一种抗 RPE – LTP 声码器压缩的端到端数据传输方法

陈立全[1,2],胡爱群[1],徐　青[1],杨晓辉[1]
(1. 东南大学信息安全研究中心,南京 210096;
2. 福建师范大学网络安全与密码技术重点实验室,福州 350007)

[摘要]　提出了一种基于正交频分复用(OFDM)的抗规则脉冲激励 – 长时预测声码器(RPE – LTP)压缩的端到端数据传输方法。根据 RPE – LTP 声码器特性,将待传输数据分别调制到正交的低频正弦载波上,用快速傅立叶逆变换运算实现信号的调制传输,调制后的波形符合声码器的时频特性。经仿真结果验证,提出的抗压缩传输方法的数据传输速率可达 2.4 kb/s,误码率小于 0.3 %,适合移动网络端到端实时安全语音数据传输使用。

[关键词]　声码器;规则脉冲激励 – 长时预测;正交频分复用;快速傅立叶变换
[中图分类号]　TN925.93; TP393.1　[文献标识码]　A　[文章编号]　1009 – 1742(2007)12 – 0081 – 05

1　引言

全球移动系统(GSM, global system for mobile communication)已经获得了广泛的应用。但随着手机窃听、移动信息泄密现象日益严重,GSM 移动信息端到端安全需求也越来越迫切。GSM 系统本身提供了一套安全系统,但其安全系统是不完整和不彻底的,存在单向鉴权、A_5 加密算法脆弱和基站后语音透明传输等安全隐患[1,2]。因此,只有在 GSM 系统上架构新的端到端安全通信技术才能保证移动信息端到端的安全。在端到端安全方面,首先需要建立端到端的安全通道。端到端的通道有 CSD 电路交换或 GPRS 的数据通道和传统语音通道两种。数据通道传输的缺点是固有时延、抖动和丢包率等 QoS 性能难以保证[3]。对于移动语音端到端的安全而言,要求端到端时延低、灵活方便并能适用已有的移动资费政策。所以,研究在传统语音通道上的端到端传输技术是实现实时移动端到端语音保密通信的关键技术之一。

GSM 系统传统语音通道上存在一编一解的 RPE – LTP 声码器模块。RPE – LTP 声码器是一种混合参数压缩编码算法,通过提取输入语音的声音模型参数进行压缩,然后传输这些参数,而在接收端通过这些模型参数恢复原有的语音[4]。接收端恢复出来的语音在语音特性上是跟原有语音基本一致,但在波形上与原有语音有差异。因此,直接在语音通道上进行语音比特加密处理会使得加密后的信号不具有语音的特征,难以有效通过 RPE – LTP 声码器,而这也限制了一般有线网络上的比特扰乱等加密方法在 GSM 语音通道上的使用。

在传统语音通道上,已有一些机制实现端到端的安全通道。白剑等描述采用信息隐藏方法来实现 GSM 系统上的端到端安全传输,但支持的传输速率低于 2.4 kb/s[5]。N. N. Katugampala 等描述了采用类语音的方法,通过频谱划分和查表模型将保密语音调制成另外一类语音形式来实现穿透声码器传输,在 1.8 kb/s 下的误码率较低[6]。文献[7]分析了 QAM, FSK, DQPSK 等调制方式通过 RPE – LTP 声码器的效

[收稿日期]　2007 – 06 – 11; 修回日期　2007 – 09 – 14
[基金项目]　中国博士后科学基金资助项目(20060400273);网络安全与密码技术重点实验室开放课题资助项目(07B004)
[作者简介]　陈立全(1976 –),男,广西省容县人,东南大学博士后,主要从事移动网络安全理论与技术研究,E-mail: lqchen@ seu. edu. cn

果,验证了 DQPSK 能支持 2.4 kb/s 的调制信号通过 RPE – LTP 声码器,但仅进行了计算机仿真,并没有完成实际 GSM 声码器传输的实验验证。

基于上述的分析,要实现 GSM 移动通信传统语音通道上端到端的安全语音通信,首先需要解决端到端传输通道的问题。笔者提出了一种新的基于 OFDM 的抗声码器压缩端到端调制传输方法,在保证低误码率基础上实现低延迟的数据抗 RPE – LTP 端到端传输。

2 抗 RPE – LTP 传输原理

2.1 正弦波调制传输性能

语音信号是一种时变的准周期信号,在模型上可以近似地看作由许多振幅和相位都随时间变化的正弦波和额外小噪声构成[8]。在研究 RPE – LTP 声码器的输入输出特性时,首先需要研究各频率的正弦波通过声码器的响应性能。GSM06.10 规范[4]以及实验测试结果都表明,低频率的单一正弦波经过声码器编解码可以得到很好的恢复。但正弦波频率越高,恢复的效果越差,超过 2 000 Hz 的正弦波传输的效果会急剧恶化。

究竟多少频率的正弦波经 PSK 调制再通过声码器编码解码后能得到较低的误码率,实验测试方法如下:首先选择一个频率的正弦载波,在该载波上调制固定误码率的数据。如选择 BPSK,采用10 000 个随机数作为测试数据,当数据为 1 时,相位为 0;当数据为 0 时,相位为π,选取的频率为 100 ~ 2 500 Hz。得到结果如表 1 和图 1a 所示。从图 1a 可见,正弦载波的频率低于 2 000 Hz 时 BPSK 调制载波通过 RPE – LTP 声码器有较低的误码率。同样,对 QPSK 调制的测试结果如表 2 和图1 b 所示。从图 1 b可以看到,正弦载波低于 1 500 Hz 时 QPSK 调制通过 RPE – LTP 声码器有较低的误码率。上述现象可以理解为:由于声码器的输入信号是固定 8000 Hz 采样的信号,所以输入信号频率越高,一个周期里的采样得到的样点数就越少。经过声码器编解码后,一个样点的畸变就会更大程度上影响整个波形的结构,从而使传输误码率提高。

表 1 **BPSK** 调制通过声码器的误码率与载波频率对应表

Table 1 BER performance vs. carrier frequency when BPSK signals pass-through the RPE – LTP vocoder

频率值/Hz	100	200	500	800	1 000	1 500	1 800	2 000	2 200	2 500
误码率 $\times 10^{-4}$	0	0	0	0	0	3	4	9	29	776

表 2 **QPSK** 调制通过声码器的误码率与载波频率对应表

Table 2 BER performance vs. carrier frequency when QPSK signals pass-through the RPE – LTP vocoder

频率值/Hz	100	200	500	800	1 000	1 200	1 500	1 800	2 000
误码率 $\times 10^{-4}$	5	6	12	26	17	28	75	194	1001

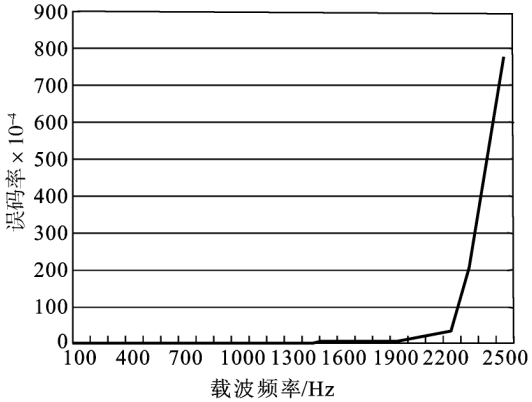
2.2 正交频分复用调制原理

根据上述结果,选择适当的频率和调制方式来实现抗声码器压缩传输。采用正交频分复用(OFDM,orthogonal frequency division multiplexing)的方法,把数据流串并变为 n 路速率较低的子数据流,用它们分别去调制 n 路正交子载波后并行传输。正交频分复用方法不仅可以增加传输效率,而且可以使用快速傅立叶变换(FFT)方法和快速傅立叶逆变换(IFFT)方法来快速实现。

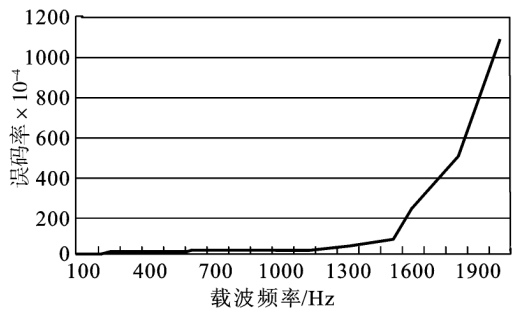
OFDM 将语音数据比特分别调制到多个正交子载波上合成,在接收方利用正交性将每个子载波上的比特解调下来。各个子载波间的正交性通过适当选取子载波间隔实现,子载波间隔应为 OFDM 符号周期的倒数。虽然子信道频谱相互混叠,子载波间的正交性却使得各个子信道依然能够被分离出来[9]。

图 2 是语音通道上基于 OFDM 的数据传输方法框图。传输数据经过 OFDM 调制实现抗声码器压缩,而在接收端通过对应的 OFDM 解调模块实现数据解调。发送侧根据载波频率调制误码率限制(见表 1 和表 2)选择子载波,数据的比特流按照符号周期进行调制,然后送至移动终端中的声码器进行传输发送。数据经过移动终端发送至基站,在基站上解码后,通过核心网络传送至另一基站。另一基站将解码后的数据经 RPE – LTP 编码后无线发送到接收侧的另外一个移动终端上,移动终端 RPE – LTP 解码后通过 OFDM 解调得到有效数据。

OFDM 合成信号的误码率大于等于各个子载波单独的误码率之和,因此,就要求子载波的数目不能太多,但同时要注意到,子载波的数量会在一定程度



(a) BPSK 调制下载波频率与误码率关系



(b) QPSK 调制下载波频率与误码率关系

图 1　BPSK/QPSK 调制下载波频率与误码率关系

Fig. 1　BER performance vs. carrier frequency when BPSK/QPSK signals pass-through the RPE-LTP vocoder

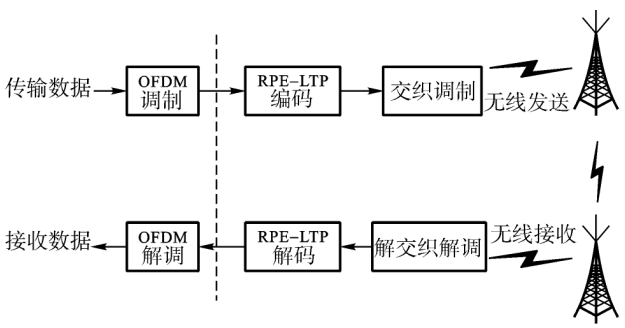


图 2　基于 OFDM 的抗声码器压缩传输方案

Fig. 2　Anti-vocoder transmission scheme based on OFDM

上影响传输的码率,所以子载波的数量也需要一个合适的数值,实验表明,10 ~ 20 个子载波数可以达到较好的效果。

3　OFDM 符号参数

由表 1 和表 2 可以看出,并不是所有频率的正弦波通过声码器都可以以很小的失真度恢复。为了取得良好的传输效果,OFDM 符号中子载波的频率、数量,子载波频率间隔、符号长度以及符号长度与声码器的速率适配问题都需要得到解决。如何保证子载波的频率在一个较低的水平上是保证 OFDM 传输方法有较低误码率的关键。

子载波的数量与子载波频率上限、正交子载波频率间隔以及数据传输速率有关。子载波的数量乘以正交频率间隔即为子载波频率上限。这个频率上限应保持在误码率较低的载波频率范围内。因此要求子载波的数目不能太多,但同时要注意到,子载波的数量会在一定程度上影响传输的误码率,所以子载波的数量需要一个适当的数值。设子载波个数为 n,正交子载波频率间隔为 f',数据传输速率为 R_b b/s,OFDM 的符号周期(也就是每个 OFDM 符号的时间长度)为 T_{ofdm},同时假设子载波采用 PSK 的调制方式,每个子载波可以调制 m 比特的数据。一个符号周期需要传输的比特数为

$$R_b T_{ofdm} = mn。$$

OFDM 的符号间隔为正交频率间隔的倒数:

$$f' = 1/T_{ofdm}。$$

将以上两式综合得到:$f' = R_b/mn$。

有了正交频率间隔,可得到信号所占带宽为

$$F = R_b(n-1)/mn。$$

设起始频率为 f_0,那么子载波的最高频率为

$$F_m = f_0 + R_b(n-1)/mn。$$

令 f_0 等于 f',上式信号的最高频率可以简化为

$$F_m = R_b/m。$$

由此式可以看出,子载波最高频率与数据速率和每个子载波上调制的比特数有直接关系,而与子载波的数量并没有直接的关系。即若要减少符合一定误码率的子载波最高频率,单纯靠减少子载波个数是不起作用的。然而,数据速率确定之后,增加子载波上携带的比特数可以很明显地降低信号子载波的最高频率。子载波上可调制的比特数与声码器的系统特性有关,实验证明,经过声码器的正弦波形最多对 2 比特的 QPSK 有较小的误码率(见表 2)。

4　仿真与分析

首先,测试 OFDM 抗声码器压缩调制方法经过一编一解 RPE – LTP 压缩编码的误码率情况。另外,仿真测试了当数据从一个手机终端到一个基站(一次 RPE – LTP 编解码过程),然后再从另外一个基站到另外一个手机终端(另一次 RPE – LTP 编解码过程)之间的 OFDM 抗声码器压缩调制方法的误

码率情况。得到结果如表 3 所示,其中经过声码器编解码一次和经过声码器编解码二次分别表示上述的两种情况。当数据的压缩速率为 2.4 kb/s 时,符号周期为 20 ms,调制方式为 QPSK,选用 24 个子载波时,经过声码器编解码一次的情况下的 OFDM 抗声码器压缩调制方法误码率为 0.29 %。经过声码器编解码二次的 OFDM 抗声码器压缩调制方法误码率要比只经过一次的大,达到 2.46 %。

表 3　OFDM 方法在 GSM 声码器上传输的误码率

Table 3 BER performance of OFDM scheme transmitted through GSM vocoder

传输速率/ kb· s^{-1}	2.4
符号周期/ ms	20 (一帧)
调制方式	QPSK
子载波个数	24
子载波频率/Hz	0 ~ 1200
误码率(经过声码器编解码一次)/%	0.29
误码率(经过声码器编解码二次))/%	2.46

上述测试得到的误码率结果都是纯调制方法的传输误码结果。在实际应用过程中,可以结合重传机制以及前向纠错 FEC 方法进一步改善 OFDM 抗声码器压缩调制方法的误码情况。

OFDM 调制本身采用多个子载波在一个 OFDM 符号上进行传输,OFDM 符号大小为 20 ms,与 RPE – LTP 声码器配对进行使用。测试并计算抗声码器压缩调制前数据和 OFDM 解调后数据之间的时延值,得到如图 3 所示的结果,横轴表示测试的数据次数,纵轴上数据表示端到端的时延值(包括 OFDM 调制编解码和 RPE – LTP 编解码的时延和)。采用 24 个子载波来实现 2.4 kb/s 码率 OFDM 调制的情况;18 个子载波实现 1.8 kb/s 码率 OFDM 调制的情况和 16 个子载波实现 1.6 kb/s 码率 OFDM 调制的情况。这三种情况的时延值在 120 ms 到 150 ms 之间。假设 RPE – LTP 的处理时延为 15 ms,算法延迟为 20 ms(需要等待 20 ms 数据才进行处理)。而 OFDM 调制传输方法的算法延迟也是 20 ms。考虑其他传输时延影响,则可以测算出来 OFDM 抗声码器压缩调制方法的处理时延为 5 ~ 20 ms。采用高速 DSP 处理芯片可以进一步降低处理时延值,达到实时处理的要求。总之,在语音通道上采用 OFDM 抗声码器压缩调制方法的端到端时延要远小于数据通道数据传输的延迟值。

最后,进行压缩语音传输的实验,验证 OFDM 抗

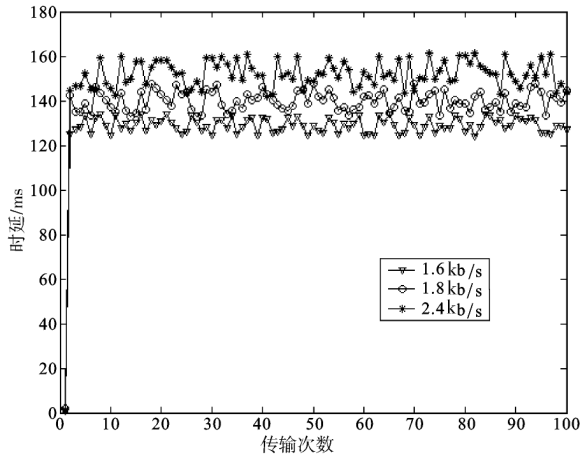


图 3　OFDM 方法端到端时延分布图

Fig. 3　End-to-end delay performance of OFDM scheme

声码器压缩调制方法的语音传输性能。选择一段男性中年语音,发音为“欢迎您来上海,罗波兹先生。**Nice to meet you, director Chen.** ”,经过 2.4 kb/s 的 MELP 压缩编码、OFDM 调制、RPE – LTP 声码器编码、解码、OFDM 解调、MELP 解压缩之后,得到输出语音波形。用 C 语言程序模拟实现 MELP 编解码来进行数据压缩,通过 MATLAB 进行 OFDM 调制和解调,再通过 RPE – LTP 声码器的编解码仿真平台,得到的原始语音波形和加解密输出语音波形如图 4 所示。

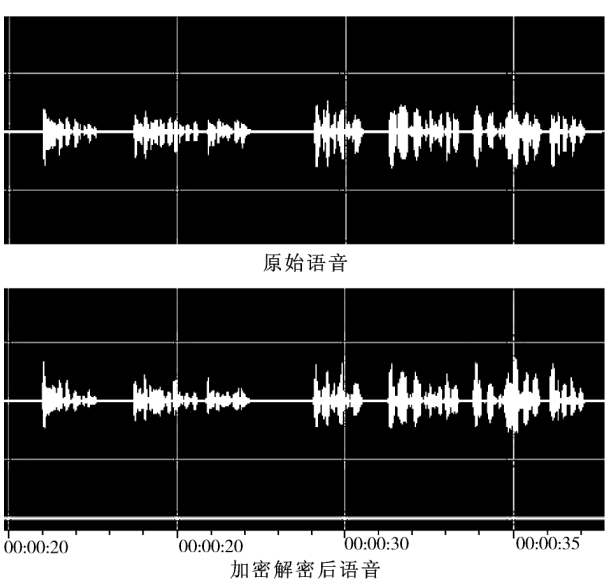


图 4　原始语音和经过加解密后的语音波形比较图

Fig. 4　the decrypted voice waveform vs. original voice waveform

从图 4 所示的时域波形上可以看出,合成后的信号较好地还原了语音的时间包络。而人耳听到的语音

具有良好的可懂度和一定的自然度。同时也可以看出,它们波形之间是有一定的差别,也就是说存在某种程度的失真,但是这种失真不会影响语音的可懂度。

5 结语

提出了一种通过 GSM 数字移动系统语音通道进行端到端安全通信的数据传输方法。将 OFDM 用于有 RPE – LTP 声码器的语音通道传输系统上。OFDM 传输方法突破了抗声码器压缩的传输问题,数据传输速率可达 2.4 kb/s,误码率小于 0.3 %,可以在话音通道上实现语音数据的端到端保密通信。该方法还可应用到如 CDMA,3G 等有语音压缩编码的语音通信系统中。

参考文献

[1] Lo Chichun, Chen Yujen. Secure communication mechanisms for GSM networks [J]. IEEE Transactions on Consumer Electronics, 1999,45(4): 1074 ~ 1079

[2] Street M. Interoperability and international operation: an introduction to end to end mobile secure [A]. IEE Secure GSM and Beyond: End to End Security for Mobile Communications [C]. London, UK, Feb 2003

[3] Challans P, Gover R, Thorlby J P. End to end data bearer performance characterization for communications over wide area mobile networks [A]. IEE Secure GSM and Beyond: End to End Security for Mobile Communications [C]. London, UK, Feb 2003

[4] ETSI Standard GSM 06.10, Digital cellular telecommunications system: Full rate speech transcoding [S]. ETSI SMG 2 Group, Valbonne, France, Mar 1997

[5] 白 剑,杨 榆,徐迎晖,等. GSM 移动通信系统中语音隐藏算法研究 [J]. 中山大学学报,2004, 43 (2): 156 ~ 159

[6] Katugampala N N, Ai-Nami K T, Villette S, et al. Real time data transmission over GSM voice channel for secure voice & data applications [A]. The 2nd IEE Secure Mobile Communications Forum: Exploring the Technical Challenges in Secure GSM and WLAN [C]. London, UK, Sept 2004

[7] 陈一帅. GSM 语音加密研究[D]. 北京: 北方交通大学, 2001

[8] Mcaulay R J, Quatieri T F. Speech analysis/synthesis based on a sinusoidal representation [J]. IEEE Transactions on Acoustics, Speech and Signal Proceeding, 1986, 34(4):744 ~ 754

[9] Speth M, Frchtel S A, Fock G, et al. Optimum receiver design for OFDM based broadband transmission-part II: a case study [J]. IEEE Transactions on Communications, 2001, 47(11): 571 ~ 578

An End-to-end Modulating Transmission Scheme With Good Robustness Against the RPE-LTP Vocoder

Chen Liquan[1,2], Hu Aiqun[1], Xu Qing[1], Yang Xiaohui[1]

(*1. Information Security Research Center, Southeast University, Nanjing, 210096, China;*
2. Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China)

[**Abstract**] A novel end-to-end data transmission scheme based on OFDM mechanism with good robustness against the RPE – LTP vocoder in GSM voice channel is proposed. According to the character of RPE – LTP vocoder, data are modulated to orthogonal low-frequency sinusoidal carrier. In OFDM, the modulation is done by IFFT and the modulated signals are conformed to the time and frequency characters of RPE-LTP vocoder. The results of simulation show that the transmission bit rate of the proposed scheme reaches 2.4 kb/s, and the bit error rate of the scheme is lower than 0.3 %. This scheme provides a new approach for real-time secure voice data transmission over GSM system.

[**Key words**] vocoder; regular pulse excited-long term prediction; OFDM; FFT