射频网络与GPRS通信的可靠性与安全性设计

孟凡勇，孟立凡

（中北大学 电子测试技术国家重点实验室，太原 030051）

摘要：提出了一种基于nRF905与GPRS的远距离无线传输系统的设计方案，重点介绍系统通信协议的设计，成功解决了射频网络中的冲突检测、隐藏节点、差错控制及重发等问题，并在分析GPRS数据安全性因素的基础上给出了解决方案，保证了系统的可靠性与安全性。本系统设计的通信协议对其他无线通信系统的实际工作具有一定的参考和借鉴意义。

关键词：射频网络；nRF905；GPRS；通信协议；可靠性；安全性

中图分类号：TN923　　**文献标识码**：A

Transmission Reliability and Security Design Based on RF Network and GPRS

Meng Fanyong, Meng Lifan

(National Key Laboratory of Electronic Measurement Technology, North University of China, Taiyuan 030051, China)

Abstract: The paper presents a design scheme of remote radio transmission system based on nRF905 and GPRS. Communication protocols are introduced. The problems of conflict detection, hide node, error control and resend policy in RF network are solved. Based on the analysis of GPRS safety factors, the paper gives a solution scheme to ensure system reliability and security. The system communication protocols are of reference significance for actual practice of other radio transmission systems.

Key words: RF network; nRF905; GPRS; communication protocol; reliability; security

与有线技术的可靠稳定相比，无线技术在一些地理条件复杂、线路架设困难的场合显出了优势。工作在免许可证的ISM频段射频通信，由于其成本低、安装方便、功耗低等优点，已经被广泛应用于汽车电子、安全认证、智能传感网络、数据传输控制等方面[1]。良好的通信协议设计是无线系统可靠通信的前提，因GPRS传输是基于TCP/IP的网络传输，需要利用Internet来完成通信任务，在享受低成本无线通信技术的同时，系统的安全性也面临一些威胁。

1　远程无线传输系统设计方案

1.1　系统通信层次结构设计

多数的射频技术只适合短距离的通信，在要求远距离通信时常采用中继的办法，无形中增加了系统的硬件成本及软件设计难度。基于以上问题，本系统将射频通信与适合远距离无线传输的GPRS技术进行融合，提出一种适合于远距离传输的无线通信系统。本系统采用的是2层通信结构设计：射频通信部分与GPRS通信部分。底层多个51单片机（含射频芯片）构成无线传感网络数据采集节点，并将采集的数据信息传送给基站。基站设有的GPRS DTU无线接入Internet，进一步将底层的数据及报警信息传送给远程监测服务器（PC机），或用短消息传送给手机终端。

1.2　系统的拓扑结构设计

考虑到系统的性能、可靠性及功耗，底层射频通信网络要选择合适的拓扑结构。这也是无线通信协议设计的基础。目前在无线领域中应用广泛的拓扑结构有星型网络结构、网状拓扑结构、星-网混合结构。本系统采用星型网络。星型网络是一个单跳系统，网络中所有无线节点都与基站进行双向通信，各节点间并不通信[2-3]。星型网络较其他2种网络具有整体功耗最低、容易移动、易于扩展等优点，但是节点与基站间的通信距离取决于单个节点的无线信号覆盖范围。由于本系统设计的初衷是为温室环境数据采集而设计，环境面积不大，完全在nRF905的通信范围内，所以采用星型网络最为实用。图1给出了系统的整体结构框架。

1.3　关键器件选型

本设计中，基站的控制器选用S3C44B0X芯片，它是基于ARM7TDMI内核的32位高速处理器，具有高性能、高实时性、低功耗、同比价格低等特点。GPRS模块选用华为公司的GTM900-C，内嵌TCP/IP、PPP拨号协议，节省了开发时间。加上通用的RS-232接口和丰富的AT指令集，就可以完成可靠的数据通信。射频模块选用

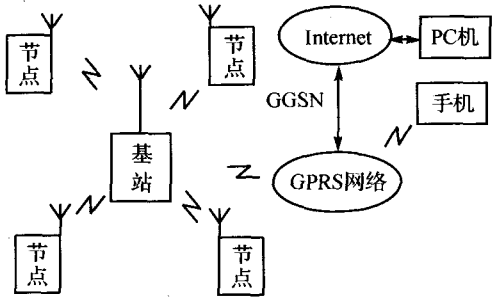

图 1 系统架构示意图

nRF905 模块，采用 SPI 总线与微控制器通信，有 2 种工作模式（发送模式与接收模式）和 2 种节能模式（掉电模式和待机模式）。它可以工作在免许可证的 433/868/915 MHz 开放 ISM 频段；最高工作速率为 50 kb/s，高效 GFSK调制，抗干扰能力强；多频道技术，满足多点通信与跳频的通信需要；内置硬件 CRC 检错（循环冗余码校验），发送/接收方式均有载波匹配和地址匹配检测，可靠性强；低功耗，1.9～3.6 V 工作，待机模式下状态仅为 2.5 μA。

2 射频网络的通信协议设计

系统主体是由 1 个基站和多个节点（从站）构成的数据通信网络。这是一种多点对点的通信模式，从站和基站之间进行有效的、协调的无线通信，需要采取相应的措施来实现。另外，对于通信中可能出现的数据错误，需要采取相应措施来预防与纠正[4]。

2.1 节点多址接入设计（介质访问控制）

该射频网络是多点对 1 点的通信系统，首先要解决的是通信中节点多址接入冲突的问题。为保证射频网络通信的畅通，要求各节点在网络中有唯一的地址，并且在 1 个时刻只允许有 1 个节点和基站进行点对点的通信，所以该系统是点对点通信系统的延伸。

本文借鉴了随机竞争协议中适合无线通信网络的 CSMA/CA（载波侦听多点接入/冲突避免）协议来解决多址接入的问题。具体实现为：在节点欲与基站通信前，先进行载波检测，当检测到信道忙时，重新检测，当检测到信道空闲时并不立即发送数据，而是通过“二进制指数退避算法”随机延迟一段退避时间，若信道仍空闲则发送数据，因为此时可能有多个节点正在等待频道空闲，易于发生冲突。由于每个节点采用的随机时间不同，这样能将冲突发生的概率降到最低[5]。

2.2 隐藏节点问题

隐藏节点是关系无线网络性能的重要问题，它是由于节点通信距离有限而产生的。如图 2 所示，各虚线圈代表各自节点的信号辐射范围，A、B 节点均在基站的信号范围内，所以 A、B 均可以与基站进行通信。若某时刻 A 节点正向基站传送数据，由于 A 节点在 B 节点的信号辐射范围之外，B 节点检测不到 A 节点正在与基站进行通信，误认为信道空闲，也向基站发送数据，于是 A、B 节点发送的数据就在基站接收时发生了冲突。隐藏节点会造成系统时隙资源的无序争用和浪费，增加数据碰撞的概率，严重影响网络的吞吐量，增大了数据传输延迟。

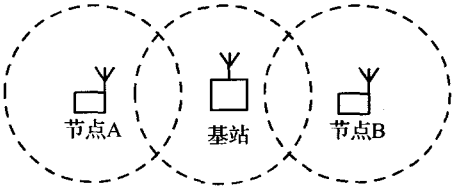

图 2 隐藏节点示意图

本文解决隐藏节点问题借鉴了 IEEE 802.11 协议中关于隐藏节点的解决办法，即在整个通信过程中采用握手信号。本系统在节点与基站的 1 个通信周期过程中设置如下握手机制[6]：

RTS，请求发送命令帧。当节点有数据向基站发送时，先通过竞争的方法获得信道使用权，然后向基站发送 RTS 命令帧，请求与基站连接。

CTS，允许发送命令帧。基站收到 1 个节点的 RTS 请求后，若此时没有其他节点与其通信，则向该节点发送 CTS 命令帧，通知对方发送数据。

DATA，欲发送的数据帧。若节点收到基站发送的 CTS 后，开始向基站发送数据帧；若节点在规定时间内没有收到 CTS 信号则认为发生冲突，重新发送 RTS 信号。

ACK，接收确认帧。基站收 DATA 帧完毕后便向对方节点发送 ACK 帧告知其发送的数据已经收妥，使节点进行下一周期的通信过程。

握手机制有效解决了隐藏节点问题。

2.3 射频通信网络帧结构设计

帧结构规定了数据通信的格式，是网络通信的基本单元。本系统为星型系统，各节点只能与基站通信，互相之间不能通信。根据系统数据信息的类型将帧类型分为握手命令帧（RTS/CTS/ACK）与有效数据帧（DATA），下面将分别介绍。

握手命令帧结构如下：

帧头	节点地址号	基站地址号	帧类型	命令码	频道序号	帧尾	CRC校验码

帧头：用于防止后面的有用数据被干扰。在数据收发过程中，有时由于硬件来不及处理数据，会造成数据的开始几位错误，所以必须加上帧头。nRF905 在收发模式下会自动处理字头，所以帧头可以不必自己设计，本文将帧

头部分省去。

节点地址号：欲与基站通信连接的节点的地址代号，基站根据此地址号从节点地址数组中判断节点地址。本系统应用环境为面积不大的温室，所以设为 2 字节，序号范围为 0～255，系统可以根据自身容量进行扩展。

基站地址号。本文主要研究的是温室网路，其基站地址是唯一的，如果是大型的温室群监测系统，基站地址可以扩展，这里设为 2 字节，序号范围为 0～255。

帧类型。握手命令帧用 0xFA 表示，数据帧用 0xFB 表示，占 1 字节。

命令码：表明该帧发送的是什么握手信号，占 1 字节。RTS 信号用 0xEF 表示，CTS 信号用 0xFE 表示，ACK 信号用 0xBF 表示。

频道序号：用于跳频通信，该序号作为 DATA 帧频道数组中的索引，本系统采用 433 MHz 频段中的 4 个频道进行通信，其中 3 个频道用于 DATA 帧通信，所以占 3 位即可满足要求。

帧尾：帧结束标志，用 0xFF 表示。

CRC 校验码：循环冗余校验，本系统为 8 位校验，由 nRF905 自动完成。

数据(DATA)帧的结构如下所示：

帧头	节点地址号	基站地址号	帧类型	顺序位	重组位	有效数据帧	帧尾	CRC 校验码

其中，帧头与 CRC 校验码由 nRF905 自动完成，节点与基站地址号、帧类型、帧尾设置与握手命令帧结构相同。下面对不同设计部分进行说明。

顺序位：用于标志发送有效数据帧的先后顺序，避免 1 个数据帧重复被基站收到，也方便有效数据帧重组。因为 nRF905 一次最多能发送 32 字节数据，所以当节点欲发送的有效数据较多时，需要分拆后发送，基站接收后将有效数据帧重组。顺序位只需占用 1 位，0 与 1 交替填充。

重组位：表示数据帧是否还有后续帧，占用 1 位，1 表示还有后续帧，0 表示为 1 条信息的最后 1 帧。

2.4 差错重传与跳频机制设计

本系统配置 nRF905 为 8 位 CRC 校验，发送数据前 CRC 校验字节的生成及接收后对数据的 CRC 校验均由 nRF905 硬件自动完成。如果传输过程中数据因干扰出错，基站接收后会因为校验错误而丢弃数据，不会向节点回传 ACK 应答信息。针对这一问题，本系统采用了数据重发机制。节点在设置的时间内收不到 ACK 应答信息，则认为传送数据失败，进行重发。系统最高重发次数为 3，若发送 3 次数据帧仍不能接收到基站的 ACK 应答帧，则放弃本次通信，并在下次通信过程中进行跳频通信。

环境中有与系统通信频道相同或相近的电磁波时，可能会产生干扰，增大系统通信误码率。由于干扰在一定时间内只存于某个频道，采用跳频机制可以很好地解决这一问题。nRF905 可以工作在 433/868/915 MHz 三个频段，每个频段又提供了 2^9 个频道，相邻频道相差 0.1 MHz，并且在 SPI 串行接口指令中 nRF905 为实现快速跳频提供了 2 字节专门指令 CC(CHANNEL－CONFIG)，格式如下[7]：

1000(4 位)	PA_PWR(2 位)	HFREQ_PLL(1 位)	CH_NO(9 位)

nRF905 的工作频道计算公式为

$$f=(422.4+(CH\_NO/10))\times(1+HFREQ\_PLL)\ MHz$$

本系统 HFREQ_PLL 取 0，工作于 433 MHz 频段，由公式可知该频段范围为 422.4～473.5 MHz。系统采用其中的 430/450/460/470 MHz 四个频道，对应 CH_NO 取值为 76/276/376/476。其中频道 430MHz 用于传输 RTS/CTS 握手信息帧，450/460/470 MHz 三个频道用于传输 DATA 帧及 ACK 应答帧。基站接收到节点发送的 RTS 请求帧中包含频道序号信息，向节点回发 CTS 应答帧后基站便跳入 RTS 帧中指定的频道，等待数据的到来。节点收到 CTS 帧后也跳入相应频道，然后向基站传送数据。如果节点没有收到基站的 ACK 确认帧，则在当前频道重新发送数据。若发送 3 次基站均无应答，则节点放弃此次通信，并在下个通信周期修改 RTS 帧中的频道序号，进行跳频。频道序号修改按照双方约定好的 450 MHz→460 MHz→470 MHz→450 MHz 频道顺序进行跳转。

3 GPRS 与 Internet 连接的安全隐患

GPRS 网络接入系统在建设初期就考虑到应该适应未来各种业务的发展需要，具有良好的适应性和可扩展性，从而成为能承载多种业务的平台。其中对通信的安全性也有一些策略。GPRS 通信系统的安全策略主要包括防止非授权的服务使用、使用身份验证和数据加密技术，使移动用户终端能够安全方便地进行数据传输。在 GPRS 综合接入系统网络中，只要用户妥善保管自己的 SIM 卡(防止 SIM 卡被复制和盗用)，并且 GPRS 综合接入系统网络管理完善，用户的个人信息和数据的安全就可以受到很好的保护[8]。虽然 GPRS 自身有很好的安全性，但当 GPRS 与易受攻击的 Internet 网络互联时，将会受到外部网络的安全威胁。Internet 的安全隐患主要包括网络安全性(非法用户侵入服务器)和信息交换安全性(窃取或篡改数据信息)[9]。

4 GPRS 通信的安全性策略

GPRS 若想通过 Internet 安全传送数据，光靠自身的

安全机制还不够，针对 Internet 的安全威胁必须采取有效的安全机制。因为 GPRS DTU 作为客户端，只对已知的 IP(或域名)发起连接，除非在域名方式下域名解析受到攻击，否则 GPRS DTU 不会和非法的服务器发生 TCP 连接。所以，GPRS DTU 基本上不会遭到攻击。而后台服务器是通过实体物理通道与 Internet 连接的，所以其收到攻击的可能性较大。本系统针对以上问题提出了一种简单实用的安全机制方案。

4.1 数据 DES 算法加密及握手机制

为了防止冒充 GPRS DTU 发起连接并向服务器发送伪造的数据以及窃取数据，本系统为双方通信设置了握手协议，并采用对称密码体制的 DES 算法对握手信息进行加密。

首先，服务器侦听网络，当侦听到 GPRS DTU 发起建立连接后，便向 GPRS DTU 发送确认帧进行握手，其实质是包含服务器 IP 地址及服务端口号信息的经 DES 算法加密的密文。GPRS DTU 经之前双方约定的密钥解密后还原得到服务器 IP 及地址信息，并判断是否为目标服务器，判断正确则向服务器发送应答帧确认握手，其实质是包含 SIM 卡序列号及手机号信息且经 DES 算法加密的密文。服务器解密后判断其合法性，如果合法则双方握手成功，服务器发送 1 个启用命令，GPRS DTU 收到后便可以进行数据收发，数据均需 DES 算法加密。如果是非法的 DTU 响应，服务器断开其 TCP 连接。本系统的初衷是为温室监控而设计，系统较小且数据量也不大，采用 DES 算法加密及握手机制便能很好地保证系统的通信安全。

4.2 VPN 专线及防火墙技术

对于企业用户，如果要求系统数据安全性极高，可以采用 VPN 专线(虚拟专用网络)。VPN 的核心就是利用公共 Internet 网络建立一个临时、安全、稳定的连接。VPN 主要采用隧道技术、加解密技术、密钥管理技术和使用者与设备身份认证技术[10]。目前国内外硬件 VPN 产品已经相对比较成熟了，并且费用不高，对企业用户来说性价比极高。

为进一步提高企业内网的安全性，防止非法入侵，可以在外网与企业内网之间安装防火墙。防火墙的具体实现形式有 IP 过滤器、安全 IP 隧道、代理服务器、Socks 服务器 4 种。本系统可以采用 IP 过滤器形式的防火墙，它能够对 Internet 和内网之间的 IP 数据包进行通/断控制。根据服务器及 GPRS DTU 之间的 IP 数据包的收发方 IP 地址、TCP 端口号、流动方向来决定 IP 数据包的通过或丢弃。ME

参考文献

[1] 郝研娜. 基于 MCU 和 nRF905 的低功耗远距离无线传输系统[J]. 电子技术应用，2007(8)：44－47.

[2] 曹世超. 基于射频技术的分布式无线监测系统的设计与实现[D]. 重庆：重庆大学，2009.

[3] 周秋石. 无线局域网络节点模块的研究与初步实现[D]. 大连：大连交通大学，2008.

[4] 闻蔷. 低成本无线工业传感网络的开发与实现[D]. 上海：上海交通大学，2009.

[5] 金保华. 基于 nRF905 的无线数据多点跳传通信系统[J]. 仪表技术及传感器，2004(9)：39－40.

[6] IEEE 802.11 协议[OL]. [2010－03]. http://zh.wikipedia.org/wiki/IEEE_802.11n#IEEE_802.11n.

[7] Nordic 公司. nRF905 Product Specification.

[8] 郑有泉. GPRS 网络的安全性能[J]. 现代电信科技，2000(12)：7－9.

[9] 徐琪，冯锋. 基于包过滤技术的 Internet 安全性研究[J]. 宁夏大学学报：自然科学版，2000，21(4)：329－331.

[10] 向旭宇. Internet 安全性与开放性浅析[J]. 湖南理工学院学报：自然科学版，2005，18(3)：30－33.

孟凡勇(硕士研究生)，研究方向为嵌入式技术、无线通信技术。

(收稿日期：2010-04-12)

第二届“时代民芯”杯电子设计大赛乘帆启航

为鼓励国内电子工程设计人员发展和强化开发、应用能力，提高创新积极性，加强勇于实践的科学精神，北京时代民芯科技有限公司在成功举办了首届 8 位 MCU 电子设计大赛的基础上，于 2010 年 6 月启动了以公司自主研发的 32 位 SPARC V8 架构 MCU 为大赛产品的第二届“时代民芯”杯电子设计大赛，向世界展示卓越的微处理器产品。

“时代民芯”杯电子设计大赛作为面向国内电子工程设计人员的科技型竞赛活动，旨在探索自主产品营销模式、拓展自主产品应用范围、提升公司品牌知名度。第二届设计大赛以“智能中国”为口号，继承第一届大赛提倡创新、拓展自主产品应用领域、激励应用开发人才、促进行业发展的宗旨，围绕“创新、应用”，采取开放式命题方式，为参赛选手提供极大的发挥空间，意在培养参赛选手的创新能力、协作精神和工程实践素质，提高参赛选手针对实际问题进行设计制作的能力以及对应用系统的理解和设计能力，鼓励国内电子工程设计人员在嵌入式设计技术领域的创新应用，推动他们不断发挥创意，设计出智能、新颖、实用又可靠的应用产品。