



一种基于信誉度的航空无线电协作频谱感知方法

李玉峰, 胡乃瑞, 王宇鹏

(沈阳航空航天大学电子信息工程学院 沈阳 110136)

摘要: 传统的航空无线电协作频谱感知算法无法区分节点的性质(普通/恶意), 而新的加权序贯检测(weighted sequential probability ratio test, WSPRT)算法虽然解决了这个问题, 但在具有频谱感知数据篡改(spectrum sensing data falsification, SSDF)攻击节点的环境中, 无法保持高的感知正确率。提出了一种改进型WSPRT算法, 在传统的WSPRT算法基础上改进了信誉度奖惩方案, 增加了临近时间内感知稳定度的量化。从实验仿真结果看, 改进后的算法不仅时间复杂度更低, 而且能够有效地识别恶意节点, 对于恶意用户的判定更准确。

关键词: 认知无线电; WSPRT; 协作频谱感知; SSDF

doi: 10.11959/j.issn.1000-0801.2015145

A Cooperative Spectrum Sensing Method of Aeronautical Radio Based on Reputation

Li Yufeng, Hu Nairui, Wang Yupeng

(School of Electronics and Engineering, Shenyang Aerospace University, Shenyang 110136, China)

Abstract: The traditional cooperative spectrum sensing algorithm of aeronautical radio can't distinguish the node type (normal/malicious), though weighted sequential probability ratio test(WSPRT) method meets the requirement but when the spectrum sensing data falsification(SSDF) node is exist, it can't keep high sensing accuracy any more. An improved WSPRT was proposed. On the foundation of traditional WSPRT, reputation rewards and punishment algorithm was improved, and sensing stability factor was taken into account. The simulation results show that it can make identify malicious cognitive nodes easier and make the fusion algorithm distinguish malicious user more accurate.

Key words: cognitive radio, weighted sequential probability ratio test, cooperative spectrum sensing, spectrum sensing data falsification

收稿日期: 2014-08-30; 修回日期: 2015-06-10

基金项目: 国家自然科学基金资助项目(No.61171081), 航空科学基金资助项目(No.20122654)

Foundation Items: National Natural Science Foundation of China(No.61171081), Aviation Science Fundion of China(No.20122654)

论文引用格式: 李玉峰, 胡乃瑞, 王宇鹏. 一种基于信誉度的航空无线电协作频谱感知方法. 电信科学, 2015145

Li Y F, Hu N R, Wang Y P. A cooperative spectrum sensing method of aeronautical radio based on reputation. Telecommunications Science, 2015145



1 引言

电磁频谱管理是无线电通信的基础,是航空电子系统发挥最大效能的关键,是信息畅通的重要保证。当今世界,电磁环境日趋复杂,空中干扰逐步向多样化、宽带化、智能化发展,大部分电磁频谱都将受到严重污染;随着通信业务量、装备数量的不断增加,通信网的自扰也日益严重。传统的静态频谱管理、分配模式已经不能满足需求。如何根据电磁环境的动态变化,实时地对频谱资源进行动态管理,是当前及未来航空通信系统亟需解决的迫切问题。只有管理好频谱,实现频谱使用效率的最大化,才能为未来军用及民用航空事业的信息化建设打下坚实的基础。

认知无线电(cognitive radio, CR)技术起源于1999年,是由软件无线电(software radio, SR)奠基人——瑞典皇家理工学院 Mitola J 博士^[1]在 SR 的基础上提出的。它可以感知无线电传输的环境特征,通过无线电知识表述语言与通信网络进行智能交流,对无线环境进行分析、理解和判断,自适应地调整系统的通信参数。而认知无线电中最首要的环节就是对认知环境的频谱分布进行感知。

频谱感知的方法可以分为两种:直接频谱感知和间接频谱感知。其中,直接频谱感知技术^[2]主要有本地震荡检测(local oscillator detection, LOD)、前摄检测(proactive detection, PD)。LOD 要求获取 CR 信号的频率及相位信息;PD 是采用反馈信息的方式来检测频谱,通过发送一个特定信号观测主接收机(primary receiver, PR)的反馈效果来判断检测结果。间接频谱感知技术有匹配滤波器检测(matched filter detection, MFD)^[3]、能量检测(energy detection, ED)、循环平稳检测(cyclostationary detection, CD)^[4]、协方差系数检测(covariance based detection, CBD)^[5]、多天线路谱检测(spectrum sensing using multiple antennas, SSUMA)^[6]。MFD 的主要优势是检测速度快,在很短的检测时间内可以达到很好的检测效果,但其对信噪比(signal to noise ratio, SNR)要求比较高,随着 SNR 的下降其检测效果迅速衰减;ED 不能区分信号的种类,且受噪声的不确定性影响很大,但其最大的优势就是不需要被检测环境的先验信息;CD 的检测效果不受 SNR 影响,在 SNR 很低时其检测效果依然很好,但相对于 MFD 其计算复杂度高了很多;CBD 是针对噪声功率、信号循环频率、信号波形等先验知识完全未知的情况下提出的全盲检测算法,其在噪声功率不确定的情况下有很好的顽健性;SSUMA 可以避免阴影

效应带来的衰减及干扰,提高频谱感知效率,但当各天线之间的性能差别较大时,简单融合并非一定能够提升感知性能,因此有很多人提出了多点协作频谱感知^[7]的方法。

一般来说,协作感知方法可以分为分布式和集中式两种。分布式感知要求每个终端都具有独立处理感知信息以及可以互相交流感知信息的能力,对终端的性能要求较高;集中式感知要求终端将感知结果统一发送至融合中心,由其对数据进行融合处理并做出最终判决。协作频谱感知的最基本融合算法有“K-N”准则、“与”准则、“或”准则。然而以上方法都没有考虑节点的地理环境、距离远近等因素造成的感知可靠性差异。为了解决 CR 的感知可靠性差异问题,参考文献[8]提出了信誉度量化的方案,参考文献[9]则提出基于本地平均信噪比权值和最大似然比的估计信任度权值方案。但以上方法均假设各个感知节点都处于正常情况下。若感知节点中存在恶意节点,且节点的攻击方式^[10]不仅仅局限于“Always-1”(全1)或者“Always-0”(全0),而是 SSDF(spectrum sensing data falsification)等复杂度比较高的攻击模式时,认知网络的整体感知效果急剧下降,感知结果几乎不可信。

本文提出了一种改进型的信誉度加权量化方案,在感知信誉度评估的基础上增加了区域时间内的感知可靠性评估。这样不仅可以防止恶意 CR 节点通过累计信誉度发起攻击,而且可以在一定程度上提高系统对网络瞬时状态变化的感知灵敏度。

2 系统模型及基础融合算法

2.1 系统模型

协同频谱感知的过程可以看作一系列二元决策的表、判定及融合过程。系统主要由授权用户、认知用户、融合中心构成,整体的系统模型如图1所示。认知用户接收到由授权用户通信时产生的无线电信号 M_n , 将判决结果 S_n 发送到融合中心,经过一系列融合算法,融合中心得出最终的判决结果 S 。

每个节点的感知信息判定方法如式(1)所示。 H_0 表示 CR 没有检测到主用户正在通信, H_1 表示 CR 在感知环境中检测到了主用户正在通信。

$$\begin{cases} H_0: y(t) = n(t) \\ H_1: y(t) = h(t)s(t) + n(t) \end{cases} \quad (1)$$

其中, $y(t)$ 表示 CR 用户所感知到的信号, $h(t)$ 表示信道增益, $n(t)$ 表示加性高斯白噪声, $s(t)$ 是主发射机发出的信号,

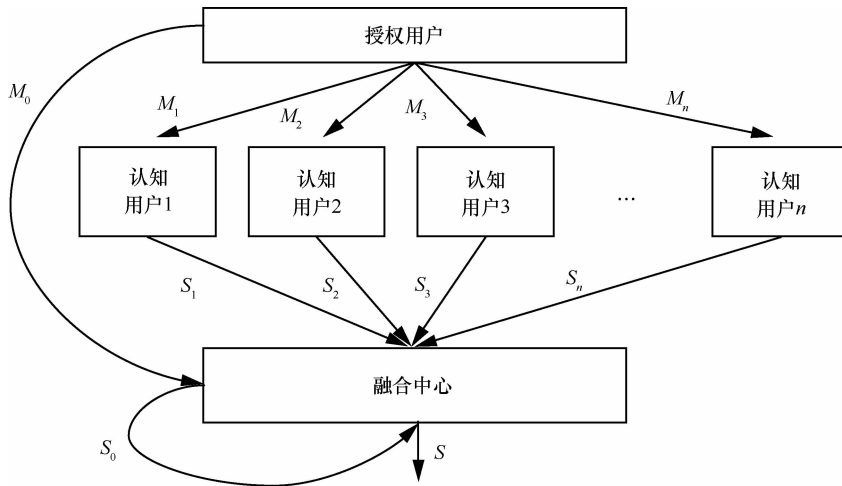


图 1 认知无线网络系统模型

而且上述参数是相互独立的。

假设各个节点之间也是相互独立的,且所处环境的 SNR 都一致,即排除了由 CR 节点与主发射机之间的距离不同而引入的 SNR 差异,使得每个正常 CR 节点的检测率(P_d)不同。

2.2 基础融合算法

融合的基本判决方法有如下 3 种。

贝叶斯检测判决方法如下:

$$\prod_{i=0}^n \frac{P[S_i|H_1]}{P[S_i|H_0]} \underset{H_0}{\overset{H_1}{>}} \frac{P_0[C_{10}-C_{00}]}{P_1[C_{01}-C_{11}]} \quad (2)$$

其中, S_i 为 CR 用户输出的感知结果(0 或 1),表示判决为 H_j 而实际为 H_k 的情况。

奈曼-皮尔逊检测判决方法如下:

$$\prod_{i=0}^n \frac{P[S_i|H_1]}{P[S_i|H_0]} \underset{H_0}{\overset{H_1}{>}} \lambda \quad (3)$$

其中, λ 是由虚警率或者检测率等参数决定的变量。

序贯检测(sequential probability ratio test, SPRT)^[11]判决方法如下:

$$S_n = \prod_{i=0}^n \frac{P[S_i|H_1]}{P[S_i|H_0]} \quad (4)$$

其中,采样数目 n 是所有协作节点个数中的任意值,检测方法采用双门限法,在给定虚警概率 P_f 和漏检概率 P_{md} 的条件下,两门限可分别表示为:

$$\begin{cases} \eta_1 = \frac{1-P_f}{P_{md}} \\ \eta_0 = \frac{P_f}{1-P_{md}} \end{cases} \quad (5)$$

其中,双门限的判决规则如下:

$$\begin{cases} S_n \geq \eta_1 \rightarrow H_1 \\ S_n \leq \eta_0 \rightarrow H_0 \\ \eta_1 \geq S_n \geq \eta_0 \rightarrow Continue \end{cases} \quad (6)$$

序贯检测相对于贝叶斯检测和奈曼-皮尔逊检测考虑了判别有效性,是一种参考样本数不确定的方法。每次数据融合不需要遍历所有 CR 用户的感知结果,从而减少了传输数据,提高了感知速度。但序贯检测的判别算法将所有节点都看作一样,没有考虑不同 CR 节点每次感知的有效性。

上述算法都未考虑恶意 CR 用户的存在,在面对恶意频谱感知攻击时,检测效果会明显降低,甚至导致整个系统瘫痪。为了应对 SSDF 攻击,有人提出了 WSPRT(weighted sequential probabty ratio test)算法^[12]。

在 WSPRT 算法中,系统会给每个 CR 用户分配信誉度值 $C_i(i=1,2,3,\dots,N)$,信誉度的更新条件按照式(7)进行:

$$\begin{cases} C_i = C_i + 1, S = C_i \\ C_i = C_i - 1, S \neq C_i \end{cases} \quad (7)$$

其中, S 表示经过融合中心判定后的协同感知结果。

假设 W_i 表示每个 CR 的感知权重,初始值为 0,常数 $-g$ 作为权重的下限, g 为上限。若 CR 的权重低于 $-g$ 就认定其为恶意节点,则 W_i 和 WSPRT 的数学表达式为:

$$W_i = fC_i = \begin{cases} 0, C_i < -g \\ \frac{C_i + g}{\max(C_i) + g}, C_i > -g \end{cases} \quad (8)$$

$$W = \prod_{i=0}^n \left(\frac{P[u_i|H_1]}{P[u_i|H_0]} \right)^{W_i} \quad (9)$$



WSPRT 算法的结果判断方法与 SPRT 一样,也就是将得到的结果 W 与预设的两个门限值 η_0 和 η_1 相比较,从而得出最终的判决结果。

3 改进的加权信誉度算法

上述算法在没有恶意 CR 用户的情况下能够很好地检测出频谱占用情况,却不能判断用户的类型(恶意/正常)。以上算法会接收任何用户的检测信息,一旦出现恶意用户,检测正确率就会急剧恶化。传统的 WSPRT 算法不能有效地区分恶意 CR 用户和判断失误的正常 CR 用户,时常会将正常 CR 用户误判为恶意 CR 用户,使得感知效率和正确率降低;而且对于 CR 节点的短时期剧烈变化反应不敏感,因此攻击用户可以通过一段时间的信誉度累计,在短时间内发起错误感知攻击,使得系统得出错误的感知结论。

WSPRT 给每个 CR 用户分配了相应的权值,每轮感知结束以后都会更新相应用户的信任权值(信誉度)。在融合计算时依据每个节点的信誉度来采纳 CR 用户的感知结果。该方法对于一些简单的攻击手段如“Always-1”和“Always-0”能有效减小和避免恶意用户造成的影响,使得在系统运行一段时间后能够区分出恶意 CR 节点,提高感知效率,降低误检率。但 WSPRT 在对于较为复杂的 SSDF 攻击时,感知正确率非常低。

本文仔细分析了传统 WSPRT 的整个流程,认为融合算法的准确度算法有待改进,而且信誉度的量化不应该只有准确度,稳定性的量化也是重要的评判依据。

传统的 WSPRT 算法只是提出了简单的对称准确度奖惩措施,如式(7),CR 节点的准确度累计和衰减速率是相同的,这样的方法不合理。奖惩措施应该是累计缓慢而衰减迅速的,这样才能有效防止 SSDF 攻击。鉴于此,本文提出了滞回型准确度统计方案,即节点的准确度衰减速率要远大于累计速率。考虑到每次感知结束后每个节点都会更新检测准确度值,计算频率高,量化算法应该简单高效,见式(10)。

$$\begin{cases} C_i = C_i + 1, S = C_i \\ C_i = C_i - 2, S \neq C_i \end{cases} \quad (10)$$

节点的累计和衰减采取了两套不同的方案,由式可知,准确度累计的速率仅为衰减速率的一半。

对一个节点的信誉度评判仅凭当前的感知准确度是不够的,节点的历史判断稳定性也从一定程度上反映了

CR 节点的感知性能。当然,不能存储节点所有的历史记录来确定其稳定性,首先算法复杂度太高,还占用存储空间。通过式(11)来判断 CR 节点某时间范围内的检测稳定性。

$$V = 2^{\sum_{i=1}^n (C_i \oplus S) - n} \quad (11)$$

其中, n 为 CR 节点所需接受检测的最近感知结果历史记录条数, n 的大小由感知环境和系统感知间隔时间来确定,其存在的形式(即队列)遵循先进先出的原则,队列长度始终保持为 n 。融合中心在每轮感知结束以后就会将当前网络状态的整体融合结果与每个节点的感知结果相比较(异或)。若比较结果相同则返回 0,不同则返回 1。再结合其 n 次历史记录,得出最终的检测稳定性结果 V 。归一化以后的结果 V 越大,表示其稳定性越好。

CR 节点的整体信誉度判断函数应该是结合准确度和稳定度得出的,结合式(9)和式(11)得出式(12)。

$$W = \prod_{i=0}^n \left(\frac{P[u_i | H_1]}{P[u_i | H_0]} \right)^{w_i \times V_i} \quad (12)$$

4 仿真与分析

假设各 CR 节点之间没有信息交换,即各个检测结果相互独立。信道衰减系数不做设定,以检测率 P_d 代替。各个节点的初始信任度为 1,即每次仿真的开始都认为所有节点的检测结果完全可信。系统设定每个节点的误警率 $P_f=0.01$,检测概率 $P_d=0.9$,最大可容忍虚警概率 $P_{fa}=0.001$,最大可容忍漏检概率 $P_{md}=0.001$,加权序贯的上下门限值分别为 $Threshold_up=999$ 、 $Threshold_down=0.001$ 。每个用户的初始权重 $cr_weight=1$ 。CR 节点的权重最高值和最低值按照仿真经验分别取 5 和 -5。CR 用户数为 50。整个仿真的方案采用蒙特卡洛仿真法,仿真次数设定为 500 次,以减小偶然因素对于仿真结果的影响。

目前的 SSDF 攻击方式最具代表性的为全 1 攻击(Always-1)、全 0 攻击(Always-0)和随机攻击。3 种方法在不同恶意用户比例下的检测正确率仿真结果如图 2 所示。

由图 2 可以看出不同恶意用户比例下 3 种攻击手段给系统检测率造成的影响。其中 Always-1 攻击模式随着恶意用户比例上升,系统检测性能衰减增大。该攻击模式有助于观察不同融合算法下系统的检测性能,因此以下仿真都基于 Always-1 攻击模式进行。

图 3 反映了在 Always-1 攻击下的“与”算法、传统 WSPRT 融合算法和本文改进算法下,恶意用户比例不同

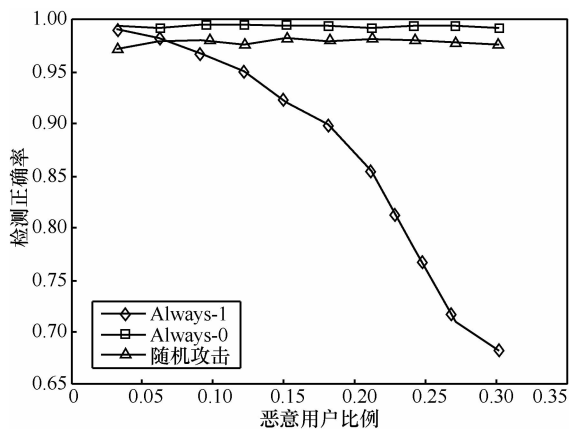


图2 不同恶意用户比例下检测率对比

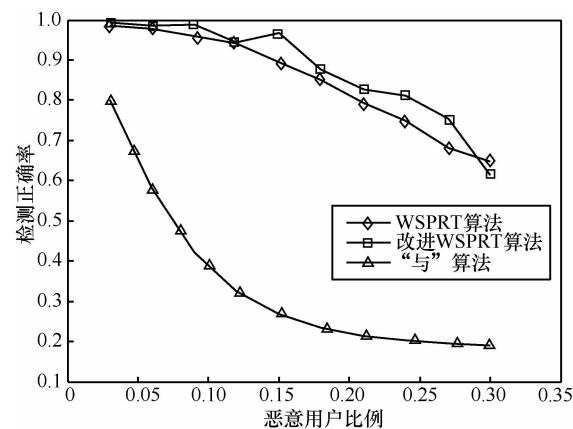


图3 不同恶意用户比例下 WSPRT 算法与改进算法对比

时的系统检测性能。在实际网络中正常用户占大多数,所以恶意用户比例选择 0~0.3。检测正确率反映了系统的检测性能,正确率越高,说明其检测效果越好。由图 3 可以看出,改进算法在检测性能上较传统 WSPRT 算法有所提升。

图 4 反映了在 Always-1 攻击下的“与”算法、传统 WSPRT 融合算法和本文改进算法下,同一恶意用户比例时

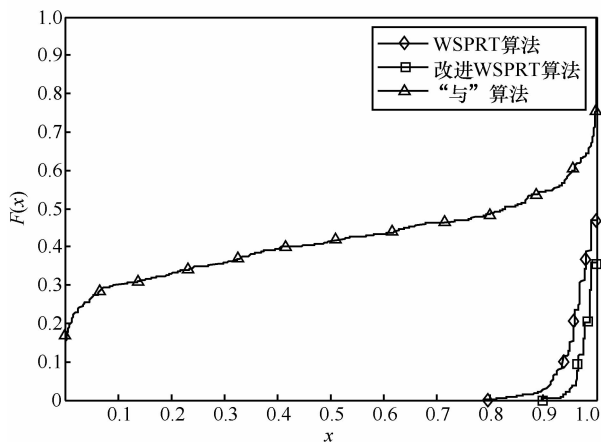


图4 同一恶意用户比例下 3 种算法检测率累计分布

的检测成功率的累计分布。这里的恶意用户比例为 0.2,每次蒙特卡洛感知实验中有 100 次连续的感知融合周期。由图 4 可以看出,改进算法的稳定性明显优于传统 WSPRT 算法,而且感知正确率更为集中地分布在大于 0.9 的区间内。

对 3 种算法在同一恶意用户比例下的时间复杂度进行分析,3 种算法的运行时间见表 1。

表 1 3 种算法的运行时间

算法种类	运行时间/s
“与”算法	0.005 71
WSPRT 算法	2.328 77
本文改进算法	1.217 49

表 1 反映了 3 种算法中,“与”算法的时间复杂度最低,但其感知正确率较低;改进算法的时间复杂度明显低于传统 WSPRT 算法。

5 结束语

本文提出了一种基于 WSPRT 的改进型协作频谱感知融合算法。在原有的基础上改进了信任度的奖惩措施,增加了临近时间内感知稳定度的量化。从实验仿真结果看,改进后的算法不仅时间复杂度更低,而且能够有效地识别恶意节点,在感知准确度和感知稳定性上都有一定的提升,对于 SSDF 攻击的顽健性也得到进一步增强。

参考文献

- 1 Mitola J, Maguire G J. Cognitive radio making software radios more personal. *Personal Communications, IEEE*, 1999, 6(4): 13~18
- 2 Liang Y, Chen K, Li G Y, *et al.* Cognitive radio networking and communications: an overview. *IEEE Transactions on Vehicular Technology*, 2011, 60(7): 3386~3407
- 3 Yang P, Xiao Y, Li L, *et al.* An improved matched-filter based detection algorithm for space-time shift keying systems. *Signal Processing Letters, IEEE*, 2012, 19(5): 271~274
- 4 Arezumand H, Azmi P, Sadeghi H. Cooperative spectrum sensing based on a low-complexity cyclostationary detection method for cognitive radio networks. *Proceedings of Computer and Knowledge Engineering (ICCKE)*, Mashhad, Iran, 2011: 308~313
- 5 Ping Y, Li Y M, Heung-Gyoon R. On the performance of covariance based spectrum sensing for cognitive radio. *IEEE Transactions on Signal Processing*, 2012, 60(7): 3670~3682
- 6 Saeid S, Abbas T, Josep S. Spectrum sensing using correlated receiving multiple antennas in cognitive radios. *IEEE Transactions on Wireless Communications*, 2013, 12(11): 5754~5766

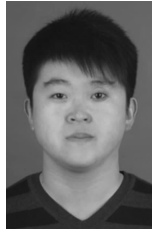


- 7 Zhao J H, Li F, Yang T. Weight sequential log-likelihood ratio detect algorithm with malicious users removing. *Journal of China Universities of Posts and Telecommunications*, 2013(2): 60~65
- 8 Quan Z, Cui S, Sayed A H. An optimal strategy for cooperative spectrum sensing in cognitive radio networks. *Proceedings of 50th Annual IEEE Global Telecommunications Conference (GLOBECOM 2007)*, New Orleans, LA, 2007: 2947~2951
- 9 Visser F E, Janssen G M, Paweczak P. Multinode spectrum sensing based on energy detection for dynamic spectrum access. *Proceedings of Vehicular Technology Conference(VTC Spring)*, Marina Bay, Singapore, 2008: 1394~1398
- 10 裴庆祺,李红宁,赵弘洋等.认知无线电网络安全综述.通信学报, 2013, 34(1):144~158
Pei Q Q, Li H N, Zhao H Y, *et al.* Security in cognitive radio networks. *Journal on Communications*, 2013, 34(1):144~158
- 11 Ming Z, Shen J F, Chen H F, *et al.* A cooperative spectrum sensing scheme based on the Bayesian reputation model in cognitive radio networks. *Proceedings of Wireless Communications and Networking Conference*, Paris, France, 2013: 614~619
- 12 Zhang L, Wu Q, Ding G, *et al.* Performance analysis of probabilistic soft SSDF attack in cooperative spectrum sensing. *Eurasip Journal on Advances in Signal Processing*, 2014 (1): 81~89

[作者简介]



李玉峰,男,博士,沈阳航空航天大学电子信息工程学院教授,主要研究方向为无线通信、图像处理与传输。



胡乃瑞,男,沈阳航空航天大学电子信息工程学院助理工程师,主要研究方向为无线通信理论及应用。



王宇鹏,男,博士,沈阳航空航天大学电子信息工程学院副教授,主要研究方向为无线通信理论及应用。