文章编号：1002-2082(2010)03-0423-04

关于OCDMA系统安全性的研究

李传起[1,2]，乙万义[1]，周园园[1]，张 媛[1]
（1. 南京信息工程大学 数理学院，江苏 南京 210044；2. 广西师范大学 电子工程学院，广西 桂林 541004）

摘 要：简要介绍了OCDMA系统的原理，分析了码型和码容量、地址序列的扩频作用对OCDMA安全性的影响，结合完全无差错探测几率给出完全探测到正确地址码所需探测次数的期望值，并以此重点分析了码字探测对OCDMA安全性的影响，比较分析了OCDMA技术与现代光纤保密通信技术的关系，给出了增加OCDMA系统安全性而采取的一些措施。

关键词：光通信；OCDMA；地址码；光纤保密通信；通信系统安全；扩频
中图分类号：TN918 **文献标志码**：A

Research on security of optical CDMA system

LI Chuan-qi[1,2], YI Wan-yi[1], ZHOU Yuan-yuan[1], ZHANG Yuan[1]
(1. College of Mathematics and Physics, Nanjing University of Information Science & Technology, Nanjing 210044, China; 2. College of Electronics Engineering, Guangxi Normal University, Guilin 541004, China)

Abstract: The OCDMA system is briefly introduced. The code pattern and code capacity, the role of sequence spread spectrum to the security of OCDMA are analyzed, the expectations of the frequency of the correct address code detection is given with complete error-free detection probability and the address code detection to the security of OCDMA is analyzed. The relationship between OCDMA technology and modern fiber-optic secure communication technology is compared. Some measures to increase security of the OCDMA system are put forward.

Key words: optical communication; optical code-division multiple access; address code; fiber-optic secure communication; communication system security; spread spectrum

引言

通信的安全是评价通信系统的一个重要指标，随着窃听技术的不断发展，用户对通信的安全性提出了更高的要求。对于基于光纤光栅保密通信技术的OCDMA系统作为未来高速全光局域网解决方案之一，并与OTDM及OWDM共同构成三大光纤信道复用技术，而其相对OTDM与OWDM有着明显的安全优势[1]，但OCDMA系统存在安全问题[2-3]，文献[4-6]提出了侦听器的模型且得到较好的仿真实验结果。现有关于OCDMA系统安全性分析的文章不够详细，本文将对影响OCDMA系统安全性的相关各因素做全面具体的分析，并提出增加OCDMA系统安全的措施。

1 OCDMA系统原理

图1是典型的OCDMA系统[7]，OCDMA系统对不同的用户分配不同的、具有良好相关特性的地址码，在发送端根据地址码构成的OCDMA编码

收稿日期：2009-11-05； **修回日期**：2009-12-29
基金项目：江苏省自然科学基金(BK2008437)；江苏省高校自然科学基金(07KJB510066)
作者简介：李传起(1964—)，男，安徽六安人，工学博士，教授，博导，主要从事物理学及光通信技术领域的科研和教学工作。
论文联系人：乙万义 E-mail：yiwanyi2007@yahoo.com.cn

器对信息进行编码。各用户的编码信号经星形耦合器叠加在一起,形成一个总的信号矢量进入光纤传输[7]。在接收端,光信号进入多个OCDMA 解码器,光解码器用匹配的地址码做相关运算,结果送入光电探测器,再经阈值判决及处理,最后恢复各自的原始信号,从而实现多址复用通信。

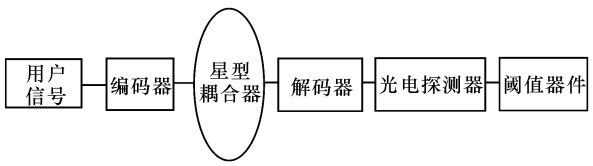

图1 典型的OCDMA 系统结构原理图

Fig. 1 Typical schematic diagram of OCDMA system

2 码型和码字容量对安全性的影响

在OCDMA 系统中,用户接受信息是用已确定的地址序列与已编码处理的信号进行相关的判决及处理,最后将用户信息从共享信道提取出来。对于不知道地址码的窃听者来说进行正确的解调是困难的,尤其在同步的多用户系统中。对于码字容量较大的系统,窃听者平均要搜索地址码的一半才可以得到用户的数据信息,所以衡量系统的安全性首先考虑的是码字的容量,而一维码系统码字容量较小,不能有效地抵挡窃听者的强行地址码盲目搜索法,而二维地址码系统码字的容量大大提高,较之一维码能较好地抵挡窃听者的强行搜索,所以在其他因素相同的情况下,二维码系统比一维码系统安全。另一方面,码型的选择决定了码字容量的大小,表1 给出了两类典型码字的码型与码容量的比较。

表1 典型码的码字容量比较

Table 1 Comparison of capacity of typical codeword

码字类型	典型代表	参数	码字容量(数量级)
一维地址码	OOC,PC,EQC	10000(码长)	约10^2
二维地址码	OOC/PC	10000(码长)/30(波片)	约10^5

总之,在其他因素相同的情形下,可以说码字容量越大系统安全性越高。

3 地址码序列的扩频作用对OCDMA 系统安全性的影响

OCDMA 系统是通过地址序列对未经编码的用户信号进行扩频处理的,以此来大幅度地增加带宽而降低信噪比,甚至能使有用信号的功率远在低于背景噪声的功率下传输,其中带来的扩频增益记为G_p,则$G_p=W/\Delta F$(W 是经编码处理后的用户信号的带宽,ΔF 是未经处理的用户信号带宽)。增益值对通信系统安全性分析提供了一个参数。从上可知地址序列扩频增加了OCDMA 系统的安全性。

OCDMA 系统是通过给不同的用户分配一个不同的、较长的且正交的地址码来区分用户,系统用户使用匹配的地址序列解扩时,就能使得其他用户信息变成了噪声。其中系统中这种正交性的地址码的优良相关性,以及较长编码位数的伪随机码为系统带来的扩频增益,都为系统提高了安全性,同时这个较长编码位数的伪随机码也为窃听者制造了困难,但这个伪随机码并不是真正的随机编码,既有密钥熵不是无限大的,同时明文的冗余度为零不现实的,OCDMA 系统传输信息的编码的冗余度是不能完全消除的,因此窃听是可能的,这也就说明了OCDM 系统的安全性是相对的,仅是在破译技术上增加了难度而已。

4 码字探测对OCDMA 系统安全性的影响

当系统码字容量较小时,采用强行的地址码盲目搜索效率较高,但是当系统码字容量较大时,采用强行的地址码盲目搜索效率较低。窃听者换之采用码字拦截的方法,假设拦截的是$\lambda-t$ 二维码系统。由完全无差错探测到地址码所需要的时间的长短来衡量OCDMA 系统安全性。完全无差错探测到地址码所需要的时间表示为

$$t_s=Dt_d \tag{1}$$

式中:D 为完全探测到正确地址码平均需要探测的次数;t_d 为探测一次的耗时(不妨设t_d 为单位"1",这样的完全无差错探测到地址码所需要的时间与完全探测到正确地址码平均需要探测的次数在量上是相等的,即$t_s=D$);t_s 为完全探测到地址码所需要的总的时间。D 即是所需要探测的次数的期望值,故可表示为如下形式:

$$\begin{aligned}D=&1*p_c+2(1-p_c)p_c+3(1-p_c)^2p_c+\cdots+\\&\varphi(1-p_c)^{\varphi-1}p_c=1-(1-p_c)^{\varphi}/p_c-\\&\varphi(1-p_c)^{\varphi}\overset{\varphi\to\infty}{\approx}\frac{1}{p_c}-\varphi(1-p_c)^{\varphi}\end{aligned} \tag{2}$$

式中:p_c 是无差错完整探测出地址码的概率;φ 为地址码容量$\varphi(NL,w,\lambda)$的简记形式,且取$\varphi(NL,w,\lambda)$为码字容量上界,取文献[8]中码字容

量上界有如下表示形式:

$$\varphi(NL,w,\lambda)\leqslant\frac{N}{w}\prod_{i=1}^{\lambda}\frac{NL-i}{w-i} \tag{3}$$

(2)式中 p_c 又有如下的表示公式[3]:

$$p_c=(1-P_M)^w(1-P_{FA})^{(NL-w)} \tag{4}$$

假设噪声是加性白噪声,则 P_M 和 P_{FA} 有如下表达式:

$$\begin{aligned}P_{FA}&=\exp(-\gamma/N_0)\\P_M&=1-Q[\sqrt{2E/N_0},\sqrt{2\gamma/N_0}]\end{aligned} \tag{5}$$

式中:E/N_0 是信噪比即脉冲能量和噪声功率谱密度;γ 是探测器的阈值;$Q(x,y)$是马库姆概率积分函数。由(1)~(5)式得到图2与图3。

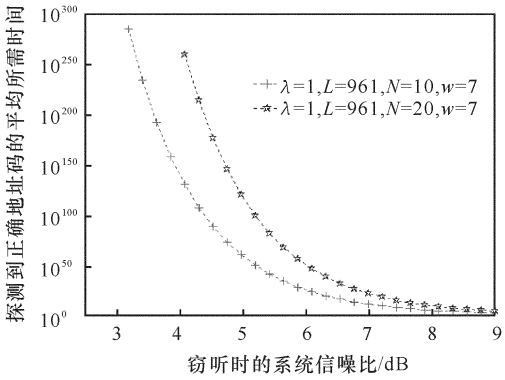

图2 不同波片数下的 t_s 曲线比较

Fig. 2 t_s versus the number of different wave-plate

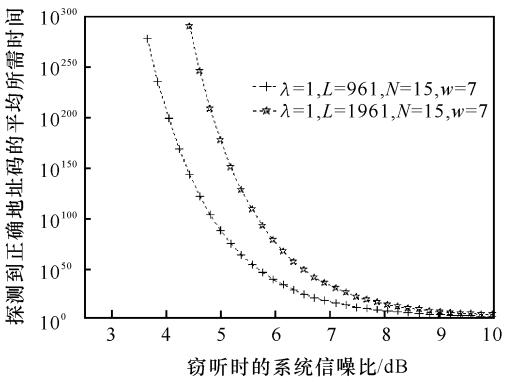

图3 不同码字长下的 t_s 曲线比较

Fig. 3 t_s versus the length of different codes

由图2和图3可知:在信噪比与码字长相同的情况下,随着波片数的增加,完全探测到地址码所需要的时间越长,OCDMA系统安全性越好。在信噪比与码片数相同的情况下,随着码字长的增加,完全探测到地址码所需要的时间越长,故OCDMA系统安全性越好。在相同的波片数与码长下,随着信噪比的增加,完全探测到地址码所需要的时间越短,故OCDMA系统安全性越差。

5 OCDMA系统与光纤保密通信的关系

OCDMA系统是基于光纤光栅的光纤码分多址保密技术,是现阶段光纤保密通信的3种主要技术之一,另2种是混沌保密通信技术和量子保密通信技术。这3种光纤保密通信技术都是利用特殊技术调制基带信号,使窃听者窃听到信号也不可能或很难得到有利用价值的信号。OCDMA技术和混沌通信技术都能克服远距离传输问题,而量子通信不能,但是前2种技术不具备量子通信中的监测功能,不可检测窃听,需要为这2种保密通信系统另外配置监测设备。对于OCDMA技术,急需具有大容量和优良相关性的地址码集合以及实现可灵活调协的编解码器。混沌技术要解决的关键问题是在混沌带宽的限制下如何提高单信道通信容量。而量子通信最重要的环节是如何长距离地在光纤上传输量子密钥。这3种技术都不是简单的数据加密,不是通过某种算法就能破解密码的,因此安全性相对来说也是较高的。

6 结束语

OCDMA系统的安全性与系统自身的参数有着密切的联系,在应用建网的过程中,应根据具体环境与系统设计的需求来设置系统参数以获取最优安全性的OCDMA系统,并通过以下措施增强OCDMA系统的安全性:取用具有优良相关性、码长较长、码容量较大的地址码;采用的用户地址码不要固定不变,并要经常改变用户地址序列;光纤的传输与输出光脉冲要宽频率、低功率;在二维码系统中,可以采用增加不连续波长数来增加OCDMA系统的安全性;从制造工艺上来提高光纤的抗窃听能力;给OCDMA系统配置监测设备,使系统能及时发现窃听事件,以便采用对策;对用户数据信号在进入编码器前或后增加一次加密。

参考文献:

[1] STOCK A, SARGENT E H. The role of optical CDMA in access networks [J]. IEEE Communication Magazines, 2002,40(9):83-87.

[2] AMIRY, YONDAE K, CRISTINA N R. On the performance of group key agreement protocols[J]. ACM Transactions Information System Security,

2004,7(3):457-488.

[3] SHAKE T H. Security performance of optical CDMA against eavedropping [J]. Journal of Lightwave Technology, 2005,23(2):655-670.

[4] SHAKE T H. Confidentiality performance of spectral phase encoded optical CDMA [J]. Journal of Lightwave Technology, 2005,23(4):1652-1663.

[5] LEAID D E, JIAN G Z, WEINER A M. Experimental investigation of security issues in OCDMA: a code-switching scheme[J]. Electro Lett, 2005,41(14):817-819.

[6] 潘武,隆冰,乔婧,等. 二维非相干光码分多址系统信息侦听技术[J]. 光学精密工程, 2008,16(5):943-949.
PAN Wu, LONG Bing, QIAO Jing, et al. Interception of 2D incoherent optical code division multiple access system [J]. Optics and Precision Engineering, 2008, 16(5): 943-949. (in Chinese with an English abstract)

[7] 李传起,李晓滨. 光纤通信OCDMA 系统[M]. 北京:科学出版社, 2008.
LI Chuan-qi, LI Xiao-bin. Optical fiber communication OCDMA system [M]. Beijing: Science Press, 2008. (in Chinese)

[8] YANG G C, KWONG C. Performance comparison of multiwavelength CDMA and WDMA+CDMA for fiber-optic networks [J]. IEEE Transaction on Communication, 1997,45(11):1426-1436.