

一种新型混沌扩频卫星隐蔽通信算法

廉晨 达新宇 张亚普

(空军工程大学信息与导航学院 西安 710077)

摘要 针对 Logistic 及改进型混沌映射只存在唯一满映射点的缺陷,设计了一种新型混沌映射函数,拓宽了满映射参数的取值范围,进而提高了混沌序列遍历性,并基于相干混沌移位键控技术,构建了新型混沌扩频卫星隐蔽通信系统。分别对新型混沌序列的随机性、相关性和平衡性,以及隐蔽通信系统的误码率进行了仿真分析,结果表明:新型混沌映射比已有映射遍历性更好,平衡性更高。原业务信号与扩频调制信号的功率比值大于 20dB 时,原业务接收机接收误码率基本不受影响。扩频因子为 80、信道信噪比大于 6dB 时,隐蔽接收机误码率小于 10^{-3} ,能满足一定的隐蔽通信要求。

关键词 卫星隐蔽通信,混沌,扩频

中图法分类号 TN914.42, TN927+.2 **文献标识码** A

Novel Algorithm of Satellite Covert Communication Based on Chaotic Spread Spectrum Modulation

LIAN Chen DA Xin-yu ZHANG Ya-pu

(School of Information and Navigation, Air Force Engineer University, Xi'an 710077, China)

Abstract In view of the fact that traditional Logistic-Map as well as the modified Logistic-Map only have one surjective parameter, a new chaotic map function was designed, which broadens the range of surjective parameter so as to improve the ergodic property of the chaotic sequence. Based on the coherent chaos shift-keying modulation, a new satellite covert communication system with chaotic spread spectrum was installed. The randomness correlation balance property of the referred chaotic sequence and the error rate of the covert communication system were analyzed. The simulation results show that the referred chaotic is better than the traditional Logistic chaotic in ergodic property and balance property. The bit error rate of original service receiver is not changed when the power ratio of original service signal to spread spectrum modulated signal is greater than 20dB. The bit error rate of covert communication receiver is below 10^{-3} when the spread spectrum factor is 80 and the SNR (Signal to Noise Ratio) is greater than 6dB. The proposed system can meet the covert communication requirements.

Keywords Satellite covert communication, Chaotic, Spread spectrum

卫星通信具有覆盖范围广、数据容量大、传输速率快等优点,可用于多种复杂通信环境。然而由于卫星信道的开放性,通信信息极易泄漏,通信隐蔽性较差。随着信息战的不断发展升级,窃密与反窃密技术的研究备受关注,因此,如何增强卫星通信的隐蔽性能,进而提高通信的保密性^[1-3]逐渐成为各国研究的热点。

传统的隐蔽信号采用 PN 序列作为扩频和解扩序列,然而,PN 序列码过于集中,地址码个数有限,这严重影响了系统的抗截获性^[4]。混沌序列对方程参数和初始值极其敏感^[5,6],不仅具有高斯统计特征和遍历性,而且具有长期不可预测性^[7,8]。基于混沌序列的上述特性,文献[9]率先采用混沌序列对隐蔽信号进行解、扩频,从而为隐蔽通信技术的研究开辟了新途径。文献[10]在 Logistic 映射基础上提出了一种改进型 Logistic 映射,其可以更早地进入混沌状态,并且具有更加理想的相关特性。然而,这种改进型 Logistic 映射生成

的混沌序列平衡性不高,且由于映射仅有唯一的满映射点,制约了混沌序列的可用性。为此,提出一种新型混沌映射,它增大了满映射的参数范围,提高了映射产生序列的遍历性,且具有较高的平衡性。

首先,从理论上介绍了 Logistic 混沌映射和改进型 Logistic 混沌映射,根据两种映射的遍历性和随机性不理想的问题,提出了一种新型混沌映射;然后,对扩频隐蔽通信系统进行建模,将新型混沌映射生成的扩频码应用于隐蔽通信;最后,通过仿真实验,分析了改进型 Logistic 映射、新型混沌映射及扩频隐蔽通信系统的性能。仿真结果表明,新型混沌映射具有更好的随机性及平衡性,适用于扩频隐蔽通信系统。

1 理论部分

1.1 Logistic 映射及其改进

Logistic 映射的定义为:

本文受国家自然科学基金(61271550)资助。

廉晨(1992—),女,硕士生,主要研究方向为卫星通信、信号处理, E-mail: sycles@163.com; 达新宇(1961—),男,教授,主要研究方向为信息与通信工程; 张亚普(1985—),男,博士生,主要研究方向为电磁脉冲防护。

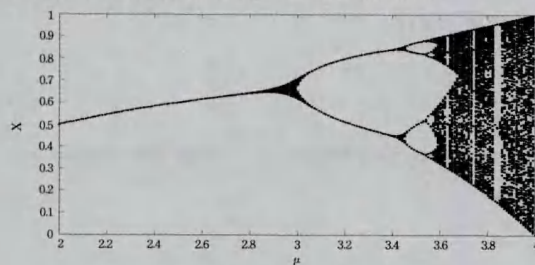
$$x_{n+1} = f(x_n) = \mu x_n (1 - x_n) \quad (1)$$

其中, 初始值 $x_0 \in (0, 1)$, 映射参数 $\mu \in (0, 4)$, 当 $\mu \in (3.57, 4)$ 时, 系统工作于混沌状态。文献[10]提出了一种改进型 Logistic 映射, 这种映射序列的均值为零, 且相关特性更加理想, 其定义为:

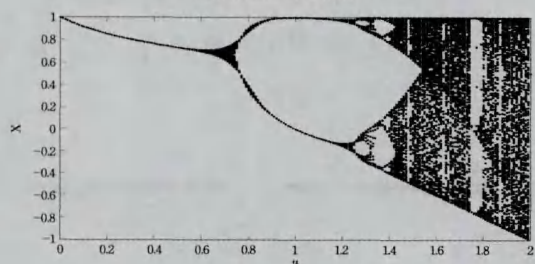
$$x_{n+1} = f(x_n) = 1 - \mu x_n^2 \quad (2)$$

其中, 初始值 $x_0 \in (-1, 1)$, 映射参数 $\mu \in (0, 2)$, 与 Logistic 映射一样, μ 的变化决定系统的状态。

Logistic 映射和改进型 Logistic 映射的分岔图如图 1 所示, 由图中可以看出映射状态与参数 μ 的关系。



(a) Logistic 混沌映射



(b) 改进型 Logistic 混沌映射

图 1 分岔图

从图 1 可以看出, Logistic 映射只有在 $\mu=4$ 时, 迭代结果才会映射到整个区间, 这称为满映射状态。改进型 Logistic 映射也只有 $\mu=2$ 时才为满映射状态, 这就导致在很大的参数范围内, 序列迭代结果范围小, 分布可能产生集中, 影响了映射生成序列的随机性。

1.2 新型混沌映射设计

针对两种 Logistic 映射只在一个参数点为满映射的缺陷, 提出一种新型混沌映射, 使其在一定参数区间内都为满映射。

新型混沌映射的定义为:

$$x_{n+1} = \frac{k^2}{2} x_n^2 + (k^2 - 2k) x_n + \frac{k^2}{2} - 2k + 1 \quad (3)$$

其中, 初始值 $x_0 \in (-1, 1)$, 映射状态与映射参数 k 的关系如图 2 所示。

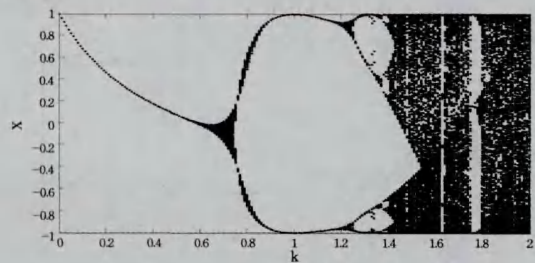


图 2 新混沌映射分岔图

从图 2 可以看出, 新型混沌映射在很大参数范围 $k \in$

(1.53, 2) 内都为满映射状态。这就说明这种新算法比现有算法的遍历性更好, 更适合应用在保密通信等领域。

1.3 实值混沌序列数字化

用于扩频的混沌序列有两种常用形式: 实值序列和数字序列。实值序列就是把混沌映射的轨迹 $x_k: k=0, 1, 2, \dots$ 直接作为扩频序列。其元素是 $(-1, 1)$ 区间上的模拟量, 不便于使用数字手段传输, 所以, 通常将实值序列进行数字化, 使之便于数字传输。

将实值序列数字化的方法有两种: 二值量化法和多比特量化法^[11]。二值量化法就是对每个实值序列元素 x_k 进行 1、0 量化, 或根据需要进行 1、-1 量化, 得到序列 $\tilde{x}_k: k=0, 1, 2, \dots$ 。多比特量化法则是对于每一个实值序列元素 x_k 进行 L 位的 0、1 量化, 对每个 x_k , 可以得到 L 个序列元素 $\tilde{x}_{ki}$, 其中 $x_k = \sum_{i=1}^L \tilde{x}_{ki} 2^{-i}$ 。

对于新型混沌映射生成序列, 采用二值量化法进行 1、-1 量化。混沌序列均值为 0, 二值量化规则为:

$$\begin{cases} \tilde{x}_k = 1, & x_k \geq 0 \\ \tilde{x}_k = -1, & x_k < 0 \end{cases} \quad (4)$$

1.4 扩频隐蔽通信系统原理

基于相干混沌移位键控 (CSK) 的卫星隐蔽通信, 是使用混沌序列将要发送的隐蔽信号进行扩频调制, 调制后的信号与卫星原业务信号进行重叠, 重叠的原则是不明显影响原业务信号的通信, 而且要保证发送的隐蔽信号能够进行通信。

卫星隐蔽通信的原理框图如图 3 所示。假设卫星信道中传输的原业务信号为 BPSK 信号, 隐蔽信号和扩频使用的混沌序列为双极性二进制信号, 将上行链路、下行链路及转发器的噪声等效为加性高斯白噪声。

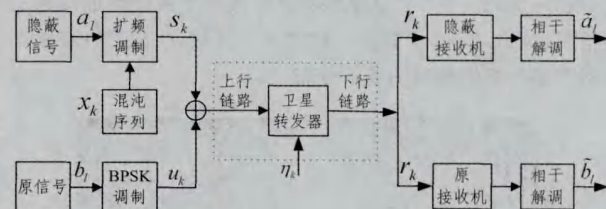


图 3 卫星隐蔽通信原理框图

如图 3 所示, 隐蔽信号 a_l 经过混沌序列 x_k 扩频调制后生成扩频调制信号 s_k , 与原业务信号 u_k 叠加, 经过上行链路、卫星转发器和下行链路, 加上等效高斯白噪声 η_k , 被原业务通信地面站的接收机和隐蔽通信接收机同时接收。接收到的信号 r_k 由扩频调制信号 s_k 、原业务信号 u_k 和等效加性高斯白噪声 η_k 3 部分组成。隐蔽通信接收机对接收到的信号进行相干解调, 得到隐蔽信号 $\tilde{a}_l$ 。

隐蔽通信发射机中的混沌信号产生器根据混沌映射和初始值生成混沌序列 $\{x_k\}, k=1, 2, \dots$ 。设隐蔽信号 $a_l \in \{-1, 1\}$ 是第 l 个被传送的比特信号, “-1”和“+1”等概率出现, 相干 CSK 系统的扩频因子为 β (一个符号内混沌样本的数目)。则在第 l 个比特信号内, 发送端的输出为 $s_k = a_l x_k, k=(l-1)\beta + 1, (l-1)\beta + 2, \dots, l\beta$ 。即隐蔽信号为“1”时, 发送端输出混沌样本信号 x_k ; 隐蔽信号为“-1”时, 发送端输出反相混沌样本信号 $-x_k$ 。

原业务信号发射机中, 用 $b_l \in \{-1, 1\}$ 表示第 l 个被传送的比特信号, 信号功率为 P_B , 这样在第 l 个符号内, 信号表示

为 $u_k = \sqrt{P_B} b_l$ 。隐蔽通信系统和原业务系统的接收信号可以表示为:

$$r_k = u_k + s_k + \eta_k \quad (5)$$

其中, η_k 表示均值为 0、功率谱密度为 $\frac{N_0}{2}$ 的等效高斯白噪声。

在隐蔽通信接收端,采用基于同步恢复的相干解调, y_l 表示接收到第 l 个比特信号时相关器的输出信号,相关器的输出为:

$$\begin{aligned} y_l &= \sum_{k=\beta(l-1)+1}^{\beta l} r_k x_k \\ &= a_l \sum_{k=\beta(l-1)+1}^{\beta l} x_k^2 + b_l \sqrt{P_B} \sum_{k=\beta(l-1)+1}^{\beta l} x_k + \sum_{k=\beta(l-1)+1}^{\beta l} x_k \eta_k \end{aligned} \quad (6)$$

相关器的输出 y_l 通过门限检测器(阈值为 0)进行判决,就可以恢复出原发送的隐蔽信号。而原业务信号接收机没有同步恢复的混沌序列,就无法解调出隐蔽信号,以此达到隐蔽通信的目的。

2 仿真分析

2.1 新型混沌映射随机性对比分析

改进型 Logistic 映射只有在 $\mu=2$ 时才为满映射状态,取 $\mu=2$ 和 $\mu=1.8$ 检验改进型 Logistic 映射生成序列的分布情况,样本点 N 取 3000。如图 4 所示, $\mu=2$ 时,映射的生成序列在其所对应的取值范围内可看作是近似均匀的随机分布, $\mu=1.8$ 时,生成序列已经不再是均匀的随机分布,而是形成一个带状区域。这就证明了现有算法在 $\mu \neq 2$ 时迭代结果分布集中,不利于保密通信。

新型混沌映射在参数范围 $k \in (1.53, 2)$ 内都为满映射状态,取 $k=2$ 和 $k=1.7$ 检验新型混沌映射生成序列的分布情况, N 取 3000,得到图 5 的结果。显然,生成序列在两个参数下都为近似均匀的随机分布。

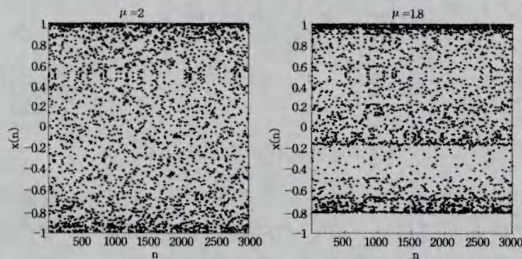


图 4 改进型 Logistic 映射的生成序列分布

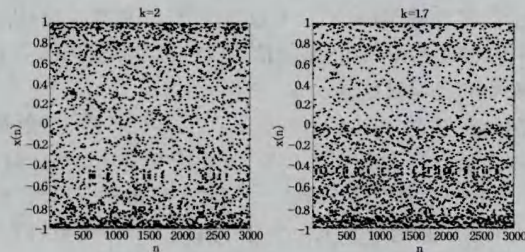


图 5 新型混沌映射的生成序列分布

2.2 截短数字混沌序列相关性分析

理论上,在计算数值精度无限的情况下,混沌序列具有理想的非周期性;实际中,计算精度越高,混沌序列的周期会越长,计算精度较高、周期较长时,混沌序列可以近似看作非周

期序列。扩频通信中多采用有限长序列,因此使用混沌序列时,需要按照需求将混沌序列截短,作为扩频序列使用。

用不同的初始值迭代出不同的混沌序列,对每个混沌序列按顺序截取成段,来研究序列的相关性。

取初值分别为 $x_{01}=0.2$ 和 $x_{02}=0.25$,改进型 Logistic 映射参数为 $\mu=2$,新型混沌映射参数为 $k=2$,序列长度 $N=1000$,考察二值量化序列的自相关和互相关特性。图 6 为改进型 Logistic 映射序列和新型混沌映射序列的自相关特性,由图知二者都是较为理想的 δ 函数;图 7 为两种映射序列的互相关特性,两种序列的互相关性都接近 0,即这两种映射具有很好的相关性。

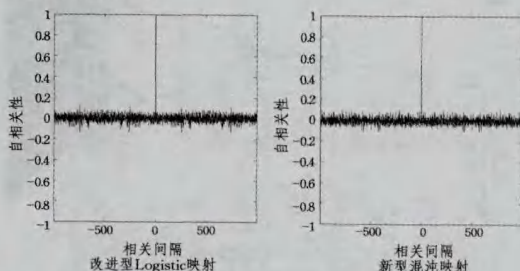


图 6 两种映射的自相关特性

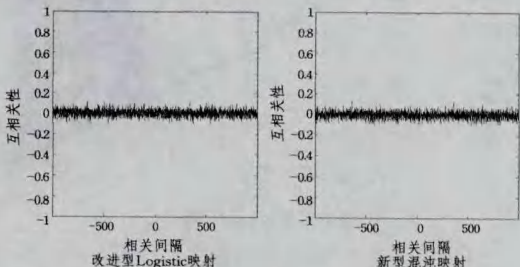


图 7 两种映射的互相关特性

2.3 新型混沌序列平衡性对比分析

扩频通信系统中,载波抑制度与扩频序列的平衡性有着密切关系,不平衡的序列会导致系统载波泄露增大,出现误码甚至信息丢失,所以混沌扩频序列的平衡性对扩频通信系统有非常重要的意义^[12]。用 P 和 Q 分别表示混沌扩频序列中 1 和 -1 的个数, K 表示序列元素总数,则序列的平衡度可以表示为:

$$E = |P - Q| / K \quad (7)$$

将新型混沌扩频序列的平衡度与改进型 Logistic 混沌扩频序列的平衡度进行比较,结果如图 8 所示。图中用实线表示新型混沌扩频序列的平衡度,虚线表示改进型 Logistic 混沌扩频序列的平衡度。可以看出,新型混沌扩频序列的平衡性明显优于现有的改进型 Logistic 混沌扩频序列的平衡性。

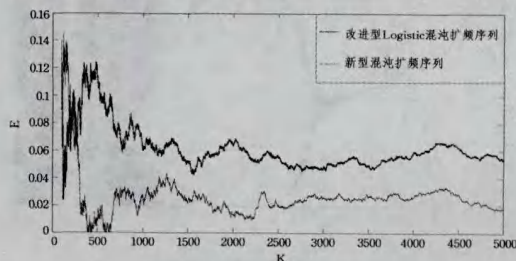


图 8 平衡性比较

2.4 扩频隐蔽通信系统误码率分析

卫星隐蔽通信系统的性能以隐蔽性能和抗干扰性能来衡量。隐蔽性能以原卫星业务系统在扩频调制信号干扰下接收端误码率的变化为衡量指标;抗干扰性能以隐蔽通信接收端的误码率作为衡量指标。

为了验证基于混沌移位键控的卫星隐蔽通信系统的性能,对系统的隐蔽性能和抗干扰性能进行仿真。

图9所示为原业务信号功率与扩频调制信号功率比分别为0dB, 5dB, 10dB和20dB时原业务接收机误码率随信噪比的变化曲线,以及原业务信号在无扩频调制信号干扰下误码率的理论值和实际值曲线。由图中可以看出,当原业务信号功率与扩频调制信号功率比值较大时,原业务接收机解调后的误码率与没有扩频调制信号影响时基本一致,根据实际情况尽量减小隐蔽信号功率,就可以满足隐蔽性。

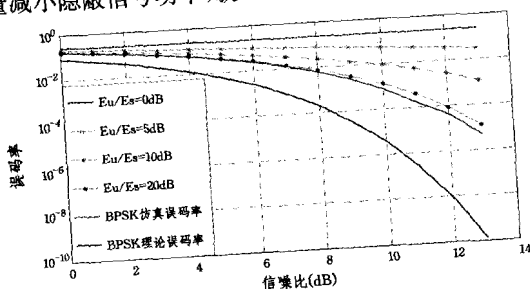


图9 原业务接收机误码率

图10所示为隐蔽信号接收机在扩频因子分别为20, 50, 80, 100时,误码率随信噪比的变化曲线,其中原业务信号功率与扩频调制信号功率比值为20dB。由图可见,虽然扩频调制信号功率较小,但当扩频因子足够大时,仍然可以正确解调出隐蔽信号,扩频因子为80、信道信噪比大于6dB时,隐蔽接收机误码率小于 10^{-3} ,系统可以满足一定的抗干扰要求。也可以看出,扩频因子达到一定值时,再增加扩频因子对误码率的影响并不明显,在实际应用中应根据情况选择合适的扩频因子。

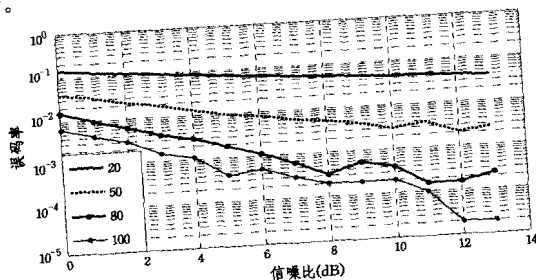


图10 隐蔽接收机误码率

结束语 Logistic及改进型Logistic混沌映射只存在唯一满映射点,致使混沌映射生成序列遍历性差和平衡性低。针对上述缺陷,设计了一种新型混沌映射函数,拓宽了满映射参数的取值范围,进而提高了混沌序列遍历性。基于相干混沌移位键控技术,采用新型混沌映射构建了混沌扩频卫星隐蔽通信系统,增加了可用地址码的数量,改善了伪随机码扩频的卫星隐蔽信号易被截获的情况,有助于提高通信的保密性。

分别对新型混沌序列的随机性、相关性和平衡性,以及隐蔽通信系统的误码率进行了仿真分析,结果表明:新型混沌映射比已有映射遍历性更好,平衡性更高。原业务信号与扩频调制信号功率比值为20dB时,原业务接收机接收误码率基本不受影响。扩频因子为80、信道信噪比大于6dB时,隐蔽接收机误码率小于 10^{-3} ,能满足一定的隐蔽通信要求,从而证明了该算法的有效性。

参考文献

- [1] 郑世慧,张国艳,杨义先,等. 基于混沌的带密钥散列函数安全分析[J]. 通信学报, 2011, 32(5): 146-152
- [2] 周庆,胡月,廖晓峰. 一种基于TD-ERCS的性特征密钥产生算法[J]. 物理学报, 2009, 58(7)
- [3] 李家标,曾以成,陈仕必,等. 改进型Henon映射生成混沌伪随机序列及性能分析[J]. 物理学报, 2011, 60(6)
- [4] 邱劲,王平,肖迪. 基于混沌映射的伪随机序列发生器[J]. 计算机科学, 2011, 38(10): 81-83
- [5] Mazzini G, Setti G, Rovatti R. Chaotic complex spreading sequences for asynchronous DS-CDMA Part2: Some theoretical performance bounds [J]. IEEE Transactions on Circuits and Systems Part1, 1998, 45(4): 496-506
- [6] 杨吉云,廖晓峰,肖迪,等. 对一种基于Logistic映射的分组加密机制的分析和改进[J]. 通信学报, 2008, 29(12): 86-90
- [7] Gu Jun-rong, Wang J H, Han Ning, et al. Analysis of an interleaved chaotic spread spectrum sequence [C] // International Conference on Wireless Communications Networking and Mobile Computing, 2008
- [8] 易称福. 混沌扩频序列设计及其在扩频通信中的应用研究[D]. 赣州: 江西理工大学, 2007
- [9] 廖旋煥,高金峰. 广义映射混沌扩频序列及其特性分析[J]. 电子与信息学报, 2006, 28(7): 1255-1257
- [10] 王亥,胡健栋. 改进型Logistic-Map混沌扩频序列[J]. 通信学报, 1997, 8(8): 71-77
- [11] 柳平,闫川,黄显高. 改进的基于Logistic映射混沌扩频序列的产生方法[J]. 通信学报, 2007, 28(2): 134-140
- [12] 任义龙,刘渊. 一种基于Holder指数的DDoS攻击检测方法[J]. 计算机应用研究, 2011, 28(2): 724-727

(上接第157页)

- [5] Stefanov A, Stojanovic M. Design and Performance Analysis of Underwater Acoustic Networks[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(10)
- [6] Dhillon S S, Chakrabarty K. Sensor placement for effective coverage and surveillance in distributed sensor networks [J]. Wireless Communications and Networking, IEEE, 2003, 3(3): 1609-1614
- [7] 蔺智挺,屈玉贵,翟羽佳,等. 一种高效覆盖的节点放置算法[J].

- 中国科学技术大学学报, 2005, 35(3)
- [8] Cortes J, et al. Coverage control for mobile sensing networks [J]. IEEE Transactions on Robotics and Automation, 2004, 20(2): 243-255
- [9] 吴小平,冯正平. 多AUV覆盖控制研究[J]. 中国造船, 2009, 50(2)
- [10] Nguyen B, Hopkin D, Yip H. Autonomous underwater vehicles a transformation of mine counter-measure operations[J]. Def. Secur. Anal., 2008, 24(3): 247-266