文章编号:1671-4598(2018)10-0009-05 DOI:10.16526/j.cnki.11—4762/tp.2018.10.003 中图分类号:TP274 文献标识码:A

基于 WSN 的水产养殖环境监测系统设计

唐 逍[1], 陈光化[1,2], 戴庆华[2], 傅志威[1]
(1. 上海大学 机电工程与自动化学院, 上海 200000;
2. 上海大学 微电子研究与开发中心, 上海 200000)

摘要: 针对传统水产养殖过程中对水质监测的实时性差, 测量精度低等问题, 设计基于无线传感器网络的水产养殖环境监测系统; 系统利用 ZigBee 无线通信技术组建传感器网络, 采用混合网拓扑结构, 通过对传感器节点硬件和软件的设计, 完成水产养殖池中的溶解氧含量、PH 值、温度等重要养殖指标的实时测量; 水质数据汇聚到中心节点后传送给主控制器, 并通过 GPRS 上传至云端保存; 另外, 针对云存储的安全问题, 利用同态加密对上传到云端的数据进行加密, 在不破坏云计算能力的前提下保护了用户的隐私数据。

关键词: ZigBee; 无线传感器网络; 水质环境; 云端安全; 同态加密

Design of Aquaculture Monitoring System Based on Wireless Sensor Network

Tang Xiao[1], Chen Guanghua[1,2], Dai Qinghua[2], Fu Zhiwei[1]
(1. School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200000, China;
2. Microelectronic R&D Center, Shanghai University, Shanghai 200000, China)

Abstract: Water quality parameters monitoring in the traditional aquaculture process has the disadvantages of poor real-time performance and poor measurement accuracy. To solve the problems, an aquaculture environmental monitoring system based on wireless sensor network (WSN) is designed. ZigBee wireless communication technology is used to build a sensor network with hybrid topology. Through the design of hardware and software, this system implements the real-time monitoring of water quality parameters, such as dissolved oxygen, pH and water temperature. Water quality parametersare collected to central node, then sent to the main controller, and uploaded to the cloud by GPRS. Furthermore, homomorphic encryption is applied in cloud database to protects users' privacy without disrupting the ability of cloud computing.

Keywords: ZigBee; wireless sensor network; water environment; cloud security; homomorphic encryption

0 引言

水质监测是水产养殖的基本工作, 水质的好坏直接关系到了水产品的产量及品质[1]。传统水质检测的方法主要是依靠人工操作配合仪表和经验进行检测, 不但花费大量精力和时间, 而且存在监测周期长, 监测范围有限等缺点。采用现场总线技术的水质在线监测系统拥有实时性好、监测范围广等特点, 但也存在布线困难、维护拓展不方便、线路易受腐蚀等问题[2]。

近年来, 无线传感器网络 (Wireless Sensor Network, 简称 WSN) 逐渐受到人们重视, WSN 是一种综合了传感器技术、信息处理技术和无线通信等技术的新型信息技术, 传感器节点分撒在目标监测区域后, 通过自组织方式形成网络[3]。无线传感器网络在军事、医疗、工农业、环境监测等方面有着广泛的应用前景[4]。

随着云端服务步入互联网市场, 云端的安全问题逐渐暴露出来[5]。与传统单机存储方式不同, 在云端服务中, 用户对自己的数据的存储位置和状态一无所知, 如果没有对数据进行保护, 就有可能被盗窃或者篡改, 加密是保证数据安全性的一种有效手段, 但是因为数据库自身的特性, 传统的加密手段 (如 AES) 会制约数据库的性能, 浪费云计算的高性能优势。而同态加密[6]能在保证数据保密性的同时使加密后的数据仍能够进行计算。

本文利用 ZigBee 通信技术组建无线传感器网络, 实现对养殖水域中溶解氧含量、pH 值、温度等水质参数的实时采集, 无线传输和远程监测功能。并针对云端数据存储中用户数据的安全性问题, 利用同态加密算法对用户隐私进行加密, 在保障数据安全性的前提下又不破坏云计算的能力。

1 系统整体设计方案

基于无线传感器网络的水质监测系统主要由 ZigBee 无线传感器网络、主控制器、云端数据库组成, 如图 1 所示。

无线传感器网络负责水质数据的采集, 处理和无线传输等工作, 采用混合网拓扑结构, 使用 ZigBee 协议进行数据传输。无线传感器网络主要由终端节点、路由节点和中心节点组成, 终端节点负责采集节点附近水域的溶解氧含量、pH 值、温度等水质数据, 路由节点是即能采集水质数

收稿日期:2018-03-10; **修回日期**:2018-03-28。

作者简介:唐 逍(1993-),男,江苏苏州人,硕士研究生,主要从事嵌入式系统设计与传感器网络方向的研究。
陈光化(1972-),男,湖南长沙人,硕士生导师,副教授,主要从事视频信号处理和嵌入式系统设计方向的研究。

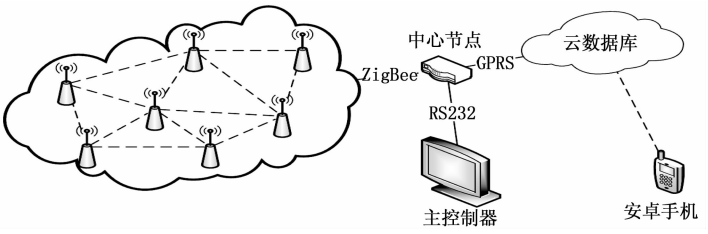

图 1 系统设计框图

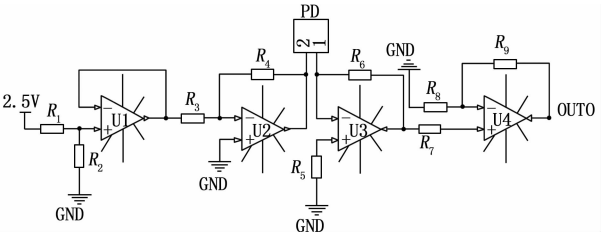

图 3 溶解氧信号调理电路

据，又能进行数据中继路由的节点，采集到的水质数据最终汇聚到中心节点。中心节点将传感器网络上传的数据进行融合后发送给主控制器进行实时显示，同时上传云端存储备份。中心节点采用 SZ11－03ZigBee＋GPRS 网关，此网关能同时使用 ZigBee 和 GPRS 通信，保证了中心节点能够同时与传感器网络和云端进行数据通信。工作人员可以通过主控制器串口屏幕查看实时的水质监测数据，同时当工作人员的位置发生移动时，也能使用安卓手机从云数据库查看水质数据。

2 传感器节点设计

2.1 传感器节点硬件设计

终端节点硬件结构如图 2 所示，主要由传感器模块、微处理器（MCU）模块、ZigBee 通信模块、电源模块组成。由于无线传感器节点采用电池供电，需要保证较长的工作寿命，因此传感器节点的 MCU 采用功耗低，稳定性高的 PIC18F67K22。在无线传输模块选择上采用顺舟科技生产的 SZ05 模块，该模块是基于 ZigBee 技术片上解决方案 CC2630 芯片所开发的，拥有功耗低、抗干扰能力强、组网灵活、网络容量大等特点，该通信模块与 MCU 通过 UART 进行数据传输。传感器模块由水质传感器，信号调理电路和 AD 转换器组成。水质传感器分别测量节点附近水域中溶解氧含量、pH 值和温度等参数。

路由节点即能进行水质参数采集又能进行数据中继路由，因此路由节点的硬件结构设计与终端节点一样。

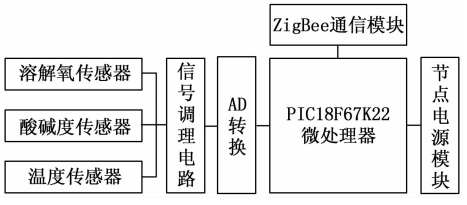

图 2 终端节点硬件结构图

2.2 传感器信号调理电路

2.2.1 溶解氧信号调理电路

溶解氧传感器选用极谱式溶解氧电流传感器[7]，传感器由阴阳两极构成，两极之间用电解液填充，顶端覆盖以聚四氟乙烯薄膜。当给阴阳两极之间施加以 685 mV 的极化电压后，渗透过薄膜的氧分子在电极上产生氧化还原反应，从而产生扩散电流，其信号调理电路如图 3 所示。

左边电路用以产生－685 mV 极化电压，第一级为电压跟随器，2.5 V 输入由高精度电源稳压器产生，经第二级反相后得到－685 mV。右边第一级将电流信号 I 转换为电压信号，第二级放大电压信号，输出电压 V_{OUTO}：

$$V_{OUTO}=\frac{-IR_6(R_8+R_9)}{R_8} \tag{1}$$

2.2.2 pH 信号调理电路

本设计采用电位法测量溶液 pH 值，玻璃电极做指示电极，甘汞电极或银电极做参比电极[8]，其测量原理是当被测溶液的氢离子浓度发生变化时，指示电极和参比电极之间的电动势发生变化。当电位为 0 V 时，表示溶液为中性，即 pH＝7，由于溶液中的 pH 值分布在 0～14 之间，所以输出信号为双极性模拟信号，电压范围大约在－500～500 mV。pH 信号调理电路如图 4 所示，电压信号分别加到 U_1、U_2 的同相端，U_1 和 U_2 为第一级电路，U_3 为第二级电路，这两级均为差分式电路。R_2，R_3，R_4 为第一级电路引入电压串联负反馈，根据“虚断”和“虚短”特征，流过 R_2，R_3，R_4 的电流相等，因此有：

$$u_{o1}-u_{o2}=\left(1+\frac{R_2+R_4}{R_3}\right)(u_{i1}-u_{i2}) \tag{2}$$

第三级 U_3 构成减法电路：

$$u_{o3}=\left(\frac{R'+R'}{R'}\right)\left(\frac{R}{R+R}\right)u_{o2}-\frac{R'}{R'}u_{o1}=u_{o2}-u_{o1} \tag{3}$$

第四级最终输出为：

$$u_{outh}=1-u_{o3}=\left(1+\frac{R_2+R_4}{R_3}\right)(u_{i1}-u_{i2}) \tag{4}$$

至此双极性电压被调节到适合 A/D 转换的范围内。由最终输出公式可知此电路只对输入信号的差进行有效放大，而当输入端出现共模信号时，电压 $u_{o3}=0$。因此，该放大电路具有很高的共模抑制比，能提高信噪比，增强抗干扰能力，使得测量数值更加精确。

2.2.3 温度传感器测量电路

温度传感器选用 pt1000 铂电阻温度传感器，金属铂的电阻值随温度变化而变化，并且具有很好的重现性和稳定性，因此应用范围非常广泛，常见于医疗、电机、工业、温度计算、阻值计算等高精温度设备的应用。按 IEC751 国际标准，pt1000 在 0℃时的标准电阻值为 1000 Ω，电阻变化率为 0.3851 Ω/℃。为了提高测量精度，pt1000 测量电路常采用三线制接法，如图 5 所示。

该电路测量原理是非平衡电桥[9]，铂电阻作为电桥的一个桥臂电阻，将一根导线接到电桥的电源端，其余两根分别接到铂电阻所在的桥臂及与其相邻的桥臂上，要求从

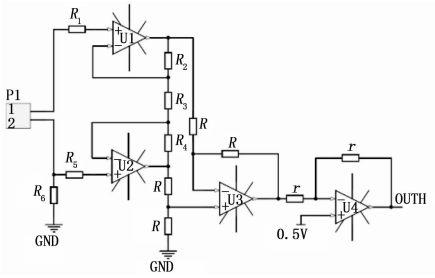

图 4　PH 信号调理电路

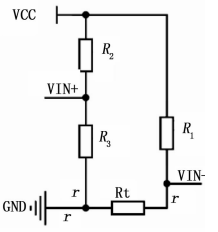

图 5　pt1000 测量电路

铂电阻引出的三根导线截面积和长度相同，设从铂电阻引出的导线电阻为 r。假设 0℃时铂电阻电阻值为 R_t，且桥路平衡，$V_{in+}=V_{in-}$，则：

$$R_t=\frac{R_1R_3+r(R_1-R_2)}{R_2} \tag{5}$$

当 $R_1=R_2$ 时，$R_t=R_3$，此时导线电阻 r 对测量结果的影响降至最低。$V_{in+}=V_{in-}$ 接至 A/D 转换器的模拟量差分输入端，其电压差值为：

$$V_{in+}-V_{in-}=\frac{R_1R_3-R_2(R_t+\Delta_R)}{(R_1+R_t)(R_2+R_3)}V_{CC} \tag{6}$$

当温度升高，铂电阻阻值 $R_t\rightarrow R_t+\Delta R$ 时：

$$V_{in+}-V_{in-}=\frac{R_1R_3-R_2(R_t+\Delta R)}{(R_1+R_t+\Delta_R)(R_2+R_3)}V_{CC}=$$

$$\frac{R_2\Delta R}{(R_1+R_t+\Delta_R)(R_2+R_3)}V_{CC} \tag{7}$$

2.3　传感器节点软件设计

传感器节点主要负责水质数据的采集和无线通信功能，其软件流程如图 6。节点上电后首先进入初始化程序，完成配置和入网工作后进入低功耗休眠状态，当有唤醒事件时，MCU 被唤醒并开始工作。当 MCU 内部看门狗定时器溢出时，节点退出休眠模式，进行溶解氧含量、PH 值和水温参数的采集和发送；当无线模块监听到路由信息时，产生中断唤醒节点进入数据路由转发的流程。

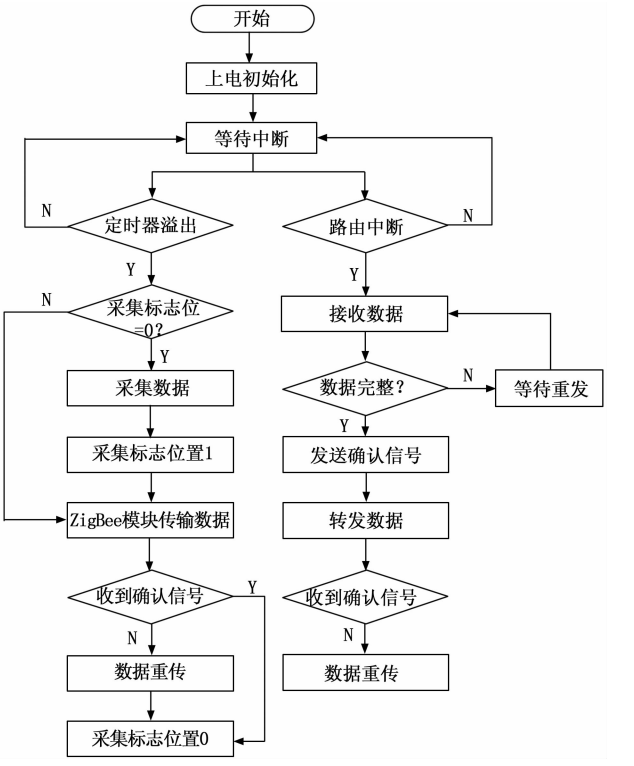

图 6　传感器节点流程图

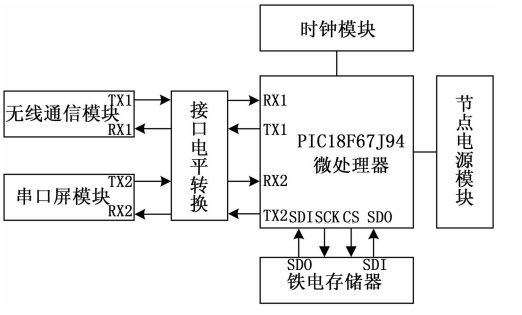

图 7　主控制器硬件结构

3　主控制器设计

3.1　主控制器硬件设计

主控制器其功能主要是通过与串口屏幕的连接，将中心节点接收到的数据进行显示，并能控制养殖池中增氧机和抛食机的工作状态，由处理器模块、无线通信模块、串口屏模块、电源模块等组成。其硬件结构如图 7 所示。MCU 选用 PIC18F67J94，无源晶振为 16 MHz，利用 MCU 内部锁相环电路超频至 64 MHz，为系统提供更高的时钟信号，以获得更快的运行速度。MCU 的工作电压为 3.3 V，设计中采用 BA33BC0FP 稳压器提供稳定的 3.3 V 电压输出。配合 PIC kit3 调试器，可以将程序通过 PGD，PGC 串口直接烧写到芯片内部。为了尽可能多地存储水质数据，增加了一块 FM25CL64B 铁电存储器，容量为 64K，数据以一个字节为单位存储，它与 MCU 通过 SPI 接口进行数据交互。铁电存储器与传统的 EEPROM 器件相比有更长的擦写寿命和更低的功耗，适合用于本设计中需要长期实时监测的水产养殖池。本系统所采用的串口屏显示器为上海久牛科技的 JN08OUT－800600RB3I，采用全双工异步串口与外部设备进行通信，接口电平为 RS232 电平，数据通信时利用 SP3232E 转换成 TTL 电平，软件使用直接变量驱动方式，所有的显示和操作都是基于预先配置好的变量配置文件来工作的，简化了软件架构，降低了二次开发难度。

3.2　主控制器软件设计

中心节点完成 WSN 的组网并将采集到的数据传送给主控制器，同时主控制器也是人机交互的平台，完成水质参数的实时显示、读取云端数据显示历史曲线等功能。其软件设计如图 8 所示。

3.3　安卓端 app 软件设计

设计安卓端 app 的主要目的是当养殖人员不在主控制器附近时，能够通过手机从云端数据库中读取实时水质数据。开发工具 eclipse，编程语言 JAVA，首先需要完成界面的布局设计，代码编程时利用 JTDS/JDBC 中的 Connection

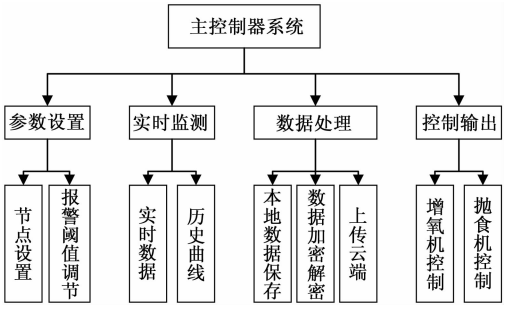

图 8 主控制器软件框图

接口创建手机端与远程数据库的连接，再利用 Statement 接口在已经建立连接的基础上向数据库发送 SQL 语句完成对数据库的操作，其界面如图 9、10 所示。

图 9 app 服务器设置界面

图 10 app 水质数据读取界面

4 实验结果与分析

系统测试过程中有 5 个传感器节点，经自组织方式形成通信网络，水质数据汇聚到中心节点，由串口屏显示数据。节点对同一水域测量 5 次，测量间隔为 20 分钟，取其平均值，结果如表 1 所示。实验结果表明系统能够实时测量水质参数，并且稳定性和测量精度都较高。

表 1 监测结果

节点编号	溶解氧含量/(mg/L)	PH 值	温度/℃
1	10.33	7.2	15.1
2	10.72	7.1	14.9
3	10.08	7.2	15.3
4	10.48	7.3	15.0
5	10.59	7.5	15.0

5 同态加密在云存储平台上的应用

水产养殖涉及经济利益，不同水质状况下鱼类的生长速度不同，用户不会希望自己的养殖数据泄露。在本设计中，水质数据都存储在云端数据库中，但在云端中，数据提供者和云服务提供者这两个角色是分离的[10]，云服务提供者由商业机构承担，这些商业机构对于水产养殖户来说是不可信的，如果用户把数据以明文形式存储在云端，那么云服务商就能利用这些数据为自己牟利，如果用户用传统加密方式将数据加密后以密文形式存储在云端，那么云端仅仅是提供了传输、存储功能，用户无法利用云计算的高计算性能优势。而同态加密提供了一种对加密数据进行处理的功能，其定义[11]如下：

设 $E(K, m)$ 表示用加密算法 E 和密钥 K 对 m 进行加密，F 表示某种运算，若对于加密算法 E 和运算 F，存在运算 G 使得：

$$E(K,F(m_1,m_2,\cdots,m_n)) = G(K,F(E(m_1),E(m_2),\cdots,E(m_n))) \tag{8}$$

就称加密 E 对于运算 F 具有同态性。若用 D_k 表示解密算法，加法同态性和乘法同态性可以分别表示为：

$$\sum_i^n m_i = D_k(E(m_1)+E(m_2)+\cdots+E(m_n))$$

$$\prod_i^n m_i = D_k(E(m_1)\times E(m_2)\times\cdots\times E(m_n))$$

由此可见同态加密能保证云端对密文进行计算操作后解密的结果与用户直接对明文进行计算操作的结果是一样的。

本文所使用的整数环上的同态加密过程描述如下：

1）密钥生成：随机选取两个大素数 P 和 Q（长度大于 512 位），计算 $N=PQ$，并选取一个随机数 R；

2）加密：将明文 M 按固定长度 L（$L<P$）分组，$M=m_1, m_2, \cdots, m_n$，计算密文 $c_i=(m_i+PR)\ mod\ N$，$C=c_1, c_2, \cdots, c_n$；

3）解密：将密文进行分组 $C=c_1, c_2, \cdots, c_n$，对每一组密文使用密钥 P 计算 $m_i=c_i\ mod\ P$，连接明文分组得到完整明文消息 $M=m_1, m_2, \cdots, m_n$。

上述加密算法同时具有加法同态性和乘法同态性，已在文献［12］中证明。现利用大数运算库 Tommath 完成对同态加密算法的本地编程测试。测试环境为个人 PC 端；WIN10 系统；VisualStudio2013 平台；C 语言编程，加密和解密程序流程如图 11 所示，图中（a）为加密流程图，（b）为解密流程图。

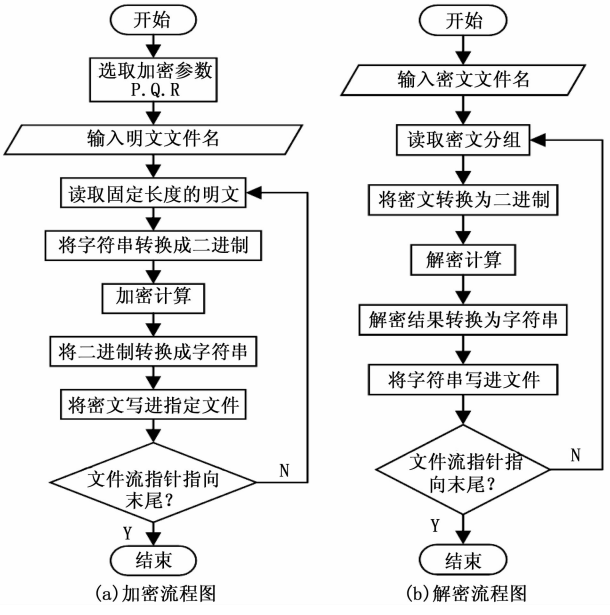

图 11 加密和解密流程图

首先，用户读取本地明文文件，利用文件指针先得到

明文的长度，并根据需要的分组长度 L 对明文进行分组，再将分组字符串转换为二进制写进 mp _ int 类型的大数，然后使用密钥 P、Q、R 对其进行加密操作。

当用户从服务器上获得云计算的密文后根据密文之间的分隔标记进行分组，再将字符串转换成二进制，利用密钥 P 进行解密计算，获得明文的二进制串后再转换成字符串，结果如图 12～15 所示。

图 12　加密算法控制台程序运行时的图像

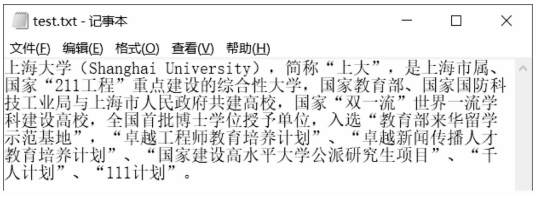

图 13　需要加密的明文

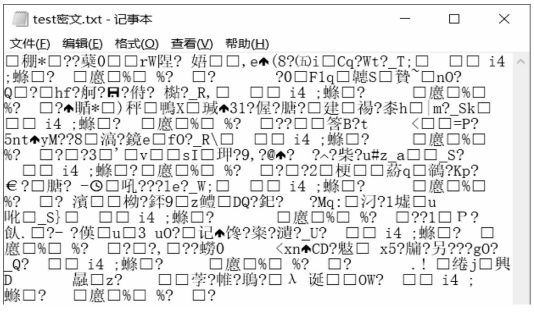

图 14　加密后的密文

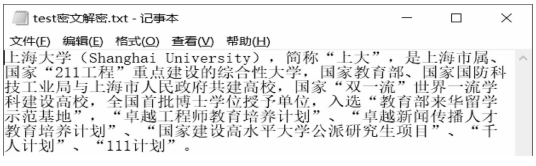

图 15　密文解密后的结果

由结果中可以看出，明文中包含了汉字、数字、符号等字符，解密结果与明文完全一致。加密算法的安全性是基于分解难题的，攻击者想要破解大数 N 只能通过穷举法，而 N 的位数为 512～1 024 bit，这将花费攻击者大量的时间。因此本文应用的同态加密算法能在不破坏云计算可行性的前提下保护用户的隐私。但是该加密算法容易受到选择明文攻击[13]，因此可以采用合适的云端数据访问控制机制[14-15]来避免遭到选择明文攻击。

6　结束语

本文利用 ZigBee 构建无线传感器网络，完成对水产养殖池的水质监测系统设计。该系统中，传感器节点负责采集溶解氧含量，PH 值，水温等水质数据，中心节点收集各节点的监测数据并进行融合，通过 RS232 串口与主控制器进行数据传输，并通过 GPRS 将数据上传至云端保存。主控制器配合串口屏幕完成水质数据的实时监测，设计了安卓手机端 app，保证用户能随时随地了解水质情况。通过该系统监测养殖池塘的水质能有效减少养殖人员的工作量，提高养殖效率。

本文针对云端的数据安全性进行研究，利用同态加密算法保护用户隐私，减少数据泄露所造成的经济损失，为了能够进一步提高云端安全性，下一步将结合访问控制机制与同态加密算法进行探索。

参考文献：

[1] 曾洋泱，匡迎春，沈　岳，等. 水产养殖监控技术研究现状及发展趋势 [J]. 渔业现代化，2013，40 (1)：40－44.

[2] 张　莹，肖令禄. 基于无线传感器网络的水产养殖水质监测系统设计 [J]. 渭南师范学院学报，2016，31 (19)：49－53.

[3] 刘敏钰，吴　泳，伍卫国. 无线传感网络 (WSN) 研究 [J]. 微电子学与计算机，2005，22 (7)：58－61.

[4] 陈　涛，刘景泰，邴志刚. 无线传感网络研究与运用综述 [J]. 总线与网络，2005，7：41－46.

[5] 刘冬兰，史方芳，刘　新，等. 大数据环境下云数据库安全防护方法研究 [J]. 山东电力技术，2017，6 (44)：41－48.

[6] 宋丹劼. 基于同态加密的云存储系统设计与实现 [D]. 北京：北京邮电大学，2013：5－6.

[7] 吕　斌，雷　卓，刘　杰，等. 基于 PIC18F2520 的极谱式溶解氧传感器设计 [J]. 山东科学，2012，25 (4)：73－77.

[8] 王　刚，万其进，叶永康. pH 化学传感器的进展 [J]. 分析科学学报，1999，15 (3)：246－251.

[9] 李　林，徐泽红，吴新全. 应用非平衡电桥测量电阻实验的研究 [J]. 实验技术与管理，2007，24 (3)：31－34.

[10] 洪汉舒，孙知信. 基于云计算的大数据存储安全的研究 [J]. 南京邮电大学学报 (自然科学版)，2014，34 (4)：26－32.

[11] 李顺东，窦家维，王道顺. 同态加密算法及其在云安全中的应用 [J]. 计算机研究与发展，2015，52 (6)：1378－1388.

[12] Li M Y，Li J，Huang C. A credible cloud storage platform based on Homomorphic Encryption [J]. Netinfo Security，2012，9：35－40.

[13] Xiong A P，GAN Q X，He X X. A Searchable Encryptionof CP－ABE Scheme in Cloud Storage [J]. IEEE，2013：345－349.

[14] 周彦萍，马艳东. 基于 CP－ABE 的访问控制研究 [J]. 电子产品世界，2013，8：42－44.

[15] Dai J Z，Luo S Y，Liu H X. A Privacy－preserving access control in outsourced storage services [J]. IEEE，2011：247－251.