一种基于振幅比较的UWB信号解调方法

张 林 王 殊
(华中科技大学电子与信息工程系 武汉 430074)

摘 要 无传统意义上的载波带来的低复杂度特性是脉冲无线电超宽带(ultra-wideband,UWB)通信的一大优势,既有较佳的接收性能又有简单的结构是UWB系统设计的目标。提出了一种基于振幅比较的UWB信号接收的解调方法,即在脉冲位置调制中的特定位置,分别对脉冲的正负半周积分获得振幅信息,并通过比较这些振幅解调出符号信息。该方法能够在接收性能和系统复杂性之间获得较好的平衡。结果表明,它以较小的复杂性代价换取了比平方律检测好5dB以上的误码性能;而与相关检测相比,误码性能约降低了2dB,但复杂度低于相关检测。

关键词 超宽带,振幅比较,平方律检测,相关检测
中图法分类号 TN92 **文献标识码** A

Demodulation Method for UWB Signal Based on Amplitude Comparison

ZHANG Lin WANG Shu
(Dept. of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract The lower complexity is an outstanding advantage of impulse radio ultra-wideband(UWB) communication due to traditional carrier free. Both better performance and a simple receiver structure are the UWB system design goals. A novel demodulation algorithm for UWB signal reception based on amplitude comparison was proposed. The pulse amplitudes were obtained by integrating positive and negative half cycle of the pulse respectively at special position in pulse position modulation scheme, and then the binary symbol was demodulated by comparing their amplitudes. The receiver can get a better balance between reception performance and system complexity by using this method. The results show that the proposed method can remarkably obtain better bit error ratio performance(over 5dB) than the square law detection with a little expense of complexity, and reduce complexity in comparison with coherent detection but less than 2dB performance degradation.

Keywords Ultra-wideband, Amplitude comparison, Square law detection, Coherent detection

随着对UWB系统研究的不断深入,实际系统的实现已变得越来越重要。寻找既有较佳的接收性能,又有简单易实现的收发方法是不少研究者关注的焦点。目前在UBW信号接收中,主要有相关解调和非相关解调两种方式。相关解调由于有较高的功率效率而广受关注。但是,要获得更高质量的接收效果,通常需要采用RAKE接收机。这样就需要预先获得每个信道的多经时延、衰落系数、脉冲形状等相关信息的估计,由此增加了系统的复杂性[1-3]。

基于平方律(能量)检测的非相关解调,由于具有较低的系统复杂性,在实际的UWB系统实现时被越来越多地采用。与相关检测不同,这种非相关检测无需预知信道的有关信息,从而降低了系统的复杂性,但同时也降低了接收性能[4-6]。

本文提出了一种基于振幅比较的非相关解调方法。与前述两种方法相比,该方法可以获得比平方律检测低得多的误码率,而系统的复杂性却低于相关检测接收机。

振幅比较检测方法的实质是:接收机检测在特定的区域内,承载信息的脉冲波形幅值是否超过特定值,从而判决是否有脉冲出现。振幅比较解调方法首选的脉冲波形是正负振幅对称的波形,如一阶高斯脉冲、一阶Hermite脉冲和正弦脉冲等[7,8]。显然,收发天线的微分特性会对振幅比较解调带来严重影响。为了克服这一影响,采用文献[7]中提出的收发器架构是一个较好的选择。其解决方法是,在信号送达发送天线前先进行积分,然后在接收天线后再进行积分,这样便消除了天线带来的影响。在本文的阐述中,采用了一阶高斯脉冲作为UWB信号脉冲序列,且假设已消除了天线的影响。

振幅比较解调方法可用于脉冲位置调制(PPM)和开关键控(OOK)调制的解调中,并且稍做修改,也可用于二进制移相键控(BPSK)调制的解调中。

文章首先描述了二进制PPM和OOK调制的振幅比较解调算法。其次着重分析了PPM调制方案下振幅比较解调的误码率性能。最后通过仿真,对相关解调、基于平方律解调和本文提出的振幅比较解调3种方法的误码率进行了对比,并给出了小结。

到稿日期:2009-11-12 返修日期:2010-01-25

张 林(1963—),男,副教授,主要研究方向为短距离超宽带无线通信、弱信号检测,E-mail:campzh@hust.edu.cn;王 殊(1956—),男,教授,博士生导师,主要研究方向为智能信号检测、传输、处理及应用和传感器及无线传感器网络等。

1 振幅比较解调算法

1.1 基于 PPM 调制的振幅比较解调

在 UWB 通信中，PPM 调制是较早提出的一种调制方式，由于其较好的性能而被广泛采用[9]。在单用户环境下，基于 PPM 调制的 UWB 信号序列可表示为

$$s(t)=\sum_{j=-\infty}^{\infty} w(t-j\cdot T_f-c_j\cdot T_c-\delta\cdot d_{\lfloor j/R\rfloor}) \tag{1}$$

式中，T_f 为脉冲的帧间隔时间，R 为每符号重复脉冲数，$\{c_j\}$ 是伪随机码，在跳时多址方案中作为区分不同用户的唯一标识码，T_c 是伪随机码单位时移。$d_{\lfloor j/R\rfloor}$ 表示二进制调制数，即 $d_{\lfloor j/R\rfloor}(\{0,1\}$。符号$\lfloor x\rfloor$表示对 x 取整，δ 为调制时移。$w(t)$ 为单位能量一阶高斯脉冲波形，即

$$w(t)=\begin{cases}-\sqrt{\dfrac{10}{\pi\tau_p}}\dfrac{t}{\tau_p}\exp\left(-\dfrac{t^2}{\tau_p^2}\right) & -2.5\tau_p\leqslant t\leqslant 2.5\tau_p\\ 0 & \text{其他}\end{cases} \tag{2}$$

式中，τ_p 为脉冲宽度因子。由于超过 99.7%的脉冲能量集中在$-2.5\tau_p$ 到 $2.5\tau_p$ 区间内，因此这里认为脉冲持续时间为 $5\tau_p$。

当仅考虑高斯白噪声(AWGN)信道时，接收端的信号为

$$r(t)=s(t)+n(t) \tag{3}$$

式中，$n(t)$表示零均值高斯白噪声随机过程。在精确定时和不考虑干扰的条件下，发送符号“0”和“1”时，收端的脉冲波形分别为图 1 中实线波形和虚线波形。

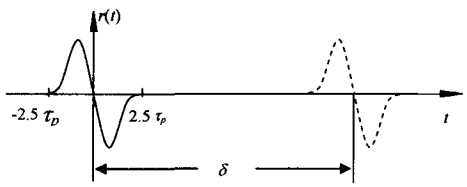

图 1 PPM 波形

通过比较 $t=0$ 处和 $t=\delta$ 处波形的振幅，便可解调出二进制符号。具体方法是：若 $t=0$ 处波形的振幅大于 $t=\delta$ 处波形的振幅，则收到符号“0”，否则收到“1”。但在实现时，并不是采用简单的门限检测方法检测振幅，而是加入了积分运算，先分别对正半周和负半周积分，然后取其差值作为振幅检测值，该算法为

$$\int_{-2.5\tau_p}^{0} r(t)\mathrm{d}t-\int_{0}^{2.5\tau_p} r(t)\mathrm{d}t\underset{1}{\overset{0}{\gtrless}}\int_{\delta-2.5\tau_p}^{\delta} r(t)\mathrm{d}t-\int_{\delta}^{\delta+2.5\tau_p} r(t)\mathrm{d}t \tag{4}$$

采用积分的目的是最大限度地减少噪声的干扰。式(4)可等价为

$$\int_{\delta-2.5\tau_p}^{\delta}[r(t-\delta)-r(t)]\mathrm{d}t\underset{1}{\overset{0}{\gtrless}}\int_{\delta}^{\delta+2.5\tau_p}[r(t-\delta)-r(t)]\mathrm{d}t \tag{5}$$

据此，检测判决器结构如图 2 所示。接收信号经延时相减后，被不同时段的两个积分器积分。判决器根据积分结果解调出二进制符号“0”和“1”。

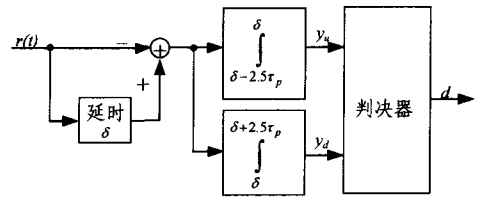

图 2 PPM 的振幅比较解调器结构

其中

$$\begin{aligned}y_u&=\int_{\delta-2.5\tau_p}^{\delta}[r(t-\delta)-r(t)]\mathrm{d}t\\ y_d&=\int_{\delta}^{\delta+2.5\tau_p}[r(t-\delta)-r(t)]\mathrm{d}t\end{aligned} \tag{6}$$

当考虑脉冲重复次数时，二进制符号判决可表示为

$$d=\begin{cases}0, & \sum_{r=0}^{R-1}y_{u,r}\geqslant\sum_{r=0}^{R-1}y_{d,r}\\ 1, & \sum_{r=0}^{R-1}y_{u,r}<\sum_{r=0}^{R-1}y_{d,r}\end{cases} \tag{7}$$

由振幅比较解调器结构看出，这里用延时线和减法器取代了相关解调器结构中的脉冲产生器和乘法器，而与平方律检测相比，多了延时线和减法器，但少了平方运算。

1.2 基于 OOK 调制的振幅比较解调

当采用 OOK 调制时，UWB 信号序列可表示为

$$s(t)=\sum_{j=-\infty}^{\infty} d_{\lfloor j/R\rfloor}w(t-j\cdot T_f-c_j\cdot T_c) \tag{8}$$

在接收机精确定时和同步条件下，发送二进制符号“1”时，无噪声和干扰的“纯净”脉冲波形如图 3 所示。其中 V_{th} 为门限值，A 为振幅，且 $A=\sqrt{\dfrac{10}{2\pi\tau_p e}}$。

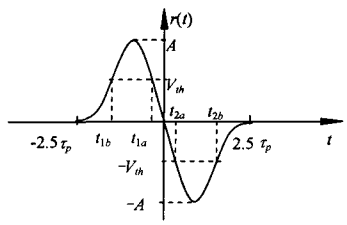

图 3 一阶高斯脉冲及双门限检测

在 OOK 信号的振幅比较解调中采用双门限比较方式。与 PPM 解调类似，此处也加入了积分运算。检测算法为：首先在两个时间段$[t_{1b},t_{1a}]$和$[t_{2a},t_{2b}]$内，分别对接收信号与两个门限的差值进行积分；然后将两个积分结果与 0 值比较，从而判定是否有脉冲波形出现。即，两个积分为

$$\begin{aligned}y_u&=\int_{t_{1b}}^{t_{1a}}(r(t)-V_{th})\mathrm{d}t\\ y_d&=\int_{t_{2a}}^{t_{2b}}(r(t)-(-V_{th}))\mathrm{d}t\end{aligned} \tag{9}$$

考虑脉冲重复次数时，符号判决为

$$d=\begin{cases}1, & \sum_{r=0}^{R-1}y_{u,r}\geqslant 0 \text{ and } \sum_{r=0}^{R-1}y_{d,r}\leqslant 0\\ 0, & \text{orthers}\end{cases} \tag{10}$$

显然，门限值的选择将直接影响误码特性。文献[10]对 OOK 调制方式做了较详细的分析。

2 误码特性分析

本节重点分析 AWGN 信道下 PPM 信号的接收误码特

性。由于式(3)中的 $n(t)$ 是零均值高斯白噪声过程，因此，式(6)中的积分结果 y_u 和 y_d 也是独立同分布的高斯随机过程。

当发送端发送符号“0”时，y_u 的均值为

$$\bar{y}_{u0}=E\{y_u\}=E\left\{\int_{\delta-2.5\tau_p}^{\delta}[r(t-\delta)-r(t)]\mathrm{d}t\right\}$$

$$=\frac{1}{2}\sqrt{\frac{10\tau_p}{\pi}}[1-\exp(-2.5^2)] \tag{11}$$

式中，$E\{\cdot\}$ 表示期望值。同理，y_d 的均值为

$$\bar{y}_{d0}=\frac{1}{2}\sqrt{\frac{10\tau_p}{\pi}}[\exp(-2.5^2)-1] \tag{12}$$

当发“1”时，y_u 和 y_d 的均值分别为

$$\bar{y}_{u1}=-\frac{1}{2}\sqrt{\frac{10\tau_p}{\pi}}[1-\exp(-2.5^2)] \tag{13}$$

$$\bar{y}_{d1}=-\frac{1}{2}\sqrt{\frac{10\tau_p}{\pi}}[\exp(-2.5^2)-1] \tag{14}$$

它们的方差是相同的，均为

$$\sigma_y^2=\sigma^2(2.5\tau_p)^2 \tag{15}$$

式中，σ^2 为噪声 $n(t)$ 的方差。为便于误码率的计算，设如下变量代换

$$z=y_u-y_d \tag{16}$$

则 z 也服从高斯分布。当考虑脉冲重复次数 R 时，$z\sim N(R(\bar{y}_u-\bar{y}_d),2R\sigma_y^2)$。根据式(7)的判据，发“0”收“0”的正确概率为

$$P(0|0)=P\{z\geqslant 0\}=\int_0^{\infty}f_z(z)\mathrm{d}z$$

$$=\left(\frac{1}{2}-\frac{1}{2}erf(-\frac{\sqrt{R}(\bar{y}_{u0}-\bar{y}_{d0})}{\sqrt{2}\sigma_y})\right) \tag{17}$$

同理，发“1”收“1”的正确概率为

$$P(1|1)=P\{z<0\}=\int_{-\infty}^{0}f_z(z)\mathrm{d}z$$

$$=\left(\frac{1}{2}+\frac{1}{2}erf(-\frac{\sqrt{R}(\bar{y}_{u1}-\bar{y}_{d1})}{\sqrt{2}\sigma_y})\right) \tag{18}$$

当等概率发送“0”和“1”，即 $P(1)=P(0)=1/2$ 时，总正确接收概率为

$$P_c=\frac{1}{2}(P(0|0)+P(1|1)) \tag{19}$$

因此总误码率为

$$P_e=1-P_c \tag{20}$$

将式(11)－式(14)分别代入式(17)和式(18)，并根据式(19)和式(20)整理得总误码率为

$$P_e=\frac{1}{2}erfc\left(\frac{1}{\sigma_y}\sqrt{\frac{5\tau_pR}{\pi}}[1-\exp(-2.5^2)]\right) \tag{21}$$

设二进制 PPM 调制方式的信噪比(SNR)为每符号(bit)功率与噪声功率之比，即

$$\gamma_b=\frac{P_b}{\sigma^2}=\frac{E_b/T_f}{WN_0/2}=\frac{E_b/T_f}{N_0/2\tau_p}=\frac{E_b}{N_0}\cdot\frac{2\tau_p}{T_f}=S_{nr}\cdot\frac{2\tau_p}{T_f} \tag{22}$$

式中，E_b 为发送“0”和“1”等概时的比特平均能量，P_b 为比特平均功率(此处利用了功率等于能量在时间上取平均的关系)，$N_0/2$ 为噪声谱密度，$W=\frac{1}{\tau_p}$ 为一阶高斯脉冲波形的带宽，T_f 为 bit 持续时间，$S_{nr}=\frac{E_b}{N_0}$ 为通常的数字信号比特信噪比。又因为

$$\gamma_b=\frac{P_b}{\sigma^2}=\frac{\frac{E_b}{T_f}}{\sigma^2}=\frac{E_w}{T_f\sigma^2}=\frac{1}{T_f\sigma^2} \tag{23}$$

式中，E_w 是脉冲波形的能量，脉冲是单位能量，所以 $E_w=1$。由式(22)、式(23)和式(15)得

$$\sigma_y=2.5\tau_p\sigma=2.5\sqrt{\frac{\tau_p}{2S_{nr}}} \tag{24}$$

将式(24)代入式(21)得误码率为

$$P_e=\frac{1}{2}erfc\left(\sqrt{\frac{8S_{nr}R}{5\pi}}[1-\exp(-2.5^2)]\right)$$

$$=Q\left(\sqrt{\frac{16S_{nr}R}{5\pi}}[1-\exp(-2.5^2)]\right) \tag{25}$$

3 仿真结果

这里，分别在 AWGN 信道和室内视距多径 CM1[11] 信道下，对振幅比较解调、相关解调和平方律解调 3 种方法的误码率进行了计算机仿真。仿真时主要参数设置为：脉冲宽度因子 0.1ns，帧间隔时间 100ns，脉冲重复次数 1，伪随机码长 18，码单位时移 4ns，调制时移 2ns。

AWGN 信道下的仿真结果如图 4 所示。由此看出，当误码率大于 10^{-5} 时，相关检测的功率效率优于本文提出的振幅比较解调约 2dB，但振幅比较解调优于平方律检测至少 5dB。

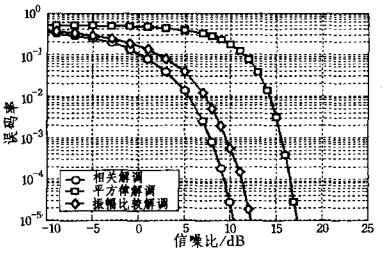

图 4 AWGN 信道下的误码率

图 5 显示了 CM1 信道下的仿真结果。与 AWGN 信道相比，由于 CM1 信道的多径衰落，使得 3 种方法的误码性能均降低超过 11dB，误码率曲线关系与 AWGN 信道类似，但影响程度有所不同。从图中看出，CM1 信道对相关检测影响最小，其次是振幅比较解调，影响最大的是平方律检测。

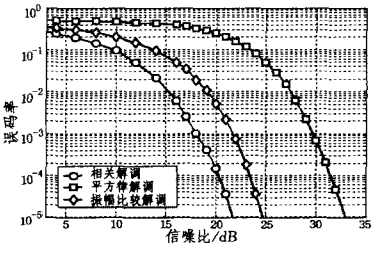

图 5 CM1 信道下的误码率

结束语 追求更加简单有效的收发方式和便于实现系统结构是 UWB 通信系统努力的方向之一。本文提出了基于振幅比较的 UWB 信号非相关解调算法。文中详细描述了该算法的实现，推导了基于 PPM 调制的 AWGN 信道下的误码特性解析式。分析和仿真表明，振幅比较解调方法的复杂度低于相关解调而略高于平方律解调；相同信噪比下误码率远低于平方律解调而略高于相关解调。说明该方法可以在复杂性和误码性能间取得较好的平衡，是一种极具价值的 UWB 信号接收解调方法。

参 考 文 献

[1] Sahin M E, Guvenc I, Arslan H. Optimization of Energy Detector Receivers for UWB Systems[C]// Stockholm. IEEE Vehicular Technol. Conf. 2005, 2: 1386-1390

(下转第 81 页)

CDH 难问题，所以无法计算用户 A 和 B 之间的共享会话密钥。

·增强的密钥泄漏模仿攻击(Strengthen Key Compromise Impersonation resilience)。假设攻击者获得了 KGC 的主私钥和 A 的私钥，则当攻击者用自己的私钥对第一个消息分量签名并发送给 A 时，由于 A 认为拟定的接收者为 B，因此利用 B 的身份信息进行验证。一旦 A 验证失败，A 立即知道有人冒充 B 与自己执行协议，因此 A 取消协议。从而攻击者 C 不能冒充 B 与 A 建立共享的会话秘密。由定义 1、定义 2 及定义 3 可知，协议若能抵抗增强的私钥泄漏模仿攻击，则一定能抵抗私钥泄漏模仿攻击和主私钥泄漏模仿攻击。

结束语 本文比较近几年基于身份的密钥协商协议后，认为王等人提出的基于身份的密钥协商协议比较特殊。根据该协议的特点，首先对私钥泄漏模仿攻击的分类进行了扩充，具体分析了王等人的协议，发现他们的协议不能抵抗主私钥泄漏模仿攻击与增强的私钥泄漏模仿攻击。之后分析了存在攻击的原因，并对协议进行了改进。最后分析了改进后协议的安全性质。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Advances in Cryptology- Crypto'84. Springer, Heidelberg, 1984, LNCS 196: 47-53

[2] Boneh D, Franklin M. Identity based encryption from the Weil pairing[C]// Advances in Cryptology-Crypto'2001. Springer, Heidelberg, 2001, LNCS 2139: 213-229

[3] Smart N P. An identity based authenticated key agreement protocol based on the Weil pairing[J]. Electro. Lett., 2002, 38: 630-632

[4] Joux A. A one-round protocol for tripartite Diffie-Hellman[C]// Algorithmic Number Theory Symposium-ANTS-IV. Springer, Heidelberg, 2000, LNCS 1838: 385-394

[5] Shim K. Efficient ID-based authenticated key agreement protocol based on the Weil pairing[J]. Electron Lett, 2003, 39: 653-654

[6] Chen L, Kudla C. Identity based authenticated key agreement from pairings[C]// IEEE Computer Security Foundations Workshop. 2003: 219-233

[7] Ryu E, Yoon E, Yoo K. An efficient ID-based authenticated key agreement protocol from pairings[C]// Networking 2004. Springer, Heidelberg, 2004. LNCS 3042: 1458-1463

[8] McCullagh N, Barreto P S L M. A new two-party identitybased authenticated key agreement[C]// Topics in Cryptology-CT-RSA 2005. Springer, Heidelberg, 2005, LNCS 3376: 262-274

[9] Choie Y, Jeong E, Lee E. Efficient identity-based authenticated key agreement protocol from pairings[J]. Appl. Math. Comput, 2005, 162: 179-188

[10] Chow S S M, Choo K-K R. Strongly-secure identity-based key agreement and anonymous extention[C]// ISC 2007. Springer, Heidelberg, 2007, LNCS 4779: 203-220

[11] Chen L, Cheng Z, Smart N P. Identity-based key agreement potocols from pairings[J]. International Journal Information Security, 2007, 6: 213-241

[12] Zhu R W, Yang Guomin, Wong Duncan S. An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices Source[J]. Theoretical Computer Science, 2007, 378(2): 198-207

[13] Gentry C. Practical identity based encryption without random oracles[C]// Proceedings of the EUROCRYPT'06. Springer Verlag, Berlin, 2006, LNCS 4004: 445-464

[14] 王圣宝，曹珍富，董晓蕾. 标准模型下可证安全的身份基认证密钥协商协议[J]. 计算机学报，2007，30(10)：1842-1852

[15] Boyd C, Mathuria A. Protocols for Authentication and a Key Establishment[M]. Berlin: Springer Verlag, 2003

(上接第 70 页)

[2] Guvenc I, Arslan H. On the Modulation Options for UWB Systems[C]//Boston. IEEE Mil. Commun. Conf. 2003, 2: 892-897

[3] Gong Yun-rui, He Di, He Chen, et al. Efficient Modulation on the Performance of Coherent Receivers for Pseudo-chaotic TH-UWB System[C]//Macao. IEEE Asia Pacific Conf. on Circ. and Syst. 2008: 1094-1097

[4] Weisenhorn M, Hirt W. Robust Noncoherent Receiver Exploiting UWB Channel Properties[C]//Kyoto. IEEE UWB Systems Joint with Conf. on UWB Syst. and Technol. Joint UWBST & IWUWBS. Intl. Workshop. 2004: 156-160

[5] Yang Liu-qing, Giannakis G B, Swami A. Noncoherent Ultra-Wideband(De)Modulation[J]. IEEE Transactions on Communications, 2007, 55(4): 810-819

[6] Goeckel D L, Mehlman J, Burkhart J. A Class of Ultra Wideband (UWB) Systems with Simple Receivers[C]// Orlando. IEEE Mil. Commun. Conf. 2007, 10: 1-7

[7] Godara B, Blamon G, Fabre A. UWB: A New Efficient Pulse Shape and its Corresponding Simple Transceiver[C]// Siena. IEEE 2nd Intl. Symposium on Wireless Commun. Syst. 2005, 9: 365-369

[8] Zaman A A, Islam N. Modulation Schemes and Pulse Shaping in Ultra-wideband[C]// Huntsville. IEEE Southeastcon. 2008, 4: 142-146

[9] Win M, Scholtz R A. Impulse Radio: How It Works [J]. IEEE Commun. Letters, 1998, 2: 36-38

[10] Zhang L, Wang S, Deng T P, et al. A Novel Demodulation Method based on Zero-Crossing Detection for UWB Signal Reception[C]// Beijing. WiCom '09. 5th Intl. Conf. on Wireless Comm. Networks Sec. Networking and Mobile Computing. 2009, 9: 1-4

[11] Foerster J. Channel modelling sub-commitee report final[R]. IEEE P802. 15-02/368r5-SG3a. 2002