一种改进的混沌掩盖技术

赵柏山　　朱义胜
(大连海事大学信息工程学院　大连　116026)

摘　要：该文分析了目前混沌掩盖系统存在的问题，产生的原因并提出了改进的方案。通过理论分析和计算机仿真，证明了改进方案真正实现了混沌掩盖通信。与原型系统对比，改进方案同时改善了系统的性能。

关键词：混沌掩盖；混沌噪声；频谱
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2007)03-0699-03

An Improved Secure Communication System Based on Chaotic Masking

Zhao Bai-shan　　Zhu Yi-sheng
(*College of Information Engineering*, *Dalian Maritime University*, *Dalian* 116026, *China*)

Abstract: This paper discusses the reason of the security weakness of generalized state-space observers-based approaches for secure communication, using chaotic masking and chaotic nodulation of a Lorenz system and proposes a method to solve this problem. Theoretical analysis and simulation show this improvement realized chaotic masking. By comparison with the original system, this method improves the performance of secure communication system based on chaotic masking.

Key words: Chaotic masking; Chaotic noise; Spectrum

1　引言

自混沌系统可以实现同步之后，利用混沌和混沌同步实现保密通信已经成为近几年保密通信技术的研究热点。人们相继提出了混沌同步传输信息的多种方法，掩盖法是其中的主要方法之一，基于掩盖原理设计出各种保密通信系统[1−4]。同时该种方法也是目前争论最多的一种方法。文献[1]中设计了基于状态空间观测器的两种不同混沌掩盖方案，并给出了可行性的证明，但在论文中没有给出调制后在信道中传输的波形；而在文献[5]中，作者通过对信道中的传输波形的处理，证明了文献[1]中混沌掩盖方案的不保密性。针对上述问题，本文探讨了混沌掩盖方案不保密的原因，并提出了解决方法。新方案是通过改善混沌噪声的频谱分布实现掩盖的目的。

2　混沌掩盖方案的不保密性

文献[1]中给出的两种混沌掩盖方案的基本模型如图 1 所示，可以用下面公式表示：

$$\left.\begin{aligned}\dot{x} &= \boldsymbol{A}x + \boldsymbol{B}s + f(x,y)\\ y &= \boldsymbol{C}x + \boldsymbol{D}s\end{aligned}\right\} \tag{1}$$

并且文献[1]中也给出了两种 Lorentz 系统及其相应参数，针对第 1 个系统：

$$\dot{x}=\begin{bmatrix}-\delta_1 & \delta_2 & 0\\ \gamma & -1 & 0\\ 0 & 0 & -b\end{bmatrix}x+\begin{pmatrix}0\\ -yx_3\\ yx_2\end{pmatrix}+\boldsymbol{B}s \tag{2}$$

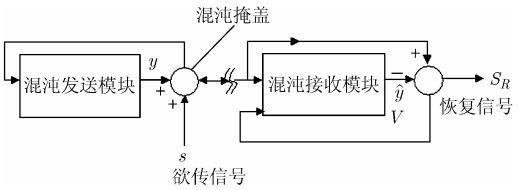


图 1　混沌系统模型

系统给定如下的参数：$(\sigma_1,\sigma_2,r,b)=[10,10,28,8/3]$, $s(t)=0.05\sin(60\pi t)$, $\boldsymbol{B}=[30\ 28\ 0]^{\mathrm{T}}$, $y=[1\ 0\ 0]x+s$。进行仿真得到图 2，图 3 所示结果。

从图 2，图 3 可以看出有用信号的幅度远小于混沌掩盖信号的幅度，满足文献[2，6]所提到的同步条件，但由图 2 可以看出 y' 信号属于慢变信号，其功率大都集中在低频。对其进行傅里叶变换，清楚地看出欲传输信号的频谱暴露突出，这点印证了文献[5]中的结论。这就失去了混沌掩盖系统的意义。经过分析可以通过改善混沌噪声的功率谱分布或改造信号的频谱特性来最终实现混沌掩盖的目的。本文提出改

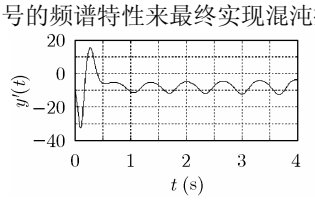


图 2　$y'(t)$波形

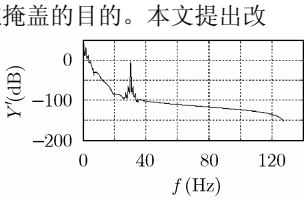


图 3　y'频谱

2005-07-14 收到，2005-12-14 改回
国家教育部博士点基金(20040151003)和交通部交通应用基础基金(200332922501)资助课题

善混沌噪声的功率谱分布的方案。

3 改善混沌噪声功率谱分布

由图 2 看出混沌噪声信号的变化速率缓慢是制约混沌掩盖技术的关键，如果能够在系统状态方程中增大状态变量导数的数值，那么混沌信号在完成一周对吸引子的趋近过程所需的时间将会缩短，反映在时域波形中，即从波峰到波峰的时间变小；反映在频域波形中，即噪声信号的频谱向高频移动。根据这一思路，我们在状态方程中给系数矩阵 $\boldsymbol{A}$ 乘上一个系数 N (N 为一常数)。考虑到文献[6]中证明了只要状态观测器的系数矩阵 $\boldsymbol{A}$ ， $\boldsymbol{C}$ ， $\boldsymbol{L}$ ，($\boldsymbol{L}$ 为式(1)中的 $\boldsymbol{B}$)满足 $(\boldsymbol{A}-\boldsymbol{C}\boldsymbol{L}^{\mathrm{T}})$ 是指数稳定矩阵，那么系统的动态误差趋于零。因此在不改变 $(\boldsymbol{A}-\boldsymbol{C}\boldsymbol{L}^{\mathrm{T}})$ 矩阵性质的前提下，在状态方程中将 $\boldsymbol{L}$ 同时乘上一个系数 N ，那么得到新的混沌系统为

$$\left.\begin{aligned}\dot{x} &= N\times\boldsymbol{A}x + N\times\boldsymbol{L}s + f(x,y)\\ y &= \boldsymbol{C}^{\mathrm{T}}x + s\end{aligned}\right\} \tag{3}$$

接收端为

$$\left.\begin{aligned}\dot{\hat{x}} &= N\times\boldsymbol{A}\hat{x} + N\times\boldsymbol{L}(y'-\hat{y}) + f(x,y')\\ \hat{y} &= \boldsymbol{C}^{\mathrm{T}}\hat{x}\end{aligned}\right\} \tag{4}$$

根据文献[6]中式(2)–式(7)的证明，新系统的系数矩阵满足

$$\left\|\exp\left(N\times(\boldsymbol{A}-\boldsymbol{L}\boldsymbol{C}^{\mathrm{T}})t\right)\right\| \le m_1^{N}\exp(-N\times\alpha_2 t) \tag{5}$$

最后只需满足

$$N\times\alpha_1 > {m_1}^{N}\gamma+\sigma\ ,\quad \sigma\ge 0 \tag{6}$$

这个条件。根据非线性理论的 Lipschitz 条件以及合理选择 $\boldsymbol{L}$ 可以得到式(6)的充分条件。

4 举例及仿真结果

以文献[3]中的第 3 个例子——混沌 Lorenz 系统为原型，对其进行改造。N 的取值决定掩盖结果的好坏，这里取 N=6 ，则系统可以表示成为

$$\left.\begin{aligned}\dot{x} &= 6\times\begin{bmatrix}-10 & 10 & 0\\ 28 & -1 & 0\\ 0 & 0 & -8/3\end{bmatrix}x + \begin{bmatrix}0\\ -y'x_3\\ y'x_2\end{bmatrix} + 6\times\boldsymbol{L}s\\ y' &= \begin{bmatrix}1 & 0 & 0\end{bmatrix}x + s\end{aligned}\right\} \tag{7}$$

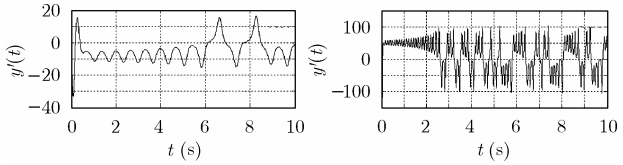
其中 s 为有用信号。接收端的系统模型为

$$\left.\begin{aligned}\dot{\hat{x}} &= 6\times\begin{bmatrix}-10 & 10 & 0\\ 28 & -1 & 0\\ 0 & 0 & -\frac{8}{3}\end{bmatrix}\hat{x} + \begin{bmatrix}0\\ -y'x_3\\ y'x_2\end{bmatrix} + 6\times\boldsymbol{L}(y'-\hat{y})\\ \hat{y} &= \begin{bmatrix}1 & 0 & 0\end{bmatrix}\hat{x}\end{aligned}\right\} \tag{8}$$

$\boldsymbol{L}$ 为文献[6]中选定的 $\boldsymbol{L}=\begin{bmatrix}30 & 28 & 0\end{bmatrix}^{\mathrm{T}}$，可得 $(N\boldsymbol{A}-N\boldsymbol{C}\boldsymbol{L}^{\mathrm{T}})$ 的特征值为–240，–6，16。仿照文献[6]中的证明过程，可以证明混沌系统的动态误差随时间的推移趋近于零。下面给出有用信号为 $s(t)=0.05\sin(60\times\pi\times t)$ 时，原型系统与改进系统参量的对照图(图 4–图 8)。

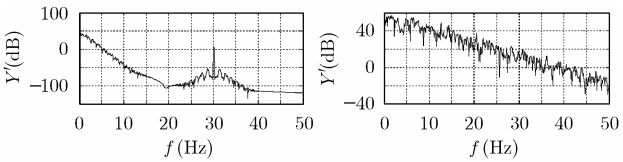
从图 4 可以看出 y' 的变化速率较原型有很大提高，观察图 5(a)中有用信号频谱暴露在外，因此用文献[5]中提到的方法可以轻易地破解出有用信号；而图 5(b)的有用信号频谱完全掩盖在混沌噪声频谱之中，实现了掩盖的目的，不能通过简单的滤波算法破解出有用信号。系统在信道中传输的混沌信号 y' 变化速率的加快也可以从图 6 的相平面图中直观看出——在相同的时间内，相曲线在两个吸引子之间的跳转次数有显著的增加。以上的仿真结果与先前的分析保持一致。

在接收端，系统的性能也同样有所改善。由于系数的增加，混沌系统的接收系统可以在相对较短的时间内恢复出欲传信号，这点反映在图 7，图 8 中。



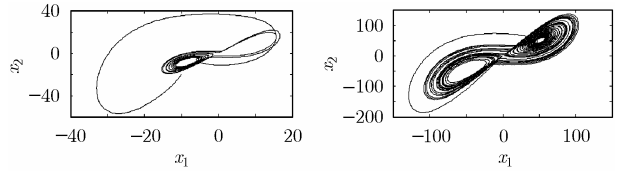
(a) 原型 y' 的时域波形　(b) 增加系数后 y' 的时域波形

图 4



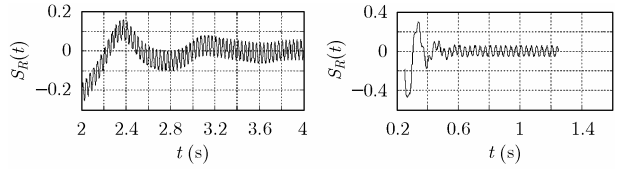
(a) 原型 y' 频谱　(b) 增加系数后 y' 频谱

图 5



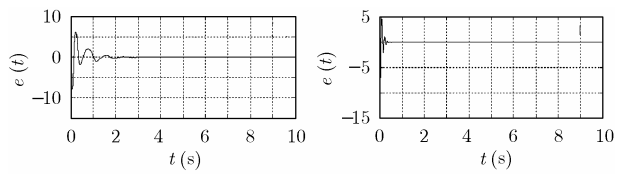
(a) 原型相平面图　(b) 增加系数后相平面图

图 6



(a) 原型 S_R 波形　(b) 增加系数后 S_R 波形

图 7



(a) 原型误差曲线　(b) 增加系数后误差曲线

图 8

需要说明的是，混沌系统在乘上一个系数后，其在信道中传输信号的幅度相对较大，这一点在模拟系统中很难实现。同时还需要指出，采用这个方案的混沌系统，在增大有用信号的频率时，混沌系统的系数 N 也得随之相应增大，使混沌噪声的功率谱能够覆盖到更高的频率，从而将有用信号频谱掩盖。否则将会出现文献[5]中提到的情况。

5　结束语

本文深入讨论了混沌掩盖技术中出现的问题：一些系统不能够实现保密通信及产生的原因，并在上述系统的基础上提出了改进的方案，经过仿真证明改进的方案能够取得预期的效果。并针对不同的情况说明了需要注意的问题。

经过仿真得到，该种改进方法也适用于其他类型的混沌掩盖系统。

参 考 文 献

[1] Boutayeb M, Darouach M, and Rafaralahy H. Generalized state-space observers for chaotic synchronization and secure communication. [J]. *IEEE Trans. Circuits Syst.* I, 2002, 49: 345–349.

[2] 李建芬, 李农. 一种新的蔡氏混沌掩盖通信方法[J]. 系统工程与电子技术, 2002, 24(4): 37–410.
Li Jian-fen and Li Nong. A new chaotic masking method for secure communications based on Chua's circuit. *Systems Engineering and Electronics*, 2002, 24(4): 37–410.

[3] 吴敏, 丘水生. 一个混沌保密通信方案的改进[J]. 通信技术, 2003, (1): 103–105.

[4] 朱双鹤, 李小春等. 一种新的混沌掩盖保密通信方案[J]. 空军工程大学学报(自然科学版), 2002, 3(6): 37–41.
Zhu Shuang-he and Li Xiao-chun, *et al.*. A new chaotic masking scheme with applications to secure communications. *Journal of Air Force Engineering University* (*Natural Science Edition*), 2002, 3(6): 37–41.

[5] Alvarez G, Montoya F, Romera M, and Pastor G. Breaking two secure communication systems based on chaotic masking. [J]. *IEEE Trans. Circuits Syst.* II, 2004, 51: 505–506.

[6] Liao T and Huang N. An observer-based approach for chaotic synchronization with applications to secure communications. [J]. *IEEE Trans. Circuits Syst.* I, 1999, 46: 1144–1150.

赵柏山：　男，1985 年生，硕士生，研究方向为滤波器理论及混沌信号处理.

朱义胜：　男，1945 年生，教授,博士生导师. 中国电子学会高级会员，美国 IEEE 高级会员，研究方向为电路理论、非线性理论及宽带接入技术.