1 网络模型

通信网络模型用有向无圈图 $G=(V,E)$ 来表示，其中 G 表示所有边均具有单位容量的非循环网络，V 代表节点集，E 代表边集。考虑单源组播情况，用 $s \subset V$ 来表示通信网络中的信源节点，集合 $T=\{t_1,t_2,\cdots,t_\sigma\} \subset V$ 表示信宿节点的集合，边 $e=(v,v')$ 的终点用 $v'=\mathrm{head}(e)$ 表示，其起点用 $v=\mathrm{tail}(e)$ 表示。对于网络中任意节点 v，用 $\Psi_I(v)$ 表示节点 $v \in V$ 的入边集合，其模 $|\Psi_I(v)|$ 表示节点 $v \in V$ 的入度，记为 $\psi_I(v)$；$\Psi_O(v)$ 表示节点 $v \in V$ 的出边集合，其模 $|\Psi_O(v)|$ 表示节点 $v \in V$ 的出度，记为 $\psi_O(v)$。

设网络的组播容量为 n，网络中每条信道的传输容量为一个数据包，信源以单位时间产生消息：

$$\boldsymbol{X}=[\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_n]^{\mathrm{T}}=\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1l} \\ x_{21} & x_{22} & \cdots & x_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nl} \end{pmatrix}$$

称 $\boldsymbol{X}_i, i=1,2,\cdots,n$ 为信息包，其中 $x_{ij} \in F_q$（F_q 为有限域，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 $\boldsymbol{\Gamma}_{e_j}\boldsymbol{X}$，其中 $\boldsymbol{\Gamma}_{e_j}$ 是信道 e_j 对应的全局编码向量。

1.1.2 弱安全

首先做如下说明：

$\boldsymbol{M}$：随机消息的集合；

$\boldsymbol{X}$：信源消息；

$\boldsymbol{U}$：$\boldsymbol{X}$ 的一个子集；

$\boldsymbol{P}$：窃听者不知道的 $m \times m$ 阶矩阵。

如果 $I(\boldsymbol{U};\boldsymbol{M})=0$，则表示从 $\boldsymbol{M}$ 中得不到关于 $\boldsymbol{U}$ 的任何信息；如果 $I(\boldsymbol{X}_i;\boldsymbol{M})=0, \forall \boldsymbol{X}_i \in \boldsymbol{U}$ 表示从 $\boldsymbol{M}$ 中得不到关于 $\boldsymbol{U}$ 的任何有意义的信息。此定义的一种特殊情况，如果 $\boldsymbol{M}$ 表示窃听者窃听到的消息，$\boldsymbol{U}=\boldsymbol{X}$ 表示信源消息，如果 $I(\boldsymbol{X}_i;\boldsymbol{M})=0$ 表示窃听者未得到关于信源的任何信息，如果 $I(\boldsymbol{X}_i;\boldsymbol{M})=0, \forall \boldsymbol{X}_i \in \boldsymbol{X}$ 称窃听者没有得到关于 $\boldsymbol{X}$ 任何有意义的信息，称为“弱安全”。

如果对信源消息 $\boldsymbol{X}$ 进行线性变换为 $\boldsymbol{PX}$，然后再进行传输，那么信道 $e_j \in E$ 传输的消息为 $\boldsymbol{\Gamma}_{e_j}\boldsymbol{PX}$。则即使窃听者能够窃听到所有的信道，他也只能得到 $\boldsymbol{PX}$ 而不是 $\boldsymbol{X}$。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，窃听者不能得到关于信源任何有意义的信息。文中研究的安全就是在窃听者不知道 $\boldsymbol{P}$ 的情况下的弱安全。

1.1.3 门限方案

令 t,w 为正整数且 $t \leqslant w$。(t,w) -门限方案是这样一种方法：在 w 个参与者组成的集体中共享消息 M，这样由任何 t 个参与者组成的子集都能重构消息 M，但是小于 t 个参与者组成的子集将无法重构 M。该方案是更多普遍的共享方案的关键构成模块。本中将用阈值方案来构造。

阈值方案：选定一个素数 p，p 应该较所有可能的消息大并且比参与者的个数 w 大。所有的计算都会执行模 p 的操作。消息 M 用一个模 p 数来表示，想要在 w 个人中进行拆分，按照这种方式要重构消息将需要其中的 t 个人。做的第一件事就是随机地选定 $t-1$ 个模 p 数，称为 $s_1,s_2,\cdots,s_{t-1}$。这样得到多项式：$s(x) \equiv M+s_1x+\cdots+s_{t-1}x^{t-1}(\mathrm{mod}p)$，该多项式满足 $s(0) \equiv M(\mathrm{mod}p)$。现在，对于 w 个参与者，选定不同的整数 $x_1,\cdots,x_w(\mathrm{mod}p)$，并给每名参与者一个数对 (x_i,y_i)，其中 $y_i \equiv s(x_i)(\mathrm{mod}p)$。例如选择 $1,2,\cdots,w$ 为 x 的值，这样就产生数对 $(1,s(1)),\cdots,(w,s(w))$，给每人一个数对。所有的人都知道素数 p 的值，而多项式 $s(x)$ 则是保密的。

现在假设 t 个人聚集并分享各自的数据对，为了简化符号，假设数据对为 $(x_1,y_1),\cdots,(x_t,y_t)$，它们想重构消息 M。

从线性逼近开始。假设有一个 $t-1$ 阶的多项式 $s(x)$，我们想要通过点 $(x_1,y_1),\cdots,(x_t,y_t)$ 重构 M，其中 $y_k=s(x_k)$。这意味着 $y_k \equiv M+s_1x^1+\cdots+s_{t-1}x^{t-1}(\mathrm{mod}p), 1 \leqslant k \leqslant t$，如果指定 $s_0=M$，那么可以重写上式如下：

$$\begin{pmatrix} 1 & x_1 & \cdots & x_1^{t-1} \\ 1 & x_2 & \cdots & x_2^{t-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & x_t & \cdots & x_t^{t-1} \end{pmatrix}\begin{pmatrix} s_0 \\ s_1 \\ \cdots \\ s_t \end{pmatrix} \equiv \begin{pmatrix} y_1 \\ y_2 \\ \cdots \\ y_t \end{pmatrix}(\mathrm{mod}p)$$

这是一个范德蒙（Vandermonde）矩阵，把它记为 $\boldsymbol{V}$。如果这个方案的矩阵 $\boldsymbol{V}$ 是模 P 非零的，则其有惟一的模 P 解。能够证明它的行列式为：

$$\det \boldsymbol{V}=\prod_{1\leqslant j<k\leqslant t}(x_k-x_i)$$

仅当两个 $x_i \bmod p$ 相等时行列式为 $0 \bmod p$（此时需要 p 为一个素数）。因此，只要有不同的 x_i 的值，方案就有惟一解。

1.2 攻击模型

基于 1.1.1 给出的通信网络中，攻击者想通过窃听网络中部分信道来得到关于信源的信息，假设存在窃听集 $\boldsymbol{A}=(\boldsymbol{A}_1,\cdots,\boldsymbol{A}_{|A|}):\boldsymbol{A}_i$ 为边集 E 的子集，$\boldsymbol{A}_i$ 表示窃听子集 $\boldsymbol{A}_i$ 中所有线性无关边的全局编码向量组成的矩阵，那么窃听者窃听到的消息便可表示为 $\boldsymbol{A}_i\boldsymbol{X}$，$a_{ij}$ 表示窃听矩阵 $\boldsymbol{A}_i$ 中第 j 行的元素。用 $k_i=|\boldsymbol{A}_i|$ 表示窃听者能够窃听到子集 $\boldsymbol{A}_i$ 的信道数，并设 $k=\max k_i$。设窃听者每次只能窃听到边集中的一个子集，且不随时间的变化而改变。

2 具体方案

设在通信网络 $G=(V,E)$ 中，构造 $(n,\Psi_O(s))$ - 门限方案，其中 n 为多播容量，$\Psi_O(s)$ 表示信源节点的出度，由最大流定理知，每个信宿节点的最大流 $\text{maxflow}(t_i)\geqslant n$，即从信源到信宿最少有 n 条路径，可以得到信源组播的数据，窃听者窃听到的信道数小于 n，无法得到组播数据。

2.1 信源编码算法

首先，信源在有限域中选定一个素数 p 和一个随机字符 a，然后合理选择 n 个数作为 x 的值，如 1,2,$\cdots$,n，其中素数 p 是公开的，然后通过多项式 $s(x)\equiv a+s_1x+\cdots+s_{n-1}x^{n-1}(\bmod p)$ 得到数对 $(1,s(1)),\cdots,(n,s(n))$ 并多播该组数对。

信源利用随机选择的字符 a 产生范德蒙行列式

$$\boldsymbol{H}=\begin{pmatrix} a & a+1 & \cdots & a+m-1 \\ a^2 & (a+1)^2 & \cdots & (a+m-1)^2 \\ \vdots & \vdots & \ddots & \vdots \\ a^n & (a+1)^n & \cdots & (a+m-1)^n \end{pmatrix}$$

将消息 $\boldsymbol{X}$ 左乘 $\boldsymbol{H}$，得到信道中要传输的消息 $\boldsymbol{X}'=\boldsymbol{H}\boldsymbol{X}$。

2.2 信宿解码算法

每个信宿节点均可得到这 n 个数对，然后计算出信源选取的随机数 a，计算出行列式 $\boldsymbol{H}$，那么经过逆运算便可得到原始的信息。

定理：对于给定的通信网络，如果窃听者窃听到边集的最小割小于网络的最大流，即 $k<n$ 时，其得不到关于信源任何有意义的信息。

证明：本方案实施的前提是，当不考虑网络的安全性时，通信网络利用网络编码可以实现网络的最大流。

首先介绍文献[13]中给出的从向量空间角度实现线性网络编码的多项式时间算法。

对于给定的通信网络，利用最大流最小割算法确定网络的最大流为 n。如果通信网络是可解的，那么对于网络中的每一个接收节点，都有 n 条相互不重合的路径到达，这 n 条路径组成了信宿节点的一个流。因为网络的最大流为 n，那么只要在每个信宿节点的 n 条路径上分别传输一个符号，便可以实现完整的数据通信。

由以上算法知，当信源组播 n 组数对时，信宿便可以得到这 n 组数对，也就可以计算出随机数 a。而由于窃听者窃听到的边集小于网络容量，那么就不可能得到所有的 n 组数对，由阈值方案知，窃听者无法得到随机数 a，也就得不到信源消息的全局编码向量，进而得不到信源任何有意义的消息。

3 网络编码在星上处理同步卫星网络中的应用

假设同步通信卫星覆盖 A、B、C、D 四个区域中的用户，区域 A 要组播数据到区域 B、C、D，其中的用户有固定节点、通信终端等。在地面移动组播中，当移动节点作为组播的源节点时，特别对于有源的组播方式，源节点的改变将会导致整个组播树的重建，这样不仅增加了通信开销，而且在新组播树建立之前，原来的源节点向组播成员发送的数据流将会发生中断，影响数据转发的连通性及网络的稳定性。在同步卫星通信中，信源到信宿只需要卫星转发一次，使组播树的重新建立变得容易，克服了移动终端用户频繁变动导致路由重建而带来的不足，利用卫星通信会导致传输的数据暴露，因此，对数据的安全性要求就更加严格。

3.1 数据传输前的密钥共享

为了在提高网络容量的利用率的前提下实现信息的安全传输，必须对所要传输的信息进行加密处理。根据前面所述的方案，首先利用地面组播方式，组播一组数据，达到密钥共享的目的，如图 1 所示。

3.2 基于编码网络的卫星通信

数据开始传输时，区域 A 中的用户对数据 $\boldsymbol{M}$ 进行加密并进行网络编码，最后传输新的消息为 $\boldsymbol{X}$，同步卫星接收到 $\boldsymbol{X}$，对数据进行随机编码得到新的数据 $\boldsymbol{X}'$，并转发到需要到达的区域，目的区域 B、C、D 对接收到的数据进行译码并根据解密矩阵对译码后的数据进行解密，便可以得到原始信息 $\boldsymbol{M}$，区域 D 附近有一个窃听者，他能窃听到区域 D 接收到的信息，设窃听者可以窃听到部分信息，则根据 1.2 节给出的攻击模型，窃听者只能窃听到部分信息的线性组合；若窃听者能够窃听到区域 D 中用户接收到的所有信息，即其窃听到的消息为 $\boldsymbol{X}'=\boldsymbol{H}\boldsymbol{X}$，由于窃听者不知道字符 a，因此也就无法得到加密矩阵 $\boldsymbol{H}$，则计算不出原始的信息 $\boldsymbol{M}$。具

体如图 2 所示。

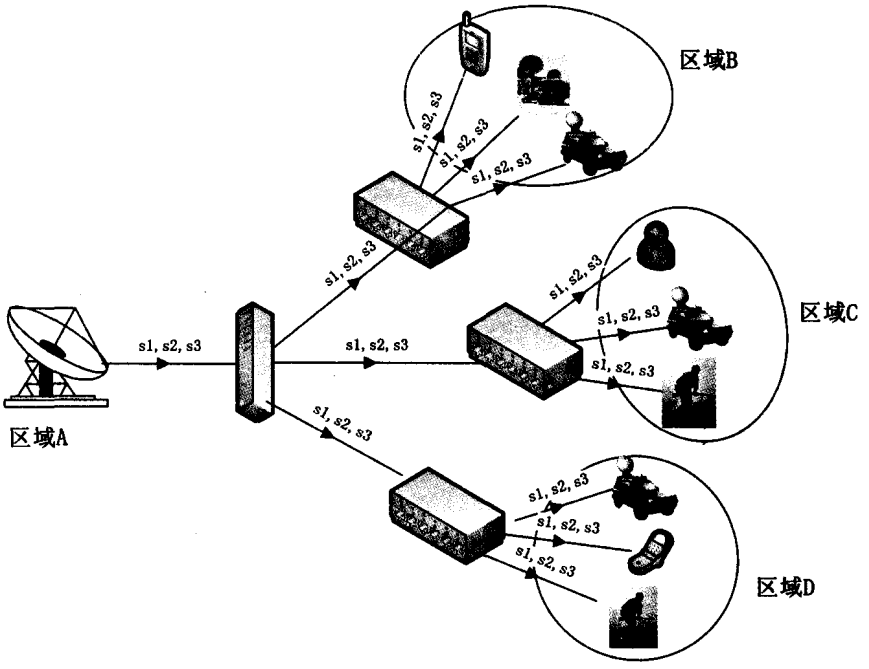

图 1 组播数据

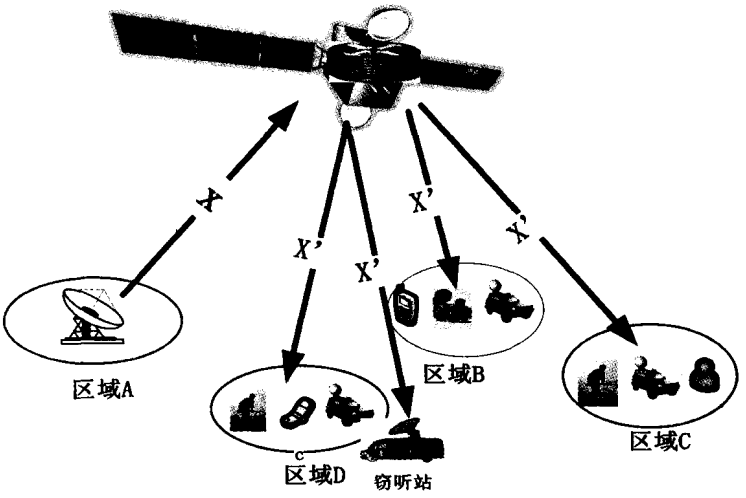

图 2 通信网络

3.3 基于卫星通信的多点通信

对于多点对多点的卫星通信网络，通过利用网络编码技术也可以提高网络容量的利用率。仍以上面的通信网络为例，若区域 B 的用户在同一时刻传送信息到区域 A 的用户，则卫星可以对接收到两区域的数据进行星上处理(编码)，然后只进行一次转发即可。其具体过程如图 3 所示。

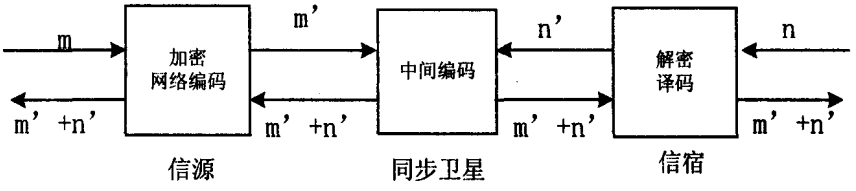

图 3 多点通信

4 结束语

文中基于同步卫星网络中的特点，针对窃听者在一定的窃听能力下，利用密码学中门限方案给出了一种能使网络达到弱安全的网络编码方案。首先，在数据传输之前，信源利用地面组播技术，组播一组可以用来计算出加密矩阵的数据，只要地面窃听者窃听到的信道数小于网络组播的最大流即可，从而实现了密钥共享。其次，数据传输过程中，用户与卫星之间传输的数据均经过加密并编码，分散了原始数据信息，即使窃听者窃听到卫星与用户之间传输的数据，也无法得到原始信息。最后，如果是多点到多点的数据通信，同步卫星对来自不同方向的数据利用网络编码技术进行编码，提高了网络容量的利用率。

参考文献：

[1] Yeung R W, Zhang Z. Distributed source coding for satellite communications [J]. IEEE Transactions on Information Theory, 1999, 45 (4): 1111-1120.

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

[3] Cai N, Yeung W. Secure network coding [C]// Proceedings of IEEE International Symposium on Information Theory. [s. l.]: IEEE, 2002.

[4] Bhattad K, Narayana K R. Weakly secure network coding [C]//First Workshop on Network Coding, Theory and Applications. Riva del Garda, Italy: [s. n.], 2005.

[5] Jain K. Security based on network topology against the wiretapping attack [J]. IEEE Wireless Communications, 2004, 11 (2): 68-71.

[6] Vilela J P, Lima L, Barros J. Lightweight security for network coding [C]//IEEE International Conference on Communications. Porto: IEEE, 2008: 1750-1754.

[7] 罗明星，杨义先，王励成，等. 抗窃听的安全网络编码[J]. 中国科学：信息科学, 2010, 40(2):

(下转第 166 页)

进行控制。可以根据需要改变参数绘制出自己所需要的效果。

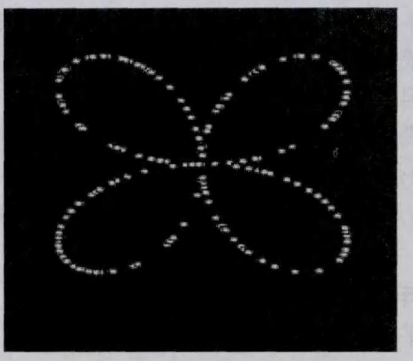

图 4 $\rho = \sin(2\theta)$ 运行结果

图 5 $v_x = \sin(2\theta)\sin(5\theta)\cos\theta$,
$v_y = \sin(2\theta)\cos\theta\sin\theta$ 运行结果

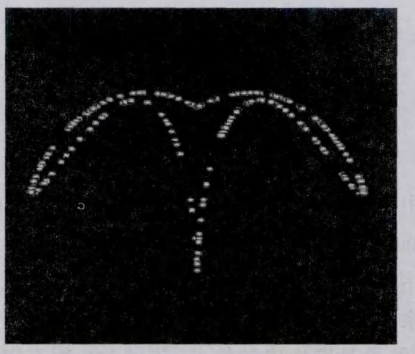

图 6 $v_x = \sin(2\theta)\sin(2\theta)\cos\theta$,
$v_y = \sin(3\theta)\cos(4\theta)\sin\theta$ 运行结果

由于需要对烟花爆炸之后的轨迹进行控制，在爆炸之后并没有考虑风速及重力的作用。另外，在此基础上，系统中还可以加入声音及其它渲染特性，使得燃放的效果更加逼真。

参考文献：

[1] 汪继文，郑 峰. 基于 OpenGL 与粒子系统的喷泉模拟实现[J]. 计算机技术与发展，2011，21(8)：161-164.

[2] Reeves W T. Particle system-a technique for modeling a class of fuzzy objects[J]. Computer Graphics，1983，2(2)：80-93.

[3] Reeves W T. Approximate and probabilistic algorithms for shading and rendering structured particle system[J]. Computer Graphics，1985，19(3)：313-322.

[4] 王晓娟. 基于粒子系统动态烟花的模拟[J]. 青海大学学报，2009(4)：29-32.

[5] Loke T，Tan D，Seah H. Rendering Fireworks Displays[J]. IEEE Computer Graphics and Applications，1992，12(3)：33-43.

[6] 罗玉玲. 粒子系统与纹理映射相结合模拟礼花的研究[J]. 电脑知识与技术，2004(20)：70-72.

[7] 蔡政策，魏 臻，凌 勇，等. 基于 ORGE 粒子系统在烟花渲染中的研究[J]. 计算机技术与发展，2011，21(10)：88-91.

[8] 陈俊丽，徐蔚峰，黄 炳，等. 基于粒子系统的飞行特效模拟[J]. 上海大学学报，2011(2)：138-142.

[9] 罗 勇. 基于粒子系统的喷泉模拟在煤炭降尘中的应用[J]. 煤炭技术，2011(4)：222-224.

[10] 和平鸽工作室. OpenGL 高级编程与可视化系统开发[J]. 北京：中国水利水电出版社，2006.

[11] 卫丽芬，李仰军. 基于粒子系统的喷泉模拟实验[J]. 电子测试，2010(2)：24-26.

[12] Shreiner D. OpenGL 编程指南[J]. 李 军，徐 波译. 北京：机械工业出版社，2010.

[13] 葛 芳，张 成，韦 穗，等. 基于粒子系统的烟花动画设计[J]. 计算机技术与发展，2010，20(8)：180-183.

(上接第 146 页)

371-380.

[8] 周业军，李 晖，马建峰，等. 一种防窃听的随机网络编码[J]. 西安电子科技大学学报，2009，35(1)：696-701.

[9] 曹张华，唐元生. 基于网络编码保密通信[J]. 通信学报. 2010(S1)：188-194.

[10] 张之学. 搭线窃听网络中的安全网络编码[D]. 北京：北京邮电大学，2010.

[11] 朱雪寒，夏卓群，刘品超，等. 基于网络编码的 ECC 验证方案在 WSN 中的研究[J]. 计算机技术与发展，2011，21(2)：173-176.

[12] 周红敏，孙名松，唐 亮. 基于网络编码的 P2P 流媒体直播系统研究[J]. 计算机技术与发展，2008，18(6)：225-227.

[13] Sanders P，Egner S，Tolhuizen L. Polynomial time algorithms for network[M]. New York，NY，USA：ACM，2003：286-294.