基于MSP430单片机及FPGA的GPS数据转换

赵恒玮 张靖
（东南大学电气工程学院）

摘 要：本文介绍了全球卫星定位系统GPS的概念、数据的格式及内容，分析了需要实现的功能，设计了基于MSP430单片机及FPGA的解决方案．文中给出了软件处理的流程图和接口电路的框图。

关键词：GPS MSP430单片机 FPGA 接口电路
中图分类号：TP392 **文献标识码**：A **文章编号**：1672-3791(2007)11(b)-0091-02

GPS导航系统是以全球24颗定位人造卫星为基础，向全球各地全天候地提供三维位置、三维速度等信息的一种无线电导航定位系统。它由三部分构成，一是地面控制部分，由主控站、地面天线、监测站及通讯辅助系统组成。二是空间部分，由24颗卫星组成，分布在6个轨道平面。三是用户装置部分，由GPS接收机和卫星天线组成。

某型号的GPS接收机每秒输出数据包十次，包括时间（时、分、秒）、三维位置、三向速度（WCG-84坐标系XYZ方向速度）。时钟统一信号秒脉冲 PPS为TTL电平。输出接口类型为RS422接口，5线：RX+、RX-、TX+、TX-、信号地。GPS解包系统的功能就是按照约定的协议接收GPS定位数据，并且在接收以后转化为指定的格式放入缓冲存储器中，下一级的应用系统可以在需要时读取GPS定位数据。

1 MSP430单片机系统的设计

MSP430系列单片机，为16位RISC结构，具有丰富的寻址方式、简洁的指令系统；大量的寄存器以及片内数据存储器；有较高的处理速度，外接8MHZ的时钟信号，指令周期为125ns。工作电压范围较宽，在1.8～3.6V电压、1MHz时钟条件下运行，耗电电流在0.1～400μ之间。MSP430系列单片机具有丰富的片内外设，具有三个定时器（看门狗定时器WDT、定时器A、定时器B）、两个串行通信接口（USART0、1）、硬件乘法器、模数转换模块ADC以及通用IO端口P0～P6。

选择MSP430X14X系列中的MSP430F149IPM作为微控制器，该型号支持在系统可编程（ISP），通过JTAG接口可以很方便地调试和编程。片上有60KB FLASH和2KBRAM。图1为系统硬件原理图。外接5.5296MHZ的高速晶振作为系统时钟源。系统启动或复位时系统在数控振荡器（DCO）时钟下运行，DCO的频率会随着温度和电压的变化而变化，所以初试化时选择稳定的高速晶体振荡器输出的时钟信号。

采用MAXIM半导体的MAX3488作为单片机MSP430F149IPM串口与RS422接口之间的转换电路。MAX3488是针对低电压应用而设计的RS422全双工收发器。无数据传送方向控制，最高数据传送速度为12Mbps。

GPS数据包由包头、GPS实时数据和包尾组成。GPS串行通信数据的波特率为57.6Kbps，起始位为1，数据位8位，停止位为0，无校验字，数据以十六进制方式传送。单片机MSP430F149IPM软件流程图2。

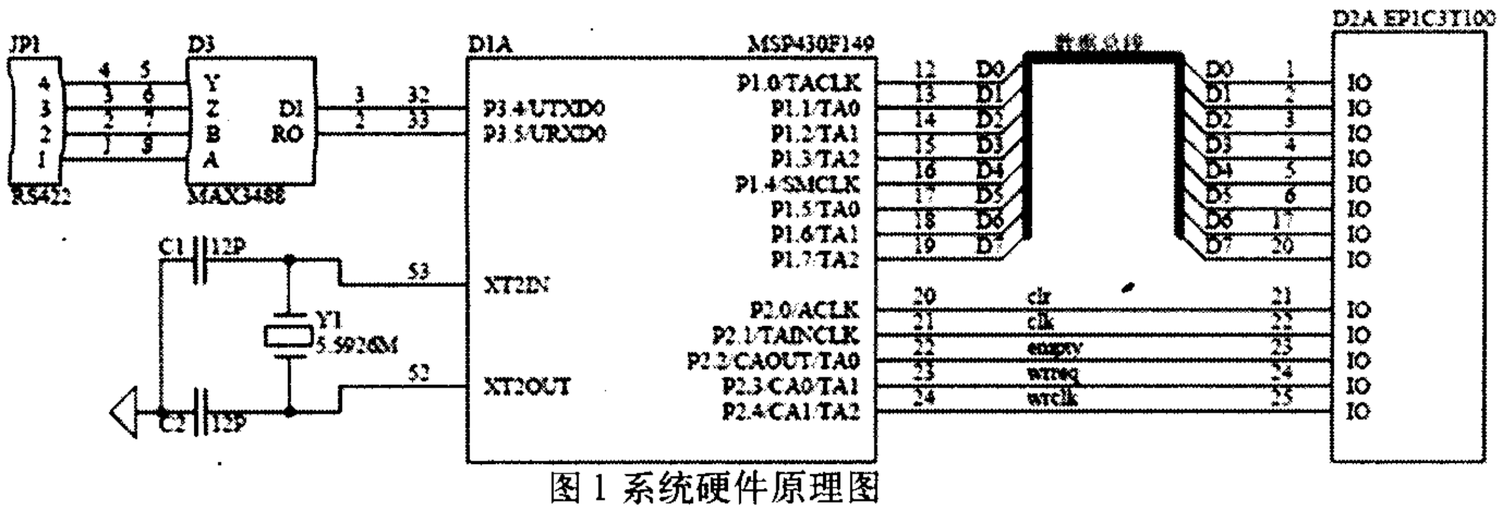

图1 系统硬件原理图

2 FPGA系统的设计

GPS数据解包处理以后，输出格式为10个32位二进制数。通过8位的数据总线输出到FPGA，在FPGA构造硬件电路将其重新排列为32位二进制数存入缓冲存储器FIFO中，下一级处理系统可以读取。

接口电路在FPGA中实现，结构框图3。

4个8位二进制数组成1个32位二进制数。在脉冲到来之前要将数据输出到总线收发器中。脉冲分配器将4个8位数据依此锁存进对应的锁存器中形成1个32位的数据。

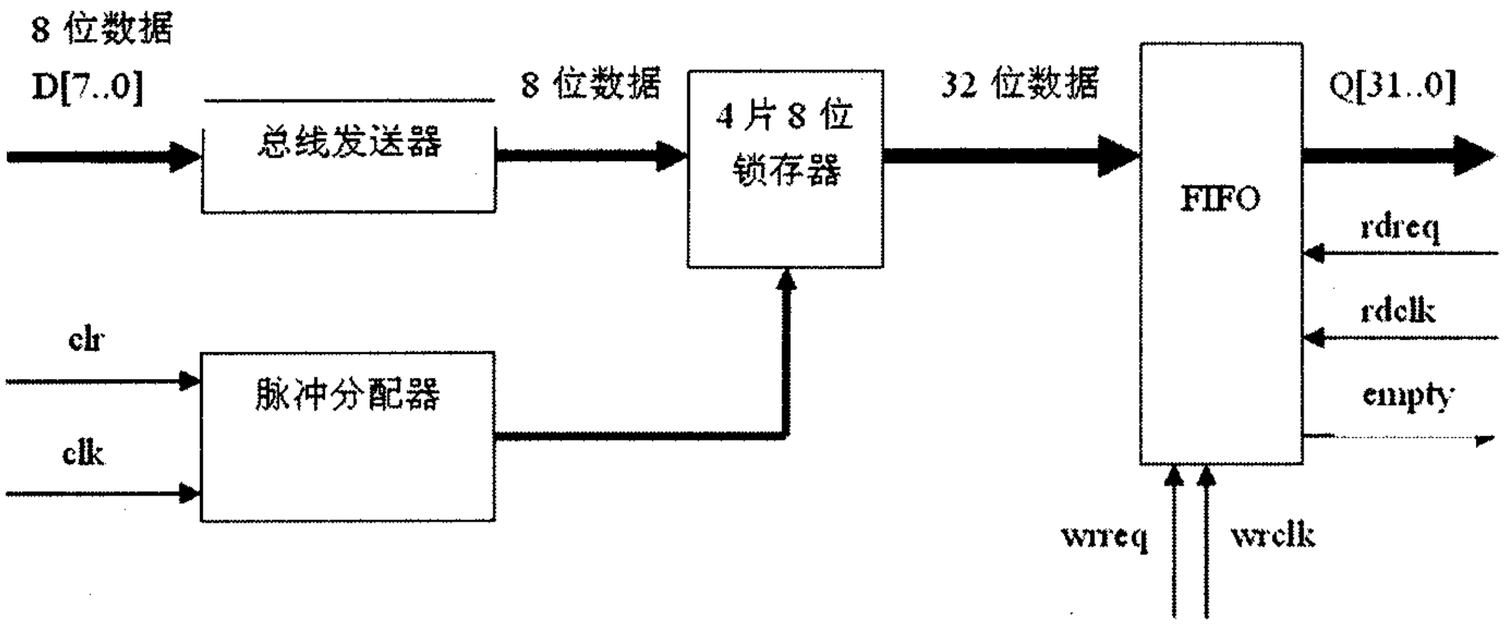

图3 接口电路结构框图

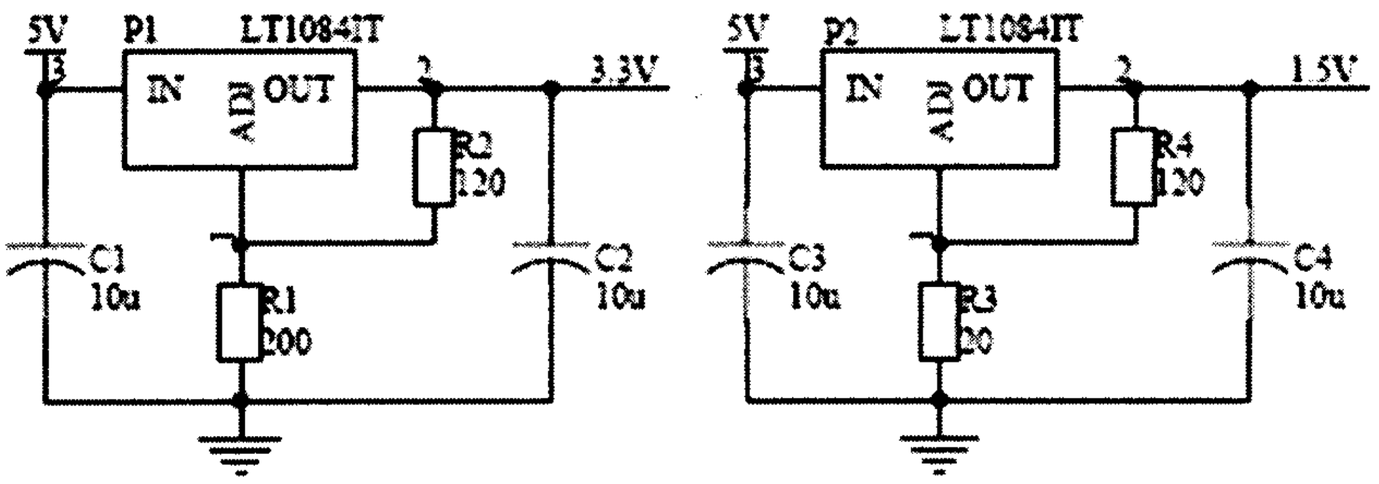

图4 电源系统原理图

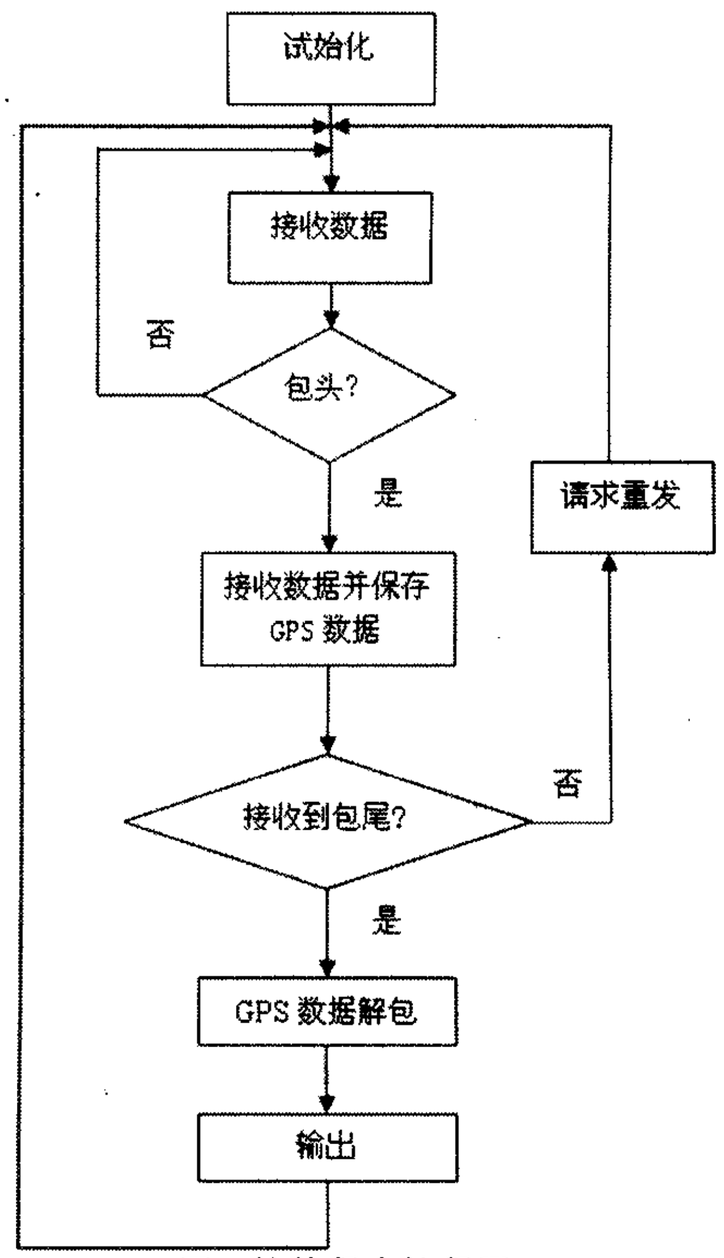

图2 软件程序流程图

匿名通信技术概述

刘益 郭华磊 徐一兵
（西安通信学院 陕西西安 710106）

摘 要：本文从不同角度对匿名技术进行分类综述，阐述了匿名通信的研究意义，对比分析了目前现有的不同匿名方法的优缺点，最后指出了匿名通信技术未来的研究方向。

关键词：匿名通信 混淆网络 洋葱路由 P2P
中图分类号：TP393 **文献标识码**：A **文章编号**：1672-3791(2007)11(b)-0092-02

1 引言

Internet网络应用的普及使用使得人们越来越关注网络的安全性，网络通信的安全性通常指网络通信的完整性、真实性、机密性、可用性和可控性，它们解决的仅是传输的信息的安全性问题，而对通信双方无保密措施，匿名性则考虑到通信的发送者和接受者也是秘密信息的情况，因此，它也被认为是安全性之一。

2 匿名通信技术的概念及其应用

匿名通信指采取一定的措施隐蔽通信流中的通信关系，使窃听者难以获取或推知通信双方的关系及内容。匿名通信的目的就是隐蔽通信双方的身份或通信关系，保护网络用户的个人通信隐私[1]。

匿名通信技术的应用领域非常广阔，它可以应用在电子现金，匿名电子邮件，网上选举(选民投票要求是匿名的)，电子拍卖(竞拍者保持匿名)，网上心理咨询(心理咨询者身份匿名)等客观要求保护用户信息的领域[2]。

3 匿名技术的分类及分析

3.1 按照代理的类型分类

按照代理的类型可以分为基于简单代理的匿名通信和基于串行代理的匿名通信。

3.1.1 基于简单代理的匿名通信系统

基于简单代理的匿名通信系统的特点就是在发送者和接收者之间只有一个中心转发代理，客户机与服务器之间的全部通信经过代理转发，服务器能觉察的也仅是代理。因此，对服务器而言，客户机达到了发送者匿名。

Anonymizer就是这样一个匿名通信系统。提供匿名的Web访问服务，它使用Anonymizer服务器的地址代替传送信息的认证头以及源地址。这样，Web服务器只能知道Anonymizer服务器的地址而不知道用户的真实地址。此处，重路由路径的唯一中间节点就是Anonymizer服务器。

单代理匿名技术简单、易用，但其信息过于集中，服务器与客户机之间的通信都由代理来转发，因此，代理具有系统中所有通信信息，一旦代理被攻陷，系统中所有信息都将暴露。

3.1.2 基于串行代理的匿名通信

基于串行代理的匿名通信解决了简单代理中的单一代理被攻陷而导致的信息暴露问题。它的特点是发送者与接受者之间存在若干串行转发代理，因此，只要代理不被全部攻陷，信息的安全性还是可以得到保障的。它的典型代表技术就是洋葱路由技术以及David Chaum的电子邮件不可追踪问题。

3.2 按照匿名的对象分类

网络中通信的实体主要包括发送者、接受者、信息传输的节点和传输代理这几部分。因此，按照匿名对象可以将匿名通信技术分为发送者匿名、接受者匿名、通信双方匿名、节点匿名和代理匿名。发送者匿名是保护信息发送者的识别信息；接受者匿名是保护信息接受者的身份识别；通信双方匿名是保护信息的发送者和接受者的身份的机密性。节点匿名是保护信息通过的路线上服务器身份的机密性；代理匿名使窃听者无法判断某节点是否是发送者和接受者传输信息的载体。

Chaum 混淆(Mixes)网络[4]就可以对接受者匿名提供很好的解决方案。发送者可以选择n个连续目标进行发送，而其中之一是真正的接受者。窃听者获取真正接受者的概率仅为1/n。在此，为加大窃听者的流量分析，中间节点在传输时进行编码，重排，延迟及填充等手段。

DC—Nets系统主要提供发送者匿名保护。系统运行的每个周期，全部通信参与者都向系统中每个成员发送一个报文，每个成员通过一定的运算操作来获知的内容，但对于发送者的身份却无法判断。

3.3 按照匿名实现机制的方式分类

3.3.1 基于广播的匿名通信系统

DC—Nets系统是最典型的基于广播的匿名通信系统，该系统的基本原理前面已经叙述过。该技术可以通过广播的方式隐蔽发送者的身份，但它还存在着一定缺陷：1)效率低。由于每次发送报文都需要所有成员参与，严重降低了传输的效率。2)冲突问题。假设同一时刻不至一个参与者发出报文，则广播的是所有报文之和，这样将导致所有报文信息的失效。

3.3.2 基于混淆网络的匿名通信系统

1981年David Chaum提出的Mix概念被认为是最可能解决网络中匿名通信问题的方法。现有的如匿名Web浏览的Freedom、匿名电子邮件的Mixmaster系统等匿名通信系统都是基于Chaum的Mix思想。如图1，基于Mix的匿名通信系统由在网络中提供匿名服务的多个Mix节点组成，报文经过多个Mix节点的处理最终到达接收者。每个Mix节点接收一定数量的报文作为输入，对其进行编码变换加密，随机排序后再成批输出。

Mix网络中的强加密机制使得除网络出口节点外的中继节点都无法获知传输内容及最终接收者地址，因而提供了很强的匿名保护措施。但是，它也存在一定不足：1) 系统中对被动的能观测所有网络流量的全局观测者缺乏匿名保护。2)针对合谋攻击的预防弱。3) Mix网络中填充流量的引入浪费大量带宽。

基于Mix网络的以上缺陷，1993年C. Park等提出了用ElGamal公钥体制加密实现的Mixes net方法，该方法固定密文长度，使之与Mixes服务器的个数无关。现在Mixes net的研究主要包括三个方面，一是Mixes net可信度的提高，Mixes net由多个服务器组成，并且其中一半以上的服务器可信，从而保证Mix网络的正确性和保密性；二是使Mix网络具有可验证性；三是使用恰当的协议和算法减少Mixes net 通信量和计算量。

3.3.3 洋葱路由技术(Onion Routing，简称OR)

洋葱路由技术[5][6]是1996年由Goldschlag、Syverson 和Reed[2][3]共同提出的。它是一种基于多次混淆方法提出的新的匿名通信技术，可以实现发送者和接受者匿名。