(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110012447 A
(43)申请公布日 2019.07.12

(21)申请号 201910348217.4

(22)申请日 2019.04.28

(71)申请人 国网新疆电力有限公司
地址 830063 新疆维吾尔自治区乌鲁木齐市水磨沟区南湖东路68号
申请人 上海泽鑫电力科技股份有限公司

(72)发明人 崔大林 庄红山 王晓飞 于冰 张丽 倪宏坤 杨斌 尹浙洪 沈秀兵

(74)专利代理机构 上海智信专利代理有限公司 31002
代理人 王洁 郑暄

(51)Int.Cl.
H04W 4/38(2018.01)
H04W 12/02(2009.01)
H04W 12/04(2009.01)

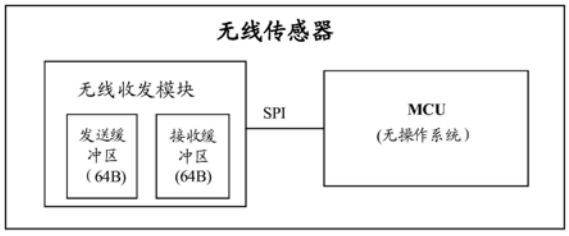
权利要求书2页 说明书7页 附图1页

(54)发明名称

变电站内基于无线传感器实现网络安全控制功能的系统及方法

(57)摘要

本发明涉及一种变电站内基于无线传感器实现网络安全控制功能的系统,包括无线传感器和无线数据采集终端,所述的无线传感器和无线数据采集终端均为无中继节点的星型网络结构。本发明还涉及一种变电站内基于无线传感器实现网络安全控制功能的方法。采用了本发明的变电站内基于无线传感器实现网络安全控制功能的系统及方法,充分考虑了无线传感器微功率运行的特点,系统地设计了网络安全的控制管理。在于密钥的管理是基于MCU的唯一编码由软件自动生成,并且只能由烧写工具读取,每一个传感器有独立的密钥,无需密钥生成器,快捷方便,安全,成本低廉,无额外的功耗。



CN 110012447 A

1.一种变电站内基于无线传感器实现网络安全控制功能的系统,其特征在于,所述的系统包括无线传感器和无线数据采集终端,所述的无线传感器和无线数据采集终端均为无中继节点的星型网络结构,所述的无线传感器用于传输无线信号,所述的无线数据采集终端用于接收和处理无线传感器发送的信号。

2.根据权利要求1所述的变电站内基于无线传感器实现网络安全控制功能的系统,其特征在于,所述的无线传感器包括:

第一微控制单元,用于对通信资源进行管理和控制;

第一无线收发模块,与所述的第一微控制单元通过串行外设接口相连接,用于对无线信号进行收发。

3.根据权利要求1所述的变电站内基于无线传感器实现网络安全控制功能的系统,其特征在于,所述的无线数据采集终端包括:

第二微控制单元,用于对通信资源进行管理和控制;

第二无线收发模块,与所述的第二微控制单元通过串行外设接口相连接,用于对无线信号进行收发;

第二串口收发模块,与所述的第二微控制单元通过串行外设接口相连接,用于通过串口收发信号。

4.根据权利要求2所述的变电站内基于无线传感器实现网络安全控制功能的系统,其特征在于,所述的第一无线收发模块包括第一无线收发发送缓冲区和第一无线收发接收缓冲区,均与所述的第一微控制单元相连接。

5.根据权利要求3所述的变电站内基于无线传感器实现网络安全控制功能的系统,其特征在于,所述的第二无线收发模块包括第二无线收发发送缓冲区和第二无线收发接收缓冲区,均与所述的第二微控制单元相连接。

6.根据权利要求3所述的变电站内基于无线传感器实现网络安全控制功能的系统,其特征在于,所述的第二串口收发模块包括第二串口收发发送缓冲区和第二串口收发接收缓冲区,均与所述的第二微控制单元相连接。

7.根据权利要求4所述的变电站内基于无线传感器实现网络安全控制功能的系统,其特征在于,所述的第一无线收发发送缓冲区和第一无线收发接收缓冲区最大为64字节。

8.根据权利要求5所述的变电站内基于无线传感器实现网络安全控制功能的系统,其特征在于,所述的第二无线收发发送缓冲区和第二无线收发接收缓冲区最大为64字节。

9.根据权利要求5所述的变电站内基于无线传感器实现网络安全控制功能的系统,其特征在于,所述的第二串口收发发送缓冲区和第二串口收发接收缓冲区最大为255字节。

10.一种基于权利要求1所述的系统实现变电站内基于无线传感器的网络安全控制方法,其特征在于,所述的方法包括以下步骤:

(1)所述的无线传感器和无线数据采集终端下装编号密钥和对应的密钥清单;

(2)所述的无线传感器通过自动生成的密钥对收发报文中的应用数据进行加密处理;

(3)所述的无线数据采集终端根据无线传感器的节点编号得到对应的密钥,还原成实际的应用数据;

(4)所述的无线数据采集终端通过其密钥进行加密处理,所述的无线传感器进行数据解密。

11.根据权利要求10所述的实现变电站内基于无线传感器的网络安全控制方法，其特征在于，所述的步骤(2)和步骤(4)中进行数据加密，具体为：

根据以下公式数据加密：

TDATA[n]＝DATA[n]+PKey[k]+CRC[r]；

其中，TDATA[n]为应用数据加密后的第n个字节位置上的值，DATA[n]为应用数据第n个字节位置上的值，PKey[k]为密钥的第k个字节位置上的值，k为N除以4的余数，r为N除以2的余数，CRC[r]为校验码。

12.根据权利要求10所述的实现变电站内基于无线传感器的网络安全控制方法，其特征在于，所述的步骤(3)和步骤(4)中进行数据解密，具体为：

根据以下公式数据解密：

DATA[n]＝TDATA[n]－PKey[k]－CRC[r]；

其中，TDATA[n]为应用数据加密后的第n个字节位置上的值，DATA[n]为应用数据第n个字节位置上的值，PKey[k]为密钥的第k个字节位置上的值，k为N除以4的余数，r为N除以2的余数，CRC[r]为校验码。

变电站内基于无线传感器实现网络安全控制功能的系统及方法

技术领域

[0001] 本发明涉及物联领域，尤其涉及变电站无线传输领域，具体是指一种变电站内基于无线传感器实现网络安全控制功能的系统及方法。

背景技术

[0002] 随着物联网技术的发展与广泛应用，当前变电站内基于无线微功率无线传感器网络逐渐得到应用。以压板状态监测系统为例，包含压板状态传感器、数据采集终端两部分。压板状态传感器以非电原理实时感知压板状态，数据采集终端实现压板位置传感器发送的小无线信号汇聚接收与处理，并与外部应用系统进行通信。无线传感器网络通常基于ISM频段，如433MHz，2.4GHz，这些频段无需许可证或费用，只需要遵守一定的发射功率(一般低于1W)，并且不要对其它频段造成干扰即可，受到其无线通信及自身节点特征的因素影响，变电站无线传感器网络在实际的运行中面临如下三个网络安全的风险：

[0003] 1)数据传输的私密性低，容易被外部系统监听并解析，造成信息外泄。

[0004] 2)来自于无线通信过程中的信号干扰，攻击者采用频率干扰的方法来破坏传感器节点接收信号，破坏传感器节点和采集终端之间的联系。

[0005] 3)攻击者伪造传感器节点，达到侵入采集终端的目的，并通过采集终端为中继进一步侵入变电站内部通信网络，造成严重的网络安全事故。

发明内容

[0006] 本发明的目的是克服了上述现有技术的缺点，提供了一种满足加密性好、通信能力强、适用范围较为广泛的变电站内基于无线传感器实现网络安全控制功能的系统及方法。

[0007] 为了实现上述目的，本发明的变电站内基于无线传感器实现网络安全控制功能的系统及方法如下：

[0008] 该变电站内基于无线传感器实现网络安全控制功能的系统，其主要特点是，所述的系统包括无线传感器和无线数据采集终端，所述的无线传感器和无线数据采集终端均为无中继节点的星型网络结构，所述的无线传感器用于传输无线信号，所述的无线数据采集终端用于接收和处理无线传感器发送的信号。

[0009] 较佳地，所述的无线传感器包括：

[0010] 第一微控制单元，用于对通信资源进行管理和控制；

[0011] 第一无线收发模块，与所述的第一微控制单元通过串行外设接口相连接，用于对无线信号进行收发。

[0012] 较佳地，所述的无线数据采集终端包括：

[0013] 第二微控制单元，用于对通信资源进行管理和控制；

[0014] 第二无线收发模块，与所述的第二微控制单元通过串行外设接口相连接，用于对

无线信号进行收发；

[0015] 第二串口收发模块，与所述的第二微控制单元通过串行外设接口相连接，用于通过串口收发信号。

[0016] 较佳地，所述的第一无线收发模块包括第一无线收发发送缓冲区和第一无线收发接收缓冲区，均与所述的第一微控制单元相连接。

[0017] 较佳地，所述的第二无线收发模块包括第二无线收发发送缓冲区和第二无线收发接收缓冲区，均与所述的第二微控制单元相连接。

[0018] 较佳地，所述的第二串口收发模块包括第二串口收发发送缓冲区和第二串口收发接收缓冲区，均与所述的第二微控制单元相连接。

[0019] 较佳地，所述的第一无线收发发送缓冲区和第一无线收发接收缓冲区最大为64字节。

[0020] 较佳地，所述的第二无线收发发送缓冲区和第二无线收发接收缓冲区最大为64字节。

[0021] 较佳地，所述的第二串口收发发送缓冲区和第二串口收发接收缓冲区最大为255字节。

[0022] 该基于上述系统变电站内实现基于无线传感器的网络安全控制方法，其主要特点是，所述的方法包括以下步骤：

[0023] (1)所述的无线传感器和无线数据采集终端下装编号密钥和对应的密钥清单；

[0024] (2)所述的无线传感器通过自动生成的密钥对收发报文中的应用数据进行加密处理；

[0025] (3)所述的无线数据采集终端根据无线传感器的节点编号得到对应的密钥，还原成实际的应用数据；

[0026] (4)所述的无线数据采集终端通过其密钥进行加密处理，所述的无线传感器进行数据解密。

[0027] 较佳地，所述的步骤(2)和步骤(4)中进行数据加密，具体为：

[0028] 根据以下公式数据加密：

[0029] TDATA[n]＝DATA[n]+PKey[k]+CRC[r]；

[0030] 其中，TDATA[n]为应用数据加密后的第n个字节位置上的值，DATA[n]为应用数据第n个字节位置上的值，PKey[k]为密钥的第k个字节位置上的值，k为N除以4的余数，r为N除以2的余数。

[0031] 较佳地，所述的步骤(3)和步骤(4)中进行数据解密，具体为：

[0032] 根据以下公式数据解密：

[0033] DATA[n]＝TDATA[n]－PKey[k]－CRC[r]；

[0034] 其中，TDATA[n]为应用数据加密后的第n个字节位置上的值，DATA[n]为应用数据第n个字节位置上的值，PKey[k]为密钥的第k个字节位置上的值，k为N除以4的余数，r为N除以2的余数。

[0035] 采用了本发明的变电站内基于无线传感器实现网络安全控制功能的系统及方法，充分考虑了无线传感器微功率运行的特点，系统地设计了网络安全的控制管理。在于密钥的管理是基于MCU的唯一编码由软件自动生成，并且只能由烧写工具读取，每一个传感器有

独立的密钥，无需密钥生成器，快捷方便，安全，成本低廉，无额外的功耗。将对外通信的模块独立，缓存置于通信模块中，实现了数据的主动处理，有效避免内存溢出攻击。与外部通信用串口通信方案，有效杜绝以太网方式的网络通信接口安全。

附图说明

[0036] 图1为本发明的变电站内基于无线传感器实现网络安全控制功能的系统的无线传感器对外通信硬件结构。

[0037] 图2为本发明的变电站内基于无线传感器实现网络安全控制功能的系统的无线数据采集终端对外通信硬件结构。

具体实施方式

[0038] 为了能够更清楚地描述本发明的技术内容，下面结合具体实施例来进行进一步的描述。

[0039] 本发明的该变电站内基于无线传感器实现网络安全控制功能的系统，其中包括：

[0040] 无线传感器和无线数据采集终端，所述的无线传感器和无线数据采集终端均为无中继节点的星型网络结构，所述的无线传感器用于传输无线信号，所述的无线数据采集终端用于接收和处理无线传感器发送的信号。

[0041] 作为本发明的优选实施方式，所述的无线传感器包括：

[0042] 第一微控制单元，用于对通信资源进行管理和控制；

[0043] 第一无线收发模块，与所述的第一微控制单元通过串行外设接口相连接，用于对无线信号进行收发。

[0044] 作为本发明的优选实施方式，所述的无线数据采集终端包括：

[0045] 第二微控制单元，用于对通信资源进行管理和控制；

[0046] 第二无线收发模块，与所述的第二微控制单元通过串行外设接口相连接，用于对无线信号进行收发；

[0047] 第二串口收发模块，与所述的第二微控制单元通过串行外设接口相连接，用于通过串口收发信号。

[0048] 作为本发明的优选实施方式，所述的第一无线收发模块包括第一无线收发发送缓冲区和第一无线收发接收缓冲区，均与所述的第一微控制单元相连接。

[0049] 作为本发明的优选实施方式，所述的第二无线收发模块包括第二无线收发发送缓冲区和第二无线收发接收缓冲区，均与所述的第二微控制单元相连接。

[0050] 作为本发明的优选实施方式，所述的第二串口收发模块包括第二串口收发发送缓冲区和第二串口收发接收缓冲区，均与所述的第二微控制单元相连接。

[0051] 作为本发明的优选实施方式，所述的第一无线收发发送缓冲区和第一无线收发接收缓冲区最大为64字节。

[0052] 作为本发明的优选实施方式，所述的第二无线收发发送缓冲区和第二无线收发接收缓冲区最大为64字节。

[0053] 作为本发明的优选实施方式，所述的第二串口收发发送缓冲区和第二串口收发接收缓冲区最大为255字节。

[0054] 本发明的该基于上述系统实现变电站内基于无线传感器的网络安全控制方法,其中包括以下步骤:

[0055] (1)所述的无线传感器和无线数据采集终端下装编号密钥和对应的密钥清单;

[0056] (2)所述的无线传感器通过自动生成的密钥对收发报文中的应用数据进行加密处理;

[0057] (3)所述的无线数据采集终端根据无线传感器的节点编号得到对应的密钥,还原成实际的应用数据;

[0058] (4)所述的无线数据采集终端通过其密钥进行加密处理,所述的无线传感器进行数据解密。

[0059] 作为本发明的优选实施方式,所述的步骤(2)和步骤(4)中进行数据加密,具体为:

[0060] 根据以下公式数据加密:

[0061] TDATA[n]=DATA[n]+PKey[k]+CRC[r];

[0062] 其中,TDATA[n]为应用数据加密后的第n个字节位置上的值,DATA[n]为应用数据第n个字节位置上的值,PKey[k]为密钥的第k个字节位置上的值,k为N除以4的余数,r为N除以2的余数。

[0063] 作为本发明的优选实施方式,所述的步骤(3)和步骤(4)中进行数据解密,具体为:

[0064] 根据以下公式数据解密:

[0065] DATA[n]=TDATA[n]-PKey[k]-CRC[r];

[0066] 其中,TDATA[n]为应用数据加密后的第n个字节位置上的值,DATA[n]为应用数据第n个字节位置上的值,PKey[k]为密钥的第k个字节位置上的值,k为N除以4的余数,r为N除以2的余数。

[0067] 本发明的具体实施方式中,充分考虑了变电站无线传感器节点能量受限,通信能力较弱,存储空间较小等特点,并结合实际的工程部署条件、网络安全管理要求,在硬件结构设计、数据传输机制、数据传输加密、对外传输接口及协议限定等多个方面进行了网络安全设计,设计了一套从硬件架构、数据传输机制、数据传输加密、对外传输接口及协议限定开始的一整套较为完备的网络安全解决方法,实现变电站内无线传感器网络安全控制。

[0068] 1、对外通信模块化分离式硬件架构:

[0069] 选用MCU与通信资源各自独立的模块化分离式硬件架构,MCU独立运行,由其对通信资源进行管理和控制,通信资源缓冲区与MCU隔离,避免了溢出性攻击对MCU的渗透,与各通讯模块采用中断通知+缓存读写方式进行数据交换。

[0070] 无线收发数据接收和发送缓冲区位于无线收发模块中,缓冲区最大64字节。通信资源缓冲区与MCU隔离。

[0071] 串口收发数据接收和发送缓冲区位于串口收发模块中,缓冲区最大255字节,通信资源缓冲区与MCU隔离。

[0072] 无线网络覆盖范围控制:选用微功耗无线收发模块,传感器无线传输距离不超过50米,压板状态传感器与数据采集终端采用无中继节点的星型网络结构,传感器就地采集数据采集终端就地接收,有效控制无线传输的范围。

[0073] 2、数据传输加密解密处理:

[0074] 每一个无线传感器、无线数据采集终端在生产时根据mcu内置的生产序列号生成

一个四字节的唯一性密钥，该密钥由软件模块上电运行时生成，并由软件烧录工具读取。

[0075] 先对无线收发的数据定义一种统一的收发数据格式：

[0076]

字节序号	填写内容	填写内容说明
1	5A	每一个报文的起始字节
2	5A	每一个报文的起始字节
3	传感器所属的数据采集终端编号	1~254
4	节点编号	0~254 0 约定为数据采集终端
5	应用数据加密后的第 1 个字节	
…	应用数据加密后的第 N 个字节	N 小于 48
4 + N	crc 校验码高字节	16 位 crc 校验码高字节
5 + N	crc 校验码低字节	16 位 crc 校验码低字节

[0077] 3、数据加解密的流程如下：

[0078] 1)在工程配置时，对无线传感器节点编号，无线数据采集终端下装其采集的无线传感器编号及对应的密钥清单，对传感器下装其归属的无线数据采集终端的密钥。

[0079] 2)无线传感器收发报文时用自动生成的密钥对收发报文中的应用数据的进行加密处理。

[0080] 数据加密的算法如下：

[0081] TDATA[n]＝DATA[n]+PKey[k]+CRC[r]；

[0082] TDATA[n]为应用数据加密后的第n个字节位置上的值；

[0083] DATA[n]为应用数据第n个字节位置上的值；

[0084] PKey[k]为密钥的第k个字节位置上的值；

[0085] k＝N除以4的余数；

[0086] r＝N除以2的余数；

[0087] CRC[r]为2字节的校验码。

[0088] 3)无线数据采集终端收到无线传感器发送的报文后，根据传感器的节点编号找到对应的密钥，然后进行还原成实际的应用数据，数据的解密算法如下：

[0089] DATA[n]＝TDATA[n]－PKey[k]－CRC[r]

[0090] 4)无线数据采集终端在发送数据时用自己的密钥进行加密处理，无线传感器使用无线数据采集终端的进行数据解密。加解密算法同上。

[0091] 4、无线数据采集终端防复制性攻击控制：为防止无线传感器发送的信号被监听后以高频率复制发送对无线数据采集终端进行高频数据攻击，无线传感器发送的数据带发送计数，无线数据采集终端只处理比缓存的发送计数大的数据，否则将直接丢弃。

[0092] 5、无线数据采集终端有线数据输出端口的安全控制：采集终端对外传输采用RS485串口通讯，选用MODBUS通讯协议(RTU)，采集终端不主动对外发送数据，采用外部系统发起读请求，采集终端回复的数据交互模式。以下是采集终端支持的功能情况清单：

[0093]

编号	功能码	功能码说明	支持情况
1	0x01	读取线圈状态(读取压板状态)	支持
2	0x02	读取输入状态	不支持
3	0x03	保持型寄存器读取(读取压板状态和传感器工作电压)	支持
4	0x05	写单一线圈	不支持
5	0x06	写单一寄存器	不支持
6	0x0F	写多线圈	不支持
7	0x10	写多寄存器	不支持

[0094] 传感器一般安装于变电站控制室内,变电站非电力公司人员不能进入,尽量讲无线网络覆盖范围控制在变电站内,可以避免无线信号被外部人员恶意监听。

[0095] 使用串口通讯是一种较为常见的网络安全控制手段。以太网的TCP/IP通讯协议是公开标准,绝大部分的网络攻击基于以太网TCP/IP协议来实现,通过RS485串口通讯,就能有效避免以太网的网络安全威胁。MODBUS是一种通用的工业上的数据交换协议,它是一种服务端控制的协议,服务端可以很好的控制数据的读取范围和读取内容,可以有效控制对外信息输出的范围。

[0096] 本技术方案总的工作流程如下:

[0097] (1)各个无线传感器用烧写器写入运行软件可执行文件;

[0098] (2)各个无线传感器上电,自动运行程序,根据MCU生产序列号自动生成四字节唯一密钥(比如:00460028),该密钥为唯一编码,所有无线传感器都不相同;

[0099] (3)程序烧写器读取各个无线传感器运行内存种4字节密钥;

[0100] (4)无线数据采集终端用软件写入运行软件可执行文件;

[0101] (5)数据采集终端上电,自动运行程序,根据MCU生产序列号自动生成四字节唯一密钥(如:003B0068),该密钥为唯一编码;

[0102] (6)烧写器对各个无线传感器下装其归属的无线数据采集终端的密钥及其节点编号,节点编号从1开始排序,节点编号在所属无线数据采集终端范围内唯一,无线传感器在发送报文时带该编号;

[0103] (7)烧写器对无线数据采集终端下装其采集的所有无线传感器编号及对应的密钥清单;

[0104] (8)无线传感器使用自己的密钥对发送的报文进行加密;

[0105] (9)无线数据采集终端的无线传输模块收到报文后向MCU发送请求处理中断;

[0106] (10)无线数据采集终端MCU读取缓冲区内报文数据,根据报文中的节点编号找到对应的密钥进行解密;

[0107] (11)无线数据采集终端解析数据中的发送计数,与缓存的该无线传感器上一次发送计数进行比较,只处理比缓存的发送计数大的报文;

[0108] (12)无线数据采集终端发送报文前使用自己的密钥对发送的报文进行加密;

[0109] (13)无线传感器的无线传输模块收到报文后向MCU发送请求处理中断;

[0110] (14)无线传感器MCU读取缓冲区内报文数据,用预置的无线数据采集终端密钥解

密,然后进行数据处理;

[0111] (15)外部系统向无线数据采集终端通过RS485串口发送数据读取请求报文(MODBUS协议03或01报文);

[0112] (16)数据采集终端串口模块收到报文后向MCU发送请求处理中断;

[0113] (17)数据采集终端MCU读取串口模块中的缓存数据进行报文过滤处理,仅处理MODBUS协议03或报文;

[0114] (18)数据采集终端MCU根据读取内容请求,组织回复报文写入串口模块缓冲区,并调用串口模块发送接口发送数据。

[0115] 采用了本发明的变电站内基于无线传感器实现网络安全控制功能的系统及方法,充分考虑了无线传感器微功率运行的特点,系统地设计了网络安全的控制管理。在于密钥的管理是基于MCU的唯一编码由软件自动生成,并且只能由烧写工具读取,每一个传感器有独立的密钥,无需密钥生成器,快捷方便,安全,成本低廉,无额外的功耗。将对外通信的模块独立,缓存置于通信模块中,实现了数据的主动处理,有效避免内存溢出攻击。与外部通信用串口通信方案,有效杜绝以太网方式的网络通信接口安全。

[0116] 在此说明书中,本发明已参照其特定的实施例作了描述。但是,很显然仍可以作出各种修改和变换而不背离本发明的精神和范围。因此,说明书和附图应被认为是说明性的而非限制性的。

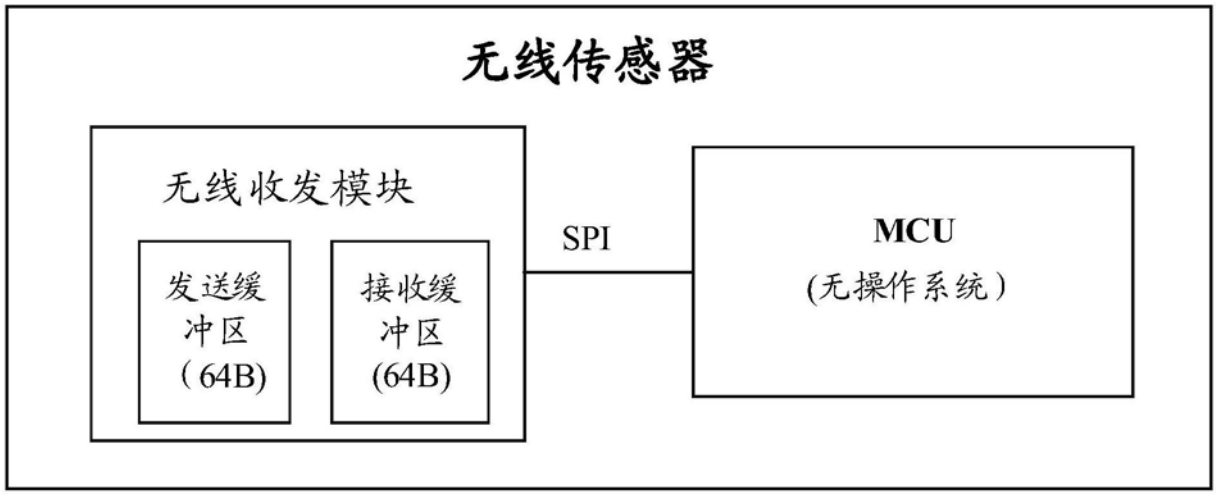

无线传感器
无线收发模块
发送缓冲区（64B）
接收缓冲区(64B)
SPI
MCU
(无操作系统)

图1

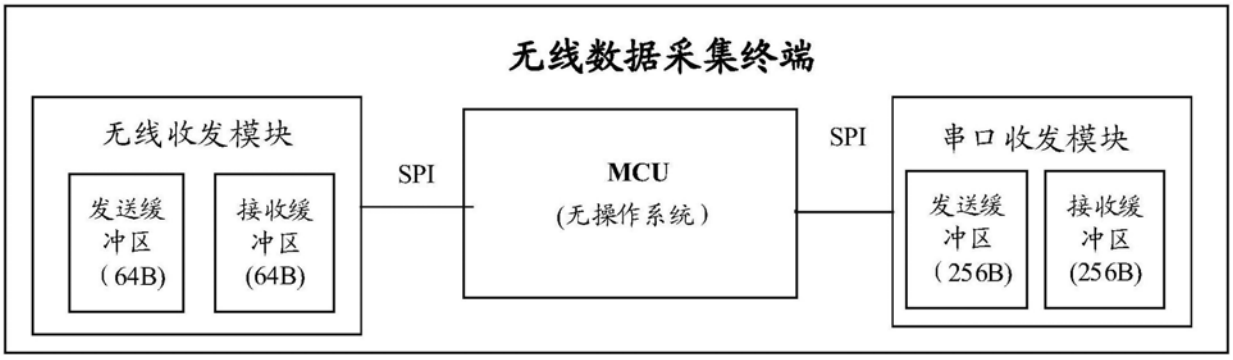

无线数据采集终端
无线收发模块
发送缓冲区（64B）
接收缓冲区(64B)
SPI
MCU
(无操作系统)
SPI
串口收发模块
发送缓冲区（256B）
接收缓冲区(256B)

图2