文章编号:1671-4598(2017)03-0180-04 DOI:10.16526/j.cnki.11—4762/tp.2017.03.049 中图分类号:TP393 文献标识码:A

面向物联网的 Sybil 入侵防御系统设计与实现

陈 琳,李 勇,王 磊
(新疆轻工职业技术学院 信息与软件分院,乌鲁木齐 830021)

摘要:设计物联网中的 Sybil 入侵防御系统,进行入侵检测,保障物联网的网络安全,针对当前入侵防御系统拦截准确性不好的问题,提出基于网络入侵信号检测和前馈调制滤波设计的物联网 Sybil 入侵防御系统设计方法;首先进行 Sybil 入侵防御系统总体设计描述和功能分析,然后进行 Sybil 入侵信号检测算法设计,最后完成面向物联网的 Sybil 入侵防御系统硬件设计和软件开发,实现系统的集成设计;仿真测试表明,采用该系统进行物联网中的 Sybil 入侵检测的准确度较高,性能较好,具有较强的兼容性和友好性。

关键词:物联网;入侵;检测;防御;网络安全

Design and Implementation of Sybil Intrusion Prevention System Based on Internet of Things

Chen Lin, Li Yong, Wang Lei
(Department of Information and Software, Xinjiang Institute of Light industry Technology, Urumqi 830021, China)

Abstract: Design the Sybil intrusion defense system of Internet of things, intrusion detection, to protect the security of Internet of things network. Aiming at the problem of current intrusion defense system, suchas: the accuracy is not good, proposed a network intrusion signal detection and feedforward modulation filter design of IOT Sybil intrusion defense system design method. First Sybil intrusion defense system overall design description and function analysis, and then the Sybil intrusion signal detection algorithm is designed, the oriented networking Sybil intrusion defense system hardware design and software development, system integration design. Simulation tests show that the system is used in the Internet of things Sybil intrusion detection accuracy is higher, better performance, with strong compatibility and friendly.

Keywords: Internet of things; intrusion; detection; defense; network security

0 引言

随着无线传感器网络通信技术和物联网技术的发展,越来越多的应用环境采用传感器和无线通信设备终端进行数据传输和信息交流,构成大型的物联网通信系统,在物联网组网环境下,由于物联网节点的自组织性和广分布性的特点,容易受到网络的攻击和病毒入侵,特别是 Sybil 入侵表现比较突出,Sybil 入侵是利用物联网感知层和中间层的通信链路漏洞进行病毒入侵,带来网络安全隐患。研究物联网中的 Sybil 入侵下的入侵防御检测问题,提高物联网安全防范能力,在网络安全和物联网组网设计中具有重要的应用价值,相关的入侵防御系统设计方法受到人们的极大重视[1-3]。

对面向物联网的 Sybil 入侵防御和识别是建立在 Sybil 入侵下的信息特征提取和入侵信号检测的基础上,面向物联网的 Sybil 入侵防御系统是利用 Sybil 入侵信号的统计特征和高阶谱聚焦特征,进行信号检测识别,并结合高速数字信号处理芯片进行入侵防御系统的开发和设计,取得一定的研究成果,其中,文献[4]提出一种基于 APD 最佳雪崩增益控制技术的物联网 Sybil 入侵检测系统设计方法,结合 Emulator 硬件开发环境实现对 Sybil 入侵检测识别,对物联网环境下的病毒入侵检测的精度较高,但是该系统设计受到基线漂移的影响容易导致失真,在受到较大强度干扰下对 Sybil 入侵检测的准确度不高;文献[5]提出一种引入偏移量递阶控制的网络入侵 HHT 检测算法,使用 AD 公司一款高性能 A/D 芯片 AD9225 进行面向物联网的 Sybil 入侵防御系统的开发设计,通过 AD 采样得到网络入侵的偏移量特征,进行偏移控制,结合 Hilbert—Huang 变换实现病毒入侵检测,实现网络入侵防御系统优化设计,取得了较好的检测性能,但是该入侵防御系统的计算开销较大,实时性不好[6-7]。针对上述问题,本文提出一种基于网络入侵信号检测和 16 位定点 DSP 内核前馈调制滤波设计的物联网的 Sybil 入侵防御系统设计方法。首先进行 Sybil 入侵防御系统总体设计,然后进行了 Sybil 入侵信号检测算法设计,最后进行了面向物联网的 Sybil 入侵防御系统硬件设计和软件开发,实现系统的集成设计,通过仿真测试进行了性能验证,展示了本文设计的入侵防御系统在入侵检测中的优越性能。

1 系统的总体设计描述与算法设计

1.1 面向物联网的 Sybil 入侵防御系统总体设计

为了实现对面向物联网的 Sybil 入侵防御系统优化设计,首先构建系统的总体结构模型,物联网路由链路层一种典型的 AD Hoc 组网,链路层结构分别可以概括为:RNICODE 和 URI 层、协议堆栈空间层等,其中 RNICODE 和 URI 层构成了物联网的感知层和中间层,在感知层和中间层的链路漏洞中容易产生 Sybil 入侵,面向物联网的 Sybil 入侵防御系统通过网络通信节点实现病毒入侵检测,主要包括了滤波电路模块、主控电路模块、AD 电路模块和检测模块。其中,对病毒入侵

收稿日期:2016-10-13; **修回日期**:2016-11-08。
基金项目:2016 年度新疆维吾尔自治区高校科研计划项目(XJEDU2016I059)。
作者简介:陈 琳(1964-),男,浙江兰溪人,硕士,副教授,主要从事网络安全方向的研究。

检测模块是整个防御系统的核心单元，面向物联网的 Sybil 入侵防御系统采用的是嵌入式系统进行集成芯片开发和信息处理，采用无线通信技术进行数据传输和病毒入侵检测，采用 PCI 总线技术进行数据采集，其时钟频率为 33 MHz 或 66 MHz，采用 32 位或 64 位数据线进行电源供电。物联网网络包括 4 类基本实体对象：目标、观测节点传感节点和感知视场，因此在进行面向物联网的 Sybil 入侵防御系统开发设计中，需要通过配置中间件完成面向物联网的 Sybil 入侵防御系统的各种配置工作，例如路由配置、定位系统配置等[8-10]。在受到网络攻击或者能量消耗终止时，接受中断请求，当硬件装置或软件指令请求中断时，状态寄存器 ST1 中发出中断响应信号/IACK，进行 Sybil 入侵检测，根据上述总体设计思想描述和功能指标分析[11-13]，得到本文设计的面向物联网的 Sybil 入侵防御系统结构框图如图 1 所示。

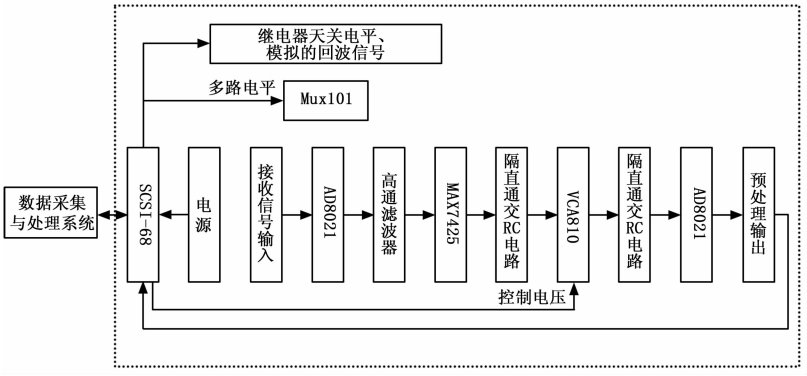

图 1　面向物联网的 Sybil 入侵防御系统结构框图

1.2　Sybil 入侵检测算法设计

在上述构建了面向物联网的 Sybil 入侵防御系统的总体设计结构模型的基础上，进行系统的开发设计，Sybil 入侵防御系统设计包括算法设计、硬件设计和软件设计三大部分[14-15]，在此，首先进行 Sybil 入侵防御系统的算法设计，检测算法在建立在信号处理算法基础上的，通过对 Sybil 入侵信号模型构建，结合信号特征提取和检测算法，进行入侵检测，在物联网环境下，给出 Sybil 入侵的信号模型表达式为：

$$z(t)=s(t)+js(t)\otimes h(t)=s(t)+j\int_{-\infty}^{+\infty}\frac{s(u)}{t-u}\,\mathrm{d}u=s(t)+jH[s(t)] \tag{1}$$

式中，$s(t)$ 称为 Sybil 入侵信号 $z(t)$ 的瞬时幅度，也称为包络；$h(t)$ 称为频域到时域的映射相位，$Z(f)$ 可由 $S(f)$ 通过小波变换得到，$H(f)$ 为 Sybil 入侵信号的局部（或域）平稳长度。Sybil 入侵信号频率分量是一组非平稳随机信号，信号的谱图具有时变性和非线性。假设 Sybil 入侵的短的时间间隔定义为 $v_m, m\in[1,n]$。计算出 Sybil 入侵过程中各个不同时刻的功率谱写作：

$$\tilde{y}(t)=\iint_{v\varphi}b(\tau,\varphi)\exp[j2\pi\varphi t]\tilde{f}(t-\tau)\mathrm{d}t\mathrm{d}\varphi \tag{2}$$

其中：$b(\tau,\varphi)$ 是非平稳扩展函数，$\tilde{f}(t)$ 为窗口附近内的频率分量，τ 为短时 Fourie 时延，φ 为 Sybil 入侵信号随着时间变化的频移特性。假设 Sybil 病毒数据在进行物联网攻击中，对其窗口附近内的信号作随机相位扩展，得到输出的信号时域扩展函数为：

$$y(t)=\iint_{a,b}\rho(a,b)\frac{1}{\sqrt{|a|}}f\Big(\frac{t-b}{a}\Big)\frac{\mathrm{d}a\mathrm{d}b}{a^2} \tag{3}$$

式中，$f(t)$ 为 Sybil 入侵信号的非平稳态频谱，$\rho(a,b)$ 为伪平稳扩展函数，a 为谱密度，b 为时延参数。为了提高检测性能，采用功率谱密度加权，加权系数 $b_0=0, c_k$ 为合适的短时窗函数，采用合适的短时窗函数进行自适应检测，得到检测输出的功率谱密度特征为：

$$y(t)=\frac{1}{c_f}\iint W_f y(a,b)\frac{1}{\sqrt{|a|}}f\Big(\frac{t-b}{a}\Big)\frac{\mathrm{d}a\mathrm{d}b}{a^2} \tag{4}$$

物联网在受到攻击下产生网络波动跳变，采用伪平稳随机过程分析处理方法，得到检测波束域为：

$$c_f=\int_{-\infty}^{+\infty}\frac{|F(\omega)|^2}{\omega}\mathrm{d}\omega<\infty \tag{5}$$

式中，$F(\omega)$ 是 $f(t)$ 傅立叶变换，常数 c_f 称为函数 $f(t)$ 的波束高阶累积特征函数。通过高阶累积量特征提取，得到 Sybil 入侵特征的复包络分别为：

$$s(v)=\int_0^v\sin\Big(\frac{\pi}{2}x^2\Big)\mathrm{d}x \tag{6}$$

$$y(t)=u(s(t-\tau))\exp(j\omega_C s(t-\tau)) \tag{7}$$

式中，v 表示满足平稳性的假设的指向性特征，$u(t)$ 为复包络，ω_C 为能量密度。对于宽带 Sybil 入侵信号，指向性增益为：

$$c(v)=\int_0^v\cos\Big(\frac{\pi}{2}x^2\Big)\mathrm{d}x \tag{8}$$

由此得到了 Sybil 入侵信号的波束指向性特征分解结果为：

$$|s(f)|=A\sqrt{\frac{1}{2k}}\{[c(v_1)+c(v_2)]^2+[s(v_1)+s(v_2)]^2\} \tag{9}$$

采用盲源分离方法，进行时频分布下的入侵检测，在 t 时刻散射特性函数为：

$$P_i(t)=\sum_{n=1}^{N}\frac{A}{r}e^{-jkr}R_{in}\frac{1}{r}e^{-ikr} \tag{10}$$

化简得：

$$P_i(t)=\frac{A}{r^2}\sum_{n=1}^{N}e^{-j2kr}a_{in}e^{j\psi_{in}} \tag{11}$$

其中：A 为 Sybil 入侵的混响幅度，r 为信号的初始频率，$k=\frac{B}{T}$ 为信号总能量，e 为调频信号带宽。根据上述检测算法设计，进行 Sybil 入侵检测的程序设计，通过程序加载模块进行 Sybil 入侵防御系统的检测模块设计。

2　系统设计与实现

2.1　Sybil 入侵防御系统的硬件模块化设计

在上述进行了 Sybil 入侵防御系统的总体设计和入侵检测算法设计的基础上，进行 Sybil 入侵防御系统的硬件设计和软件开发，系统的模块化设计主要包括了滤波电路模块、主控电路模块、AD 电路模块和检测模块。采用前馈调制滤波器进行 Sybil 入侵检测特征匹配，构建滤波器电路。

以面向物联网的 Sybil 入侵信号为原始输入，给出一种简单的滤波器形式：

$$H(z)=\frac{N(z)}{D(z)} \tag{12}$$

式中，$N(z)$ 是 Sybil 入侵防御系统的低通信道函数，它的零点在 $z=e^{\pm j\omega_0}$ 处，$D(z)$ 为等效低通信道初始状态，由滤波器的频率参数 a 和带宽参数 r，确定前馈调制滤波器的起始频率与初始相位为：

$$\omega_0=\arccos(-a/2) \tag{13}$$

在各测量噪声互不相关的情况下，通过加权，得到 Sybil 入侵检测前馈滤波器高频响应特征函数为：

$$e^{j\pi}=V(e^{j\omega_0})=\frac{\sin\theta_2+\sin\theta_1(1+\sin\theta_2)e^{j\omega_0}+e^{j2\omega_0}}{1+\sin\theta_1(1+\sin\theta_2)e^{j\omega_0}+\sin\theta_2 e^{j2\omega_0}} \tag{14}$$

由此得到设计的 Sybil 入侵防御系统的前馈调制滤波器的传递函数为：

$$H(z)=\frac{1}{2}[1+V(z)]V(e^{j\omega})+e^{j\Phi(\omega)} \tag{15}$$

当满足约束条件为：

$$TW<<\frac{c}{2\mid v\mid},\left|\frac{2v}{c}\right|<<1 \tag{16}$$

得到的输出响应特征最大，此时能满足 Sybil 入侵检测的性能要求。根据上述设计，得到滤波电路如图 2 所示。

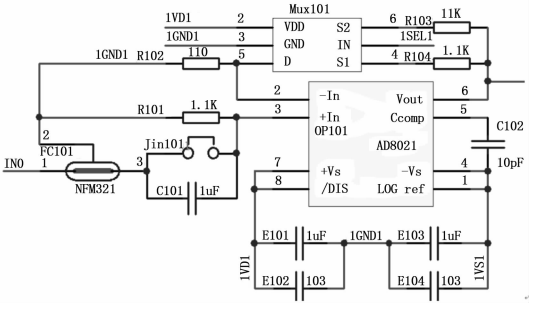

图 2 防御系统的滤波电路

主控电路模块是进行 Sybil 入侵防御检测的控制模块，采用的是 16 位定点 DSP 作为控制芯片，主控电路模块具有 8 个 32 位定时器/计数器功能，采用 ADG3301 进行 AD/DA 转换，通过交流耦合，采用 PCI9054 的 LOCAL 总线设计方法，进行面向物联网的 Sybil 入侵防御系统的数据采集，得到主控电路模块如图 3 所示。

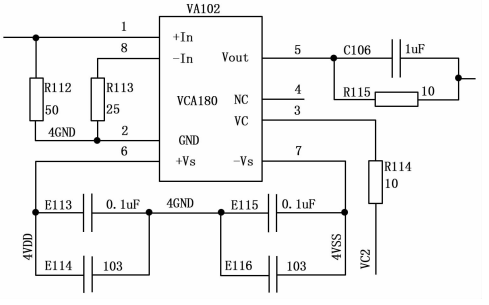

图 3 主控电路模块

AD 电路模块设计是 Sybil 入侵防御系统的数据采集部分，包括 A/D 转换器 AD7864 两片外部 I/O 设备，面向物联网的 Sybil 入侵防御系统 A/D 电路接口设计如图 4 所示。

检测模块通过入侵检测算法的程序加载，实现面向物联网的 Sybil 入侵防御系统内部时钟振荡检测和病毒入侵检测，采

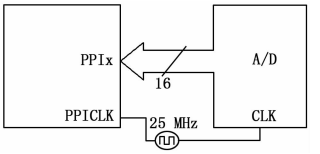

图 4 A/D 电路接口设计

用 DSP 数字信号处理芯片进行程序加载电路设计，程序加载是实现 Sybil 入侵检测算法的程序写入的功能，面向物联网的 Sybil 入侵防御系统的复位电路从串行的 TWI 存储器引导，选择 TWI 存储器进行位置信息存储，实现入侵检测。

2.2 软件开发实现

在上述进行了面向物联网的 Sybil 入侵防御系统的硬件设计的基础上，进行系统的软件设计，Sybil 入侵防御系统的软件开发处理程序是在 CCS 2.20 开发平台下进行。采用 C5409A XDS510 Emulator 仿真器进行硬件在线编程（Emulator），实现对检测算法的写入和数据图读取，读写操作通过 DMA 控制器实现系统的程序驱动，在 Sybil 入侵防御检测中，程序分成用户态和内核态，经过汇编和链接生成 .out 文件，通过 WDM 驱动程序与底层硬件进行入侵防御检测。

3 仿真实验与结果分析

为了测试本文设计的面向物联网的 Sybil 入侵防御系统的性能，进行系统调试和仿真实验，实验中，检测算法设计采用 Matlab 进行编程实现。Sybil 入侵信号中心频率测试为 $f_0=1\ 000$ Hz，Sybil 入侵数据信息的离散采样率为 $f_s=10*f_0$ Hz=10 kHz，串口控制的带宽为 $B=1\ 000$ Hz。Sybil 入侵防御系统的滤波器参数选择为：$\varphi=\varphi=0.5$，中断向量的阶数为 24，入侵检测的迭代步长均为 0.01，根据上述设计，运用 WIN32 API 函数 CreateFile () 函数打开 PCI 设备执行检测程序加载，实现对网络入侵检测仿真，得到面向物联网的 Sybil 入侵信号检测的原始数据时域波形如图 5 所示。

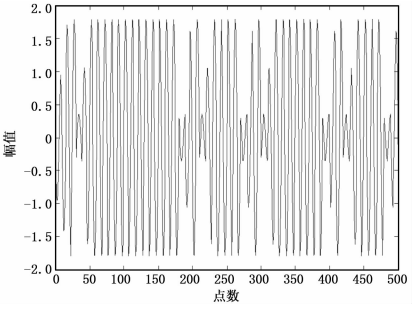

图 5 物联网数据采集原始数据波形

从图可见，在受到网络环境的干扰下，难以有效检测到 Sybil 入侵信号，采用本文方法进行 Sybil 入侵检测设计，得到网络入侵检测的信号分离结果如图 6 所示。

从图可见，采用本文方法进行 Sybil 入侵防御系统，能实现对入侵信息特征的准确分离，检测准确度较高，抗干扰能力较强，为了对比性能，采用本文方法和传统方法进行入侵防御，通过 10000 次试验取均值，得到物联网中信息传输的丢包率平均值如图 7 所示。

从图 7 可见，采用本文方法进行 Sybil 入侵防御系统设计，嵌入式设计到物联网中，进行数据传输，通过准确检测到

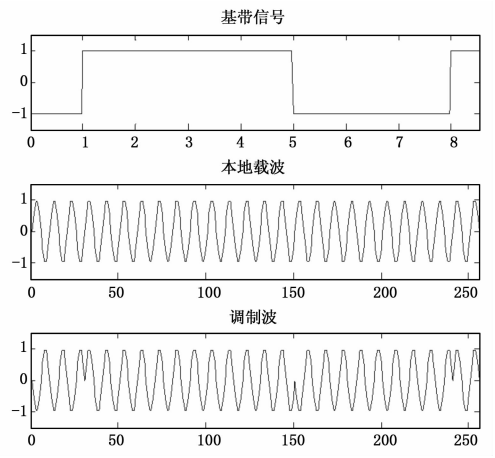

图 6　Sybil 入侵检测的信号分离结果

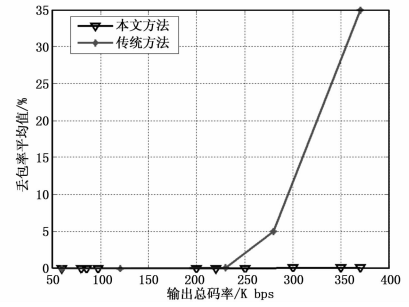

图 7　性能对比

入侵信息，提高了网络安全性能，降低了数据传输的丢包率。通过测试得知，本文设计系统具有较强的兼容性。

4　结束语

本文研究物联网中的 Sybil 入侵下的入侵防御检测问题，提高物联网安全防范能力，提出一种基于网络入侵信号检测和 16 位定点 DSP 内核设计的物联网的 Sybil 入侵防御系统设计方法。首先进行 Sybil 入侵防御系统总体设计描述和功能分析，进行了 Sybil 入侵信号检测算法设计，采用 C5409A XDS510 Emulator 仿真器进行硬件在线编程，在 CCS 2.20 开发平台下进行面向物联网的 Sybil 入侵防御系统的软件开发，实现系统的集成设计。测试结果表明，本文系统进行网络防御性能较好，可靠稳定。

参考文献：

[1] 陆兴华，张晓军. 人员图像跟踪过程中多人交叉区域防丢失方法[J]. 计算机仿真，2014，31 (9)：243－246.
[2] 于　涛，胡炳樑，高晓惠，等. 高光谱干涉图像动态追踪补偿方法研究[J]. 光子学报，2016，45 (7)：716－723.
[3] 陆兴华，吴恩燊，黄冠华. 基于 Android 的智能家居控制系统软件设计研究[J]. 物联网技术，2015，35 (5)：692－695.
[4] 张军强，王汝传，黄海平. 基于分簇的无线多媒体传感器网络数据聚合方案研究[J]. 电子与信息学报，2014，36 (1)：8－14.
[5] 章武媚，陈庆章. 引入偏移量递阶控制的网络入侵 HHT 检测算法[J]. 计算机科学，2014，41 (12)：107－111.
[6] 周小娟. 一种轻量级大数据分析系统的实现[J]. 电子设计工程，2016，23 (8)：40－43.
[7] 夏光辉，秦建军，王大成. 基于 FPGA 的双 CF 卡数据采集系统设计[J]. 电子设计工程，2016，21 (4)：19－21.
[8] 冯　颖，张　合，张祥金，等. 激光探测系统雪崩管实时补偿研究[J]. 南京理工大学学报 (自然科学版)，2010，34 (6)：787－791.
[9] Choi J，Yu K，Kim Y. A New Adaptive Component－Substitution－based Satellite Image Fusion by Using Partial Replacement[J]. IEEE Transactions on Geoscience and Remote Sensing，2011，49 (1)：295－309.
[10] 王跃飞，于　炯，鲁　亮. 面向内存云的数据块索引方法[J]. 计算机应用，2016，36 (5)：1222－1227.
[11] 葛文杰，赵春江. 农业物联网研究与应用现状及发展对策研究[J]. 农业机械学报，2014，45 (7)：222－230.
[12] 杨　楠，李世国. 物联网环境下的智能产品原型设计研究[J]. 包装工程，2014，21 (6)：55－58.
[13] 秦怀斌，李道亮，郭　理. 农业物联网的发展及关键技术应用进展[J]. 农机化研究，2014，18 (4)：246－248.
[14] 荆孟春，王继业，程志华，等. 电力物联网传感器信息模型研究与应用[J]. 电网技术，2014，38 (2)：532－537.
[15] 肖守伟，姚凯学，何　勇. 基于物联网的新型视频监控系统的设计与实现[J]. 计算机测量与控制，2015，23 (10)：3354－3356.

(上接第 171 页)

参考文献：

[1] 赵红梅，章卫国，刘小雄，等. 飞控系统传感器故障诊断的在线方法研究[J]. 计算机测量与控制，2010，18 (5)：1097－1099.
[2] 刘　华，唐永哲，郝　涛，等. 飞控系统传感器故障诊断研究[J]. 计算机仿真，2010，27 (2)：30－33.
[3] 李家群，候孝宗，毛俊隽. 浅析差动变压器传感器的几种测量方法[J]. 水利水文自动化，2008 (3)：40－43.
[4] 孟武胜，苗溢文，董　蓉. 一种新型差动变压器式角位移传感器[J]. 微特电机，2010 (8)：32－34.
[5] 冯广丽，卢朝东. 红外瓦斯无线传感检测系统设计与实现[J]. 计算机测量与控制，2013，21 (1)：80－81.
[6] 冯　强，耿爱辉. 基于 LabVIEW 的四象限光电探测器数据采集系统设计[J]. 计算机测量与控制，2013，21 (5)：1397－1399.
[7] 胡海涛，高　闻. 高性能 LVDT 位移传感器调理电路设计[J]. 仪表技术，2012 (8)：39－42.
[8] 魏　婷，夏德天. 基于 LVDT/RVDT 的交流模拟量解调方法研究[J]. 航空计算技术，2013 (1)：116－118.
[9] 王　龙，史丽晨，王海涛. 基于 LVDT 的新型信号调理电路的设计[J]. 计算机测量与控制，2015. 23 (3)：953－955.
[10] 樊泽明，郭　月，袁朝辉. 基于 AD698 的旋转变压器驱动及解码电路设计[J]. 测控技术，2013，2 (32)：110－113.
[11] 罗德荣，周　成，黄科元，等. 基于 AD2S1200 的旋转接口电路设计及信号处理[J]. 电力电子技术，2008，42 (8)：68－70.
[12] 李耀海，胡广艳，郝瑞祥，等. 基于 AU6802NI 的旋转变压器信号接口电路的设计和应用[J]. 电子设计应用，2006，40 (2)：110－114.
[13] 冯广丽，卢朝东. 红外瓦斯无线传感检测系统设计与实现[J]. 计算机测量与控制，2013，21 (1)：80－81，88.
[14] 李　稷，李　玲，张　辉，等. LVDT 传感器仿真电路的设计与研究[J]. 仪表技术，2011 (9)：67－70.
[15] 尹成竹，柏受军，黄　平，等. 一种基于 AD598 的精密位移传感器的研制[J]. 传感器与微系统，2007，26 (2)：68－70.