一种基于混沌序列的安全网络编码设计与分析

徐光宪 李晓彤 罗荟荟
(辽宁工程技术大学电子与信息工程学院 葫芦岛 125105)

摘 要 提出了一种低开销的安全网络编码方案。该方案利用混沌序列较高的随机性和对初始条件极度敏感的特性,将混沌序列与原始信源消息向量相结合,构造出"一次一密"的密码体制,从而实现该编码方案的完善保密性。该方案仅在原随机网络编码体制的基础上对信源进行了改变,中间节点保持不变,具有普遍通用性;并且在信源处仅加入一个干扰信号来保证编码方案的安全性。理论分析结果表明,在攻击者具有有限窃听能力的情况下,该安全网络编码方案可以保证完善其保密性,且发送信号的开销最小。

关键词 网络编码,混沌序列,一次一密,通用性,完善保密,低开销
中图法分类号 TP309.7 **文献标识码** A

Analysis and Design of Network Coding Based on Chaotic Sequence

XU Guang-xian LI Xiao-tong LUO Hui-hui
(School of Electronic and Information Engineering, Liaoning Technical University, Huludao 125105, China)

Abstract A minimum overhead secure network coding based on chaotic sequence was presented in this paper. Only the source needs to be modified, and intermediate nodes implement a classical distributed network code. So the proposed scheme is applied to all the linear network coding. It combines the chaotic sequence with original source information vector, because of the high randomness and the sensitivity to initial state of chaotic sequence, and the presented network code is "One-Time Pad (OTP)". So the secure network coding achieves complete secrecy. This scheme requires only one noisy symbol to be embedded in the original information symbol vector to achieve complete secrecy. The theoretical analysis confirms that this scheme can achieve the information-theoretic security condition and the signaling overhead to obtain complete security is minimized, while the attacker has limited wiretapping ability.

Keywords Network coding, Chaotic sequence, One-time pad (OTP), Applicability, Complete secrecy, Minimum overhead

2000年,Ahlwede等[1]基于网络信息流的概念,首次提出了网络编码的思想,其目的是实现网络最大流和提高网络的吞吐量,然而更深一步的研究指出网络编码同时也是安全网络传输的好方法[1,2]。随后,Cai、J. Feldman、Zhang等[3-6]分别从窃听的网络通信模型、构造信息论安全的网络编码、安全网络编码的编码开销、信源消息的安全等方面展开研究。但由于在执行过程中伪装了数据,它们均增加了编码开销和网络节点的复杂性。

为了提高网络编码的鲁棒性,同时减小开销,M. R. 等[7]提出了将一种训练序列嵌入到信源数据中,并同时结合了信道编码的安全网络编码。该方案中将信道编码应用于整个数据包,增加了编码的复杂度。徐光宪等[8]利用稀疏矩阵的性质来降低节点的复杂性,然而其方案仍然要加入相当数量的保密冗余,编码开销并未减小。Adeli等[9]提出了一种基于Hash函数的小开销安全网络编码,但该方案却存在重要的安全漏洞[10]。Jain等[11]利用hash函数和网络编码相结合的方法,使得网络能以更高的速率传输数据。然而,这种方法使得编解码过程复杂化,仅仅适合节点数目较少、易得到整个网络拓扑的小型网络。Bhattad等[12]给出了一种体系较简单、有一定适用范围的抗窃听的弱安全网络编码。该编码方案使得安全网络编码的复杂性和开销降低,然而该方案实现的不是信息论意义上的安全,且线性变换的编码开销也不是最小的。赵慧、卓新建等[13]提出了一种安全性定理,并证明在编码中使用伪随机函数更能确保信源消息不被恶意攻击者获取。但是,该方案却需要知道整个网络的拓扑结构,不适用于大规模的网络。

而通过研究发现,在信源处编码使网络达到安全性要求是一种很实用的方法[14,15],它不仅降低了安全网络编码中间节点处理的复杂性,而且通过选择合适的变换和处理可以使编码开销达到最小。

综上所述,本文在以上研究的基础上,提出了一种在信源处加入伪随机序列的小开销安全网络编码方案。通过理论分

到稿日期:2012-09-10 返修日期:2012-12-18 本文受2012年辽宁省推荐国家级"大学生创新创业训练计划"项目(201210147036),辽宁高等学校杰出青年学者成长计划项目(LJQ2012029)资助。

徐光宪(1977—),男,博士,副教授,主要研究方向为网络编码与信号处理,E-mail:flybirdxgx@sohu.com;李晓彤(1990—),女,主要研究方向为信息论与编码;罗荟荟(1991—),女,主要研究方向为信息论与编码。

析和安全性定理的证明表明，该编码方案使用唯一的随机数和混沌序列与信源结合，通过合适的网络编码达到了完善保密性，保证了安全通信。

1 相关知识与定义

本文主要集中讨论一类非循环、无延时的单信源多信宿多播通信网络，以简化问题的分析。对于一个无环多播网络 $G=(V,E)$，V 是点的集合，E 是信道的集合，为构造网络码[1]，令 $GF(q)$ 为 q 阶有限域(这里 q 为一个大素数)。

定义 1(网络编码) 设 $G=(V,E)$ 为一个有向网络，在 G 上的 n 维线性网络码对 G 的每一条边 $e\in E$ 分配一个向量 $u(e)$，并使其具有以下性质(称 $u(e)$ 为信道 e 的"全局编码核"(global encoding kernel))。

(1)为信源 X 分配的向量空间为一个 n 维向量空间 $z(X)=GF_n(q)$；

(2)为边 $e\in E$ 分配的向量是到达边 e 尾节点 $tail(e)$ 的所有边上的向量的线性组合；若信源 X 是 e 的尾节点，则 e 上的向量在 $z(X)$ 中选取；

(3)在每一个信宿节点处，必须存在能够恢复信源信息的特定解码函数操作。

设节点 S 的向量空间为 $z(S)$，则对于任何非源节点 S，$z(S)$ 是到达 S 的每一条边上向量的所有可能线性组合的集合。所以对于 $e\in E$，有 $u(e)\in z(tail(e))$。

定义 2(信源 X) X 产生不可压缩的数据信息，记为 m。这些信息组成长度为 n 的向量，表示为 $m=(m_1,m_2,\cdots,m_n)^{\mathrm{T}}$；信宿 T：网络中共有 t 个信宿。

定义 3(攻击者 C) 攻击者 C 具有有限窃听能力，能够窃听 k 个信道，$\Omega=\{\alpha_1,\alpha_2,\cdots,\alpha_k\}$ 表示可被窃听的信道所构成的集合。

根据以上定义和相关知识，构建线性网络编码。每条边拥有一个编码向量 v_i，其中 i 表示网络中边的数目，即 i 从 1 到 $N=\|E\|$，则有：

$$v_i=(v_{i1},v_{i2},\cdots,v_{in})^{\mathrm{T}} \tag{1}$$

这些编码向量选自同一编码域。信道上传输的信息表示为 x_i，x_i 为所有信息的线性组合，有：

$$x_i=v_i^{\mathrm{T}}m,i=1,2,\cdots,N \tag{2}$$

2 原有安全网络编码方案

设攻击者最多可以窃听 k 个独立边(独立边指的是每条边相应的编码向量线性独立)，为了阻止攻击者获得有意义的信息，从编码域中选取 a 个随机数加入到信源信息中，表示为：

$$\overline{m}=(m_1,m_2,\cdots,m_{n-a},z_1,z_2,\cdots,z_a)^{\mathrm{T}} \tag{3}$$

回顾文献[3-6]中已提出的可达到完善保密的安全网络编码方案。他们的基本方法是确保攻击者不会使加入信息中的冗余信息无效。为达到这一目的，设

$$V\overline{m}=[v_1,v_2,\cdots,v_k]^{\mathrm{T}}\overline{m}=[x_1,x_2,\cdots,x_k]^{\mathrm{T}} \tag{4}$$

式中，v_i 代表 i 边相应的 n 维编码向量，V 是这些编码向量组合而成的矩阵。

若将 $V_{k\times n}$ 分割成为两个子矩阵，其中 $A_{k\times(n-a)}$ 对应含有原始信源消息向量的 $\overline{m}$，$B_{k\times a}$ 对应冗余信息，则有：

$$[A_{k\times(n-a)}\,|\,B_{k\times a}]\overline{m}=(x_1,x_2,\cdots,x_k)^{\mathrm{T}} \tag{5}$$

若要使攻击者不能通过窃听而得到有用的信息，就要求子矩阵 B 中的列均线性独立，即 $a\geqslant k$。因此，$\overline{m}$ 中分配的冗余信息数量应不少于 k。

现有的方案主要是将随机数加入到编码向量中，然后与信息进行线性组合。这种方法就使得安全网络编码存在大量编码开销；而且，对于已给的加入冗余后的信息，攻击者可以通过获得更多的独立边的信息来破坏它的安全性。本文的低开销安全网络编码的基本方法是：使用混沌序列和网络编码相结合，构造"一次一密"加密体制。

3 混沌序列

混沌序列是一种伪随机序列，是具有丰富内部层次的一种有序结构，只是没有表现出明显的周期性和对称性。

混沌序列主要有以下几种特性[15]：

(1)混沌序列的产生和接收可以受到使用者的控制。

(2)混沌在非线性映射或非线性系统中才能产生，且混沌的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非是可逆的。

(3)混沌系统对初值极度敏感。这一特性可以增加系统的抗破译能力。

通过充分了解混沌序列的以上几种特性，可以将其应用到保密通信领域作为加密的一种方法。Shannon 和国内一些学者[13]已将混沌理论应用到密码学中，而如何选取满足密码学特性要求的混沌映射是一个需要解决的关键问题。

几种主要的混沌映射有以下 3 种：Logistic 映射、改进型 Logistic 映射和 Chebyshev 映射。它们的表达式如图 1 所示。

混沌映射	表达式
Logistic 映射	$x_{n+1}=\lambda\cdot x_n(1-x_n),x_n\in(0,1)$
改进型 Logistic 映射	$x_{n+1}=1-2\cdot x_n^2,-1<x_n<1$
Chebyshev 映射	$x_{n+1}=\cos(g\cdot\arccos x_n),-1<x_n<1$

图 1 几种主要的混沌映射比较图

其中，在 Logistic 映射中，λ 为分形参数，当 $\lambda\in(3.5699,4]$ 时，系统处于混沌状态；在 Chebyshev 映射中，g 为 Chebyshev 映射阶数，当 $g>2$ 时，系统处于混沌状态。

4 低开销安全网络编码

本文的安全网络编码方案的目的是在保证达到信息论安全性的同时将编码的开销降到最小。该方案采用混沌序列，由混沌序列的性质可知，混沌序列的产生是可以受使用者控制的，即可以产生固定长度的序列；并且，给定混沌映射和初值之后可以计算得到混沌序列，然而给出的混沌序列却不可能计算出初值，这种单向性保证了生成的密文的安全性；同时，混沌序列是伪随机的，在一定的长度内不可能有重复值出现。使用混沌序列的另一个主要原因是它仅使用一个冗余便可以产生不同的随机信号。它的安全性相当于对 $\overline{m}$ 中的 $n-1$ 个信息使用 $n-1$ 个独立向量去加密。这样就构成了传统密码方案中的"一次一密"机制。

4.1 混沌序列的选取

由于本文的主要目的是构造低开销的安全网络编码方案，因此为了避免增加网络中需要传输的参数，选择了改进型 Logistic 映射来产生混沌序列。通过仿真实验论证，改进型 Logistic 映射所产生的混沌序列的初值敏感性(初值与混沌

序列之间的单向性)符合本文的要求。仿真图如图 2 所示。

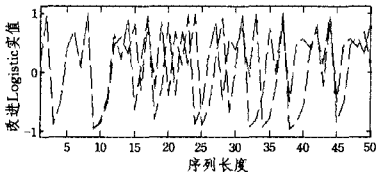

图 2　改进型 Logistic 映射混沌序列

图 2 中,蓝线代表初值为 0.1234 的混沌序列,红线代表初值为 0.1235 的混沌序列,序列长度为 1024。

数字化后,经 matlab 统计,改进型 Logistic 映射数字序列的 0/1 变化率为 50.68%。这表明改进型 Logistic 映射产生的混沌序列的初值敏感性很强,破译难度大,正适用于保密通信。改进型 Logistic 映射的这种不可逆性质正符合“一次一密”密码体制的要求。

4.2　编码方案

在单信源多信宿的组播网络 $G=(V,E)$ 中,设信源要发送 $n-1$ 个字符 $x_1,x_2,\cdots,x_{n-1}\in F_q$。令 $Y(\cdot)$ 表示混沌序列 $y_1,y_2,\cdots,y_n$,且 $y_n=1-2y_{n-1}^2$ $(-1<y_n<1)$。利用改进型 Logistic 映射所生成的混沌序列 $Y(\cdot)$ 与随机数 β 可生成一个消息向量,如式(6)所示:

$$\overline{m}=(x_1+Y(\beta),x_2+Y(x_1,\beta),x_3+Y(x_1,x_2,\beta),\cdots,x_{n-1}+Y(x_1,x_2,\cdots,x_{n-2},\beta),\beta)^{\mathrm{T}} \tag{6}$$

式中,$Y(\cdot)$ 中变量之间的逗号分隔符表示将各部分联合到一起作为一个变量,然后再将其作为混沌映射的初值输入。为简便起见,将其记为:

$$\overline{m}=(e_1,e_2,\cdots,e_{n-1},\beta)^{\mathrm{T}} \tag{7}$$

并且,$e_1,e_2,\cdots,e_{n-1}$ 服从均匀分布,且 $q>\max\{t,|\Omega|\}$。

注意到式(6)中混沌序列 $Y(\cdot)$ 的初值是各不相同的(类似于一次一密加密)。因此,即使攻击者得到了 $\overline{m}$ 中前 $n-1$ 个数据,只要随机数 β 是安全的,攻击者就不可能在多项式时间内获得关于 $x_1,x_2,\cdots,x_{n-1}$ 的任何信息。所以该方案仅用一个随机信号,就达到了隐藏信息的目的。余下的编码过程为:将 $\overline{m}$ 线性组合(线性网络编码),然后通过网络传输给各个信宿。

4.3　译码方案

本方案中的改进型 Logistic 映射对于任何一方都是公开的(包括攻击者)。信宿 T 恢复 $\overline{m}$ 的难易程度取决于基本线性网络编码的复杂性。

由于信宿 T 知道改进型 Logistic 映射,因此在恢复 $\overline{m}$ 之后,再通过运用 β,可以恢复出所有的信息。从而信宿成功译码得到原始信源消息向量。

5　安全性及可行性分析

5.1　一次一密加密体制的安全性

定理 1　“一次一密”密码体制具有完善保密性。

证明:假设:

u:信源发出的明文序列 $u=(u_1,u_2,\cdots,u_n)$;

d:信宿收到的密文序列 $d=(d_1,d_2,\cdots,d_n)$;

P_u:信源发出明文序列为 u 的概率;

r_d:信宿收到密文序列为 d 的概率;

q_k:信源用来加密明文的密钥的概率。

要证明完善保密性,就是要证明:$P_r(u|d)=P_u$　(8)

由于密钥只存在一个,并且密钥由 n 个独立随机变量组成,因此有

$$q_k=\frac{1}{2^n} \tag{9}$$

于是

$$r_d=\sum_{u\in P}\frac{P_u}{2^n} \tag{10}$$

又因为密钥的选取是独立于明文而选择的

$$P_r(u\cap d)=\frac{P_u}{2^n} \tag{11}$$

所以,$P_r(u|d)=\dfrac{P_r(u\cap d)}{r_d}=\dfrac{\frac{P_u}{2^n}}{\frac{1}{2^n}}=P_u$　(12)

则式(8)成立,所以“一次一密”加密体制的完善保密性得证。

5.2　编码算法的可行性和信息论安全性

定理 2　在单信源多信宿的组播网络 $G=(V,E)$ 中,若 $q>t$(q 为有限域的阶,t 为信宿的个数),则可在多项式时间内构造合适的线性网络编码[16],使得网络中的信源可以发送消息到多个信宿中去。

证明:设 h 表示信源和信宿之间可以传送数据包数目的最大值,即网络容量。构造随机线性网络编码时,寻找到一条由信源到信宿的路径需要用时 $O(|E|)$。为每一条边分配编码向量需要用时 $O(|T|)$,同时每一个信宿检验所分配编码向量的线性独立性花费时间为 $O(h\cdot|T|)$,则所有的信宿检验所分配编码向量的线性独立性可在 $O(|T|\cdot h^2)$ 内完成[16]。

所以,若在编码域内选择合适的编码向量来构成网络编码的全局编码核,则线性网络编码可在 $O(|E|\cdot|T|\cdot h^2)$ 内完成。证明过程与文献[14]相似,此处不再赘述。

定理 3　在单信源多信宿的组播网络 $G=(V,E)$ 中,$\Omega=\{\alpha_1,\alpha_2,\cdots,\alpha_w\}$ 为可能被窃听信道构成的集合。如第 4 节所述的编码方案,若 $e_1,e_2,\cdots,e_{n-1}$ 在 F_{q^r} 服从均匀分布,且 $q>\max\{t,|\Omega|\}$,则在此组播网络中实现安全通信,即达到信息论安全性。

证明:由文献[10]可知,当 $e_1,e_2,\cdots,e_{n-1}$ 服从均匀分布时,攻击者在窃听信道上获得的信息构成了线性无关向量组,窃听者不能得到关于 β 的任何信息,所以窃听者不可能知道混沌序列,且加密体制是“一次一密”的。由定理 1 知,本文安全网络编码方案是完善保密的。由定理 2 可知,当 $q>t$ 时,符合条件的线性网络编码是可构造的,所以本文提出的低开销安全网络编码是可实现保密通信的。

5.3　编码算法的通用性

在本文所提低开销安全网络编码中,利用一个已给定的线性网络码,在其信源处对信源信息进行一定的处理形成密文,再将生成的密文作为新的源信息在网络编码体制中传输,而后在信宿处进行相应的译码恢复出信源原始消息即可。流程图如图 3 所示。

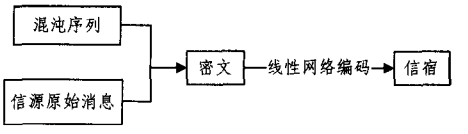

图 3　安全网络编码流程图

(下转第 163 页)

[4] Cha J C, Cheon J H. An identity-based signature from gap Diffie-Hellman groups [C] // Proceeding of LNCS. Heidelberg: Springer-Verlag, 2003: 18-30

[5] Hess F. Efficient identity based signature schemes based on pairings[C] // Proceeding of LNCS. Heidelberg: Springer-Verlag, 2003: 310-324

[6] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model[C] // Proceedings of the 11th Australasian Conferece on Information Security and Privacy. Berlin/Heidelberg: Springer-Velag, 2006: 207-222

[7] Miyazaki K, Susaki S, Iwamura M, et al. Digital documents sanitizing problem[J]. IEICE Technical Report, 2003, 103: 61-67

[8] Steinfeld R, Bull L, Zheng Y. Content extraction signatures[C] // Proceeding of Information Security and Cryptology-ICISC. Berlin: Springer-Verlag, 2001: 285-304

[9] Ateniese G, Chou D H, de Medeiros B, et al. Sanitizable signatures[C] // Proceeding of Computer Security-ESORICS. Berlin: Springer-Verlag, 2005: 159-177

[10] Lonowskim M, Lauks A. Extended sanitizable signatures[C] // Proceeding of Information Security and Cryptology-ICISC. Berlin: Springer-Verlag, 2006: 343-355

[11] Canard S, Laguillaumie F, Milhau M. Trapdoor sanitizable signatures and their application to content protection[C] // Proceedings of Applied Cryptography and Network Security. Berlin: Springer-Verlag, 2008: 258-276

[12] Brzuska C, Fischlin M, Freudenreich T, et al. Security of sanitizable signatures revisited[C] // Proceedings of Public Key Cryptography-PKC. Berlin: Springer-Verlag, 2009: 317-336

[13] Brzuskac, Fischlinm, Lehmanna, et al. Sanitizable signatures: how to partially delegate control for authenticated data[C] // Proceedings of Special Interest Group on Biometrics and Electronic Signatures. Bonn: GI, 2009: 117-128

[14] Brzuskac, Fischlinm, Lehmanna, et al. Unlinkability of sanitizable signatures[C] // Proceedings of Public-Key Cryptography-PKC. Berlin: Springer-Verlag, 2010: 444-461

[15] Ming Yang, Shen Xiao-qin, Peng Ya-mian. Identity- Based Sanitizable Signature Scheme in the Standard Model[C] // Proceedings of International Conference on Intormation Computing and Application. Berlin/Heidelberg: Springer-Verlag 2010: 9-16

[16] Waters B. Efficient identity-based encryption without random oracles [C] // Proceedings of Eurocrypt. Berlin/Heidelberg: Springer-Verlag, 2005: 114-127

[17] 李继国，姜平进. 标准模型下可证安全的基于身份的高效签名方案[J]. 计算机学报，2009(11)：2130-2136

(上接第 149 页)

由图 3 可见，在整个过程中，线性网络编码中间节点的处理过程保持不变；并且，网络编码是作用在已产生的密文上的。所以尽管产生混沌序列的初值是在实数域中进行选择，但它并未影响到进行网络编码的有限域，整个安全网络编码的有限域没有任何改变。所以，基于混沌序列的安全网络编码具有普遍通用性。

结束语 本文提出了一种基于混沌序列的低开销的安全网络编码方案，其利用混沌序列和“一次一密”加密体制的特性，结合线性随机网络编码，对原始信源消息向量进行了改变。该安全网络编码方案不需要知道网络拓扑，内部节点不需要任何新的功能且对有线和无线网络均适用。

经理论特性分析和安全性定理的证明表明，改进的安全网络编码方案在攻击者有有限计算能力和窃听能力的情况下，能够达到信息论安全的要求，有效地减小了开销，并且适用于所有线性网络编码。

参 考 文 献

[1] Ahlswede R, Cai Ning, Li S Y R, et al. Network Information Flow [J]. IEEE Transactions on Information Theory, 2000, 46 (4): 1204-1216

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

[3] Cai N, Yeung R. Secure network coding [C]// IEEE International Symposium Information Theory. 2002, 2: 323

[4] Feldman J, Malkin T, Servedio R A. On the capacity of secure network coding [C] // 42nd Annual Allerton Conf. Commun. 2004

[5] Feldman J, Malkin T, Servedio R A. Secure network coding via filtered secret sharing [C] // 42nd Annual Allerton Conf. Commun. 2004

[6] Zhang Yan, Xu Cheng-qi, Wang Feng. A novel scheme for secure network coding using one-time pad [C] // International Conference on Networks Security, Wireless Communications and Trusted Computing. vol. 1, 2009: 92-98

[7] Maximilian R, Sagduyu Y E, Honig M L, et al. Training overhead for decoding random linear network codes in wireless networks [J]. IEEE Journal on Selected Areas in Communications, 2009, 27(5): 729-737

[8] 徐光宪，付晓. 基于稀疏矩阵的低复杂度安全网络编码算法[J]. 计算机工程，2012，38(9)：55-57

[9] Adeli M, Liu Hua-ping. Secure Network Coding with Minimum Overhead Based on Hash Functions [J]. IEEE Communications Letters, 2009, 13(12): 956-958

[10] 李克荣. 基于网络编码和 Hash 函数的一个保密通信方案 [D]. 扬州：扬州大学，2010

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

[12] Bhattad K, Narayanan K R. Weakly Secure Network Coding [EB/OL]. http://netcod.org/papers/06Bhattad N-final.pdf, 2007-05-22

[13] 赵慧，卓新建，陆传赉. 一种基于网络拓扑的安全网络编码算法分析 [C]//通信理论与技术新进展—第十三届全国青少年通信学术会议. 2008: 844-846

[14] 徐光宪，付晓. 抗万能攻击的安全网络编码[J]. 计算机科学，2012，39(8)：88-91

[15] 徐光宪，吴巍. 基于伪随机序列的 Arnold 加密算法[J]. 计算机科学，2012，39(12)：79-82

[15] 李菲菲. 混沌扩频序列的研究 [D]. 葫芦岛：辽宁工程技术大学，2011

[16] Jaggi S, Sanders P, Chou P A, et al. Polynomial time algorithms for multicast network code construction [J]. IEEE Transactions on Information Theory, 2005, 51(6): 1973-1982

[17] 王汝言，楼芃雯，樊思龙，等. 容迟网络编码节点状态感知的数据转发策略[J]. 重庆邮电大学学报：自然科学版，2013，25(2)：215-220