混沌序列在安全网络编码算法中的应用研究*

徐光宪，吴 巍
（辽宁工程技术大学 电子与信息工程学院，辽宁 葫芦岛 125105）

摘 要：为提高网络编码的安全性提出了一种在信源处使用混沌序列与信源信息相结合，在信宿处列表译码的安全网络编码算法。该算法使用改进型 Logistic 映射产生混沌序列对信源消息进行处理，传输过程保持原有网络编码体制不变，可以抵抗多种窃听和污染攻击。经过系统仿真及理论分析可知，该算法舍弃部分带宽来保证网络的安全性，以较小的开销达到了信息论安全的要求。最终实现了混沌序列在安全网络编码算法中的应用。

关键词：安全网络编码；改进型 Logistic 映射；混沌序列；列表译码；系统仿真
中图分类号：TP393.08 **文献标志码**：A **文章编号**：1001-3695(2014)04-1212-03
doi:10.3969/j.issn.1001-3695.2014.04.061

Research on application of chaotic sequence in security of network coding

XU Guang-xian, WU Wei
(*School of Electronic & Information Engineering, Liaoning Technical University, Huludao Liaoning* 125105, *China*)

Abstract: To improve the security of network coding, this paper presented a secure network coding algorithm. It combined chaotic sequence with source information and used list-decoding to sink. This algorithm adopted advanced Logistic map to generate chaotic sequence in order to deal with the source information and the transmission process still kept the original network coding system. It not only can resist a variety of wiretapping attacks but also can resist pollution attacks. The system simulation and theoretical analysis confirm that this algorithm abandons part of bandwidth to ensure the security of network and achieves the information-theoretic security condition with minimum overhead. It finally realized the application of chaotic sequence in the secure network coding algorithm.

Key words: secure network coding; advanced logistic map; chaotic sequence; list-decoding; system simulation

传统的计算机网络大多是基于存储和转发的路由机制，该网络的中间节点除了复制数据以外，一般不需要作何数据处理。2000 年 Ahlswede 等人[1]首次阐述了网络编码的基本原理，其核心思想是中间节点对接收到的信息按照合适的方式进行编码处理后传输给下级节点，直到经过编码处理后的信息全部到达信宿，通过信宿的译码处理，获得信源发出的原始信息。网络编码技术实现了网络的最大流传输，有效解决了中继节点传输的瓶颈问题，在提高网络吞吐量、改善负载均衡、减小传输延迟、节约节点能耗、增强网络鲁棒性等方面均具有重要意义。黄佳庆等人[2]归纳了网络编码理论问题研究内容和成果并讨论了其发展方向。在应用网络编码的网络中，由于信息的扩散性较强，这种情况下，攻击者只需加入很小的污染信息就能对大部分网络造成影响，因此与传统网络相比，相同的攻击手段，在基于网络编码的网络中攻击效率更高，传染性更强。网络编码的安全问题目前考虑的主要是窃听攻击和污染攻击。窃听攻击是指攻击者通过对网络中的节点进行窃听来获取有用信息。2002 年 Cai 等人[3]构建了窃听网络的通信模型，设计了一种信息论安全的网络编码算法。在此基础上 Feldman 等人[4]通过舍弃部分带宽给出了在较小有限域上的编码算法，简化了 Cai 等人的算法。在上述抵抗窃听攻击的方案中，均需假设窃听者的计算能力有限。污染攻击则是指攻击者对信道中传输的信息进行窜改，阻止信宿正确地恢复出源消息。俞立峰等人[5]介绍了基于密码学的 SPOC(secure practical network coding)和 P-coding 模式，并对两者进行了分析比较。Krohn 等人[6]提出用同态哈希函数来核实 P2P 系统下载文件的原始文件组的线性组合。Gkantsidis 等人[7]对 Krohn 的方案进行了扩展，针对基于网络编码的 P2P 文件分发系统的抗污染攻击能力，提出了同态哈希方案。在上述方案中均需要一条额外的安全信道，使得该方案在大多数情况下不可行，在信源处采用列表详码法的编码方案。

基于以上背景，本文提出了一种在信源处结合混沌序列，在信宿处采用列表译码法的编码方案。

1 基本概念

本文主要研究单源无圈网络，在有向图 $G=(V,E)$ 中，V 称为图 G 的节点集，E 称为图 G 的链路集。有向链路用 $e=(u,v)$ 表示，用 $v=\text{head}(e)$ 来表示链路 e 的头，用 $u=\text{tail}(e)$ 来表示链路的尾。定义 $\Gamma_I(v)=\{e\in E|\text{head}(e)=v\}$ 即节点 v 的输入链路集合，称其大小 $|\Gamma_I(v)|$ 为节点 v 的入度；定义 $\Gamma_O(v)=\{e\in E|\text{tail}(e)=v\}$ 即节点 v 的输出链路集合，称其大小 $|\Gamma_O(v)|$ 为节点 v 的出度。本文只考虑线性网络编码，下文关于线性网络编码的基本概念引自文献[8]。

定义 1 令 F 为有限域，ω 为正整数。非循环网络中一个 ω 维，F 取值的线性网络编码，对每一对邻接信道对 (d,e)，存

收稿日期：2013-06-07；**修回日期**：2013-07-29 **基金项目**：辽宁省高等学校杰出青年学者成长计划资助项目(LJQ2012029)

作者简介：徐光宪(1977-)，男，江苏盐城人，副教授，博士，主要研究方向为网络编码与信息处理(flybirdxgx@sohu.com)；吴巍(1988-)，女，硕士研究生，主要研究方向为信息论与编码.

在一个标量 $k_{d,e}$,每条信道 e 对应一个 ω 维列向量 f_e,称为信道 e 的全局编码核,并满足如下条件:

a) $f_e = \sum_{d \in \Gamma_I(T)} k_{d,e} f_d$,其中 $e \in \Gamma_O(T)$;

b) ω 个虚拟信道 $e \in \Gamma_I(S)$ 的向量 f_e 形成了向量空间 F^ω 的自然基底。

由定义 1 可知,假设信源 S 产生的 n 维消息向量用 $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ 表示,该向量的各个分量均取自有限域 F,从而信道 e 上传输的数据为 xf_e,记为 $Y(e)$。若信宿节点 T 的输入用向量 $\boldsymbol{z} = (z_1, z_2, \cdots, z_n)$ 来表示,则可以用 $\boldsymbol{z} = \boldsymbol{x}\boldsymbol{M}$ 来表示输入变量与输出变量之间的关系,其中矩阵 $\boldsymbol{M}$ 就称为系统转移矩阵。因此,若想信源节点可以由接收到的消息解码出信源的输入消息,就必须要求系统的转移矩阵 $\boldsymbol{M}$ 是可逆的。对系统转移矩阵的求解方法详见文献[8]。

2　基于混沌序列的安全网络编码方案

混沌序列[9]是一种伪随机序列,理论分析表明,混沌序列具有非常好的伪随机性、自相关与互相关特性,对初值具有敏感性、难以预测性和可重复性,且混沌序列在非线性映射或非线性系统中才能产生,其映射状态是在反复的分离与折叠下形成的,所以混沌的映射关系绝不可逆。因此混沌序列在保密通信中具有非常大的应用前景。目前混沌序列在网络加密中的应用已经有了大量相关研究,并逐渐渗透到安全网络编码领域。付晓在文献[10]提出了一种基于混沌序列的安全网络编码方案。这种算法实现了一次一密的加密体质,达到了信息论安全的要求。但是该方案仅能抵抗窃听攻击,对污染攻击抵抗能力差。然而在大多数网络中污染攻击都是可能存在的,因而该方案具有漏洞,在实际应用中存在弊端。

3　改进的安全网络编码方案

本方案在文献[10]的基础上融合了列表译码法的思想,不仅利用混沌序列实现了一次一密的编码体制,从而抵抗全能的窃听攻击,又利用了列表译码法来加强了对污染攻击的抵抗能力。该方案的编码流程如图 1 所示。

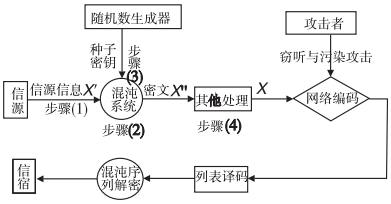


图1　安全网络编码流程图

3.1　信源消息加密

假设信源的网络容量为 m,信源发送 n 个长度为 $n-1$ 的信源消息向量 $\boldsymbol{X}'$ 如式(1)所示,注意 $n \leqslant m$。

$$\boldsymbol{X}' = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & & \vdots \\ x_{(n-1)1} & x_{(n-1)2} & \cdots & x_{(n-1)n} \end{pmatrix} \tag{1}$$

混沌系统使用改进型 Logistic 映射来生成混沌序列 $y_1, y_2, \cdots, y_n$,将其用 $Y(\,)$ 表示,该映射的函数表达式为 $y_n = 1 - 2y_{n-1}^2 (-1 < y_n < 1)$。

随机数生成器生成 n 个随机数 $\beta_1\beta_2\cdots\beta_n$ 作为种子密钥,然后利用步骤(2)中生成的混沌序列与步骤(3)中生成的随机数对信源发出的每一个原始消息加密,算法如下所示,其中 $1 \leqslant k \leqslant n$。

$$X_k = (x_{1k} + Y(\beta_k), \cdots, x_{(n-1)k} + Y(x_{1k}, \cdots, x_{(n-2)k}, \beta_k), \beta_k)^{\mathrm{T}}$$

则 $\boldsymbol{X}'' = (X_1 \quad X_2 \quad \cdots \quad X_k \quad \cdots \quad X_n)$;构建矩阵 $\boldsymbol{X} = \begin{pmatrix} \boldsymbol{I} \\ \boldsymbol{X}'' \end{pmatrix}$,$\boldsymbol{I}$ 为 $n \times n$ 的单位矩阵,用来记录传输过程中随机编码向量的单位矩阵。将该消息向量 $\boldsymbol{X}$ 输入信道,利用中间节点对其进行随机线性组合即网络编码。

3.2　信宿译码

记攻击者输入的 t 个污染消息向量构成 $n \times t$ 的矩阵 $\boldsymbol{T}$,信宿 z 接收到的消息向量记为 $\boldsymbol{Z}$,$\boldsymbol{X}$ 和 $\boldsymbol{Z}$ 对应的传输矩阵分别为 $\boldsymbol{M}$ 和 $\boldsymbol{M}'$。

a)信宿 $\boldsymbol{Z}$ 接收到的消息如式(2)所示:

$$\boldsymbol{Z} = \boldsymbol{M}\boldsymbol{X} + \boldsymbol{M}'\boldsymbol{T} = (\boldsymbol{M} \quad \boldsymbol{M}') \begin{pmatrix} \boldsymbol{X} \\ \boldsymbol{T} \end{pmatrix} \tag{2}$$

b) 构建 $\boldsymbol{Z}$ 中列向量的一极大线性无关组构成的矩阵即秩为 $n+t$ 的矩阵 $\boldsymbol{Z}^n$,注意 $\boldsymbol{Z}^n$ 要包含 $\boldsymbol{Z}$ 的前 n 列;

c)求解出矩阵 $\boldsymbol{G}$,如式(3)所示:

$$\boldsymbol{G} = (\boldsymbol{Z}^n)^{-1}\boldsymbol{Z} \tag{3}$$

d)设 $\boldsymbol{X}^n$ 和 $\boldsymbol{T}^n$ 是 $\boldsymbol{X}$ 和 $\boldsymbol{T}$ 中与 $\boldsymbol{Z}^n$ 对应的列组成的矩阵,则有

$$\boldsymbol{X} = \boldsymbol{X}^n\boldsymbol{G} \tag{4}$$

$$\boldsymbol{T} = \boldsymbol{T}^n\boldsymbol{G} \tag{5}$$

e)设 $\boldsymbol{G}_1$ 表示 $\boldsymbol{G}$ 的前 n 列,$\boldsymbol{G}_2$ 表示 $\boldsymbol{G}$ 的后 t 列,所以由式(6)可以恢复信源发出的消息 $\boldsymbol{X}''$。

$$\boldsymbol{X}'' = G_1 + X_1^n G_2 \tag{6}$$

f)经过上述步骤后,信宿 $\boldsymbol{Z}$ 已恢复了 $\boldsymbol{X}''$,由于信宿知道改进型 Logistic 映射,再通过运用随机数 $\beta_1\beta_2\cdots\beta_n$,分别恢复出信源的 n 个原始消息向量。

4　系统仿真

本文仿真环境为 Dell PC 机,处理器为 Intel® Core™ i5-3210M CPU @ 2.50 GHz,内存为 4.00 GB,操作系统为 64 位 Windows 7,使用 MATLAB R2011b 进行系统仿真。

假设信源每次可发送 9×10 的矩阵,即表达式(1)中的 $n = 10$。要发送的文件为“网络编码. txt”,如图 2(a)所示,经过混沌序列处理后,得到的文件如图 2(b)所示,经过解码后得到的文件如图 2(c)所示。

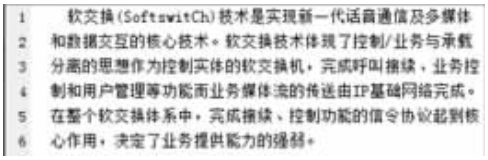
创建 10 个文本文档,大小分别为 100 Byte,200 Byte,300 Byte,…,1000 Byte。将这些文档依次送入仿真系统中进行传输并记录传输所用时间 t,由公式 $R = \frac{I}{t}$ 即可求得信息传输速率。其中 R 表示信息传输速率,I 表示信息量,即文本的大小。这 10 个文本的信息传输速率曲线如图 3 所示,其横坐标为传输所用时间 t,单位为 s,纵坐标为传输速率 R,单位为 kbps。

经过上述仿真可验证该算法可以有效地利用改进型 Logistic 映射对信源信息进行混沌处理,在以较高的速率传输信息的同时能以极小的误码率恢复原始信源信息。

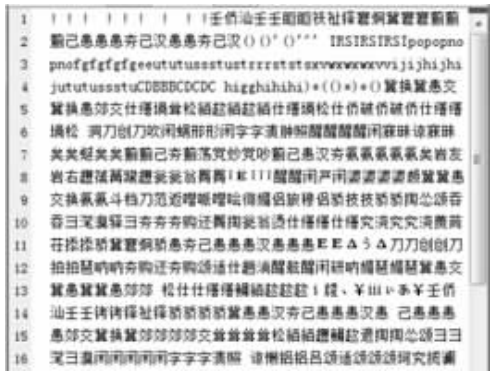
5　性能比较与分析

文献[11]提出了一种利用字符的本原根构造新的信息向量的信源编码算法。该算法在构造的信息向量中加入了字符 p

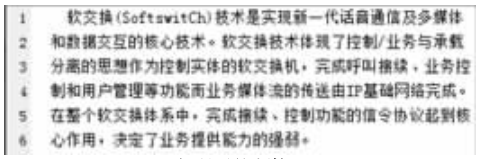
和它的一个本原根 a。为了保证窃听者不能获得原始信息,则两个字符中的任何一个都不能被窃听。该算法不仅增加了加密信息的带宽占用率,而且限制了编码向量的分配。文献[12]利用一次一密的思想加密了信息,达到了保密通信的要求,但是仅适用于容量为偶数的网络。在本文的方案中,仅通过引入一个密钥信息就达到了一次一密的保密通信的要求。与上述方案相比,既降低了加密信息的带宽占用率又减小了对编码向量分配的限制,同时该算法对网络容量没有做过多要求。



(a)等待发送的文件



(b)经混沌处理后的文件



(c)解码后的文件

图2 源文件及处理后的文件

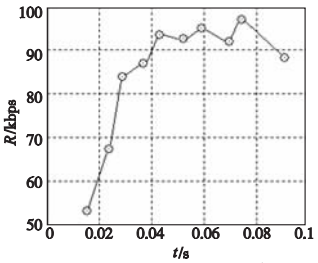


图3 信息传输速率曲线

此外,本文提出的算法既能有效抵抗窃听攻击也能过滤掉主动攻击者注入的污染信息,达到抵抗污染攻击的目的。下面分别对上述两种攻击者存在的情况下,系统仍然能够实现保密通信的功能加以说明。

在本文中假设窃听者可以窃听网络中的所有信道,为了与其进行对抗,本文利用了一次一密的密码体制对原始消息进行了加密,并将密钥整合进加密后的消息中,不需要额外的保密信道。对于窃听者来说,即使获得了网络中传输的消息数据,也难以获得信源消息,即窃听者窃听到的数据为 $Q=\begin{bmatrix} i_{11} & i_{12} & \cdots & i_{1n}q_{11} & q_{12} & \cdots & q_{1n} \\ i_{21} & i_{22} & \cdots & i_{2n}q_{21} & q_{22} & \cdots & q_{2n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ i_{n1} & i_{n2} & \cdots & i_{nn}q_{n1} & q_{n2} & \cdots & q_{nn} \end{bmatrix}$。由于改进型 Logistic 映射产生的混沌序列 $y_1,y_2,\cdots,y_n$ 是不可逆的,只要保证随机数 $\beta_1\beta_2\cdots\beta_n$ 的安全,即使窃听者经过计算获得随机序列,也无法恢复出信源原始消息,即 $I(Q|X')=0$,从而有效抵抗了全能窃听攻击。

对于污染攻击,由基于网络编码的列表译码法可以得出该算法能够以高于 $1-q^{n\varepsilon}$(ε 为某个小正数)的概率解出 X''[13],从而达到排除污染信息的目的,满足了安全通信的要求。

虽然本文提出的算法中为了实现信息安全加入了密钥信息,占用了源信息带宽,假设源信息率为 $H(X)$,密钥信息率为 $H(K)$,则在本文提出的方案中 $H(K)=\frac{1}{n-1}H(X)$,能实现安全通信。定义参量 $\rho=\frac{H(K)}{H(X)+H(K)}$ 为加密信息带宽占用率[14],则本文中的加密信息带宽占用率为 $\rho=\frac{\frac{1}{n-1}H(X)}{\frac{1}{n-1}H(X)+H(X)}=\frac{1}{n}$,表明当接收节点的入度足够大时,密钥所占带宽可忽略不计。

6 结束语

本文提出了一种既能抵抗窃听攻击又能抵抗污染攻击的安全网络编码算法。该算法利用了混沌序列与列表译码法的特性,对线性随机网络编码系统的信源和信宿编解码算法进行了改变,并对该算法进行了仿真。经理论分析和计算可知该算法虽然牺牲了较小的带宽,但能够以很高的概率达到信息论安全的要求,适用于所有的线性网络编码。

参考文献:

[1] AHLSWEDE R, CAI N, LI S Y R, *et al*. Network information flow [J]. IEEE Trans on Information Theory, 2000, 46(4): 1204-1216.

[2] 黄佳庆,陶少国,熊志强,等. 网络编码关键理论问题研究[J]. 计算机应用研究,2008,25(8):2260-2264.

[3] CAI N, YEUNG R W. Secure network coding[C]// Proc of IEEE International Symposium on Information Theory. [S. l.]: IEEE Computer Society, 2002: 323-340.

[4] FELDMAN J, MALKIN T, STEIN C, *et al*. On the capacity of secure network coding[C]// Proc of the 42nd Annual Allerton Conference on Communication, Control, and Computing. Monticello: Curran Associates, 2004: 30-40.

[5] 俞立峰,杨琼,于娟,等. 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.

[6] KROHN M N, FREEDMAN M, MAZIERESJ D. On-the-fly verification of rateless erasure codes for efficient content distribution[C]// Proc of IEEE Symposium on Security and Privacy. [S. l.]: IEEE Computer Society, 2004: 226-240.

[7] GKANTSIDIS C, RODRIGUEZ P. Cooperative security for network coding file distribution[C]//Proc of the 25th IEEE International Conference on Computer Communications. 2006: 743-757.

[8] 陈立山. 网络编码的安全性分析与研究[D]. 西安:西安电子科技大学,2010.

[9] 尹恒,吴陈. 混沌伪随机序列的产生及在网络安全中的应用[J]. 江苏船舶,2003,20(1): 32-34.

[10] 付晓. 防窃听和抗污染的低能耗安全网络编码方案研究[D]. 葫芦岛:辽宁工程技术大学,2012.

[11] 刘琼,潘进,刘炯. 基于信息论安全的防窃听网络编码方案[J]. 计算机工程,2012,38(22):107-110.

[12] 张岩. 一种改进的安全网络编码方案的研究[C]//中国电子学会第十五届信息论学术年会论文集. 北京: 国防工业出版社,2008: 962-966.

[13] 徐光宪,付晓. 一种基于列表译码法的改进的安全网络编码[J]. 小型微型计算机系统,2013,34(4):769-773.

[14] 李大霖,林雪红,林家儒,等. 安全网络编码的一个必要条件[J]. 北京邮电大学学报,2008,31(5):9-12.