

基于泄漏电缆的周界入侵探测系统设计

于慧洁¹, 李建杰¹, 凌小峰², 梁晨¹, 刘源¹

(1. 上海理工大学 光电信息与计算机工程学院, 上海 200093; 2. 华东理工大学 信息科学与工程学院, 上海 200237)

摘要: 针对传统周界入侵探测系统存在的定位精度不高及误报漏报率高等问题,设计了一种基于泄漏电缆的新型周界入侵探测系统.根据入侵探测系统的功能需求,将两根经特殊设计的泄漏电缆埋地安装,然后利用现场可编程门阵列实现泄漏电缆中信号的发送和处理,其泄漏的电磁场形成一堵无形的防护区,最后通过自行开发的测试软件实现泄漏电缆远程自动探测流程.实验结果表明,该基于泄漏电缆的入侵探测系统对入侵的定位精度实测达到了5 m,具有全隐藏安装、准确定位入侵位置及误报漏报率低等优点.

关键词: 周界入侵探测; 泄漏电缆; 现场可编程门阵列; 定位精度

中图分类号: TM 930.12 **文献标志码:** A

Design of a Perimeter Intrusion Detection System Based on Leaky Cable

YU Huijie¹, LI Jianjie¹, LING Xiaofeng², LIANG Chen¹, LIU Yuan¹

(1. School of Optical-Electrical and Computer Engineering, Shanghai 200093, China;

2. School information Science and Engineering,

East China University of Science and Technology, Shanghai 200237, China)

Abstract: For the problem of low positioning accuracy, high false and missed alarm rate of traditional perimeter intrusion detection systems, a new type of perimeter intrusion detection system was designed based on leaky coaxial cables. According to the functional requirements of the intrusion detection system, two specially designed leaky cables were buried underground, forming an invisible protective zone by its electromagnetic field, while the signals propagating in the leaky cables were sent and processed by a field-programmable gate array. Finally, a self-developed test software was applied to achieve the remote automatic detection process. The experimental results show that the intrusion detection system based on leaky cables has achieved the positioning accuracy of 5 m. In addition, it has the advantages of fully hidden installation, accurate intrusion locating capability and low false and missed alarm rate.

收稿日期: 2017-07-11

基金项目: 国家自然科学基金资助项目(61601291)

第一作者: 于慧洁(1992-),女,硕士研究生.研究方向:新型传感器. E-mail:2572704260@qq.com

通信作者: 李建杰(1981-),男,讲师.研究方向:微波射频电路、新型传感器. E-mail:86787499@qq.com

Keywords: *perimeter intrusion detection; leaky cable; field-programmable gate array; positioning accuracy*

随着社会经济的发展和人们生活水平的提高,人们对自身所处的生活环境的安全有了更高的要求^[1].传统的方法如围墙、钢丝网等物理屏障将无法阻止蓄意入侵犯罪份子的破坏、盗窃等活动,人们需要更先进的安防设备来保障重要的区域不被入侵^[2-3].周界入侵探测已成为安防行业最具挑战性的领域之一,其主要任务是当设防周界发生非法入侵时,系统能够及时、准确、无误地早期告警^[4-5].

市场上存在很多基于声、光、电、压力等物理原理的安防设备,主要有红外对射探测器^[6]、振动传感电缆^[7]、激光对射探测器^[8]、墙振动入侵探测器^[9]、微波探测器^[10],以及视频运动探测与跟踪系统等.这些系统除了各有自己的特点和适用范围外,还存在着明显的缺点:受气候环境影响比较大、误报漏报率高及缺乏精确定位能力等^[3,11-12].泄漏电缆探测技术用于入侵探测最早出现于 20 世纪 70 年代,该技术具有误报漏报率低、隐蔽性高、受环境影响小、适应各种地理条件等特点,已经成为目前应用最广、发展前景十分良好的一种技术和产品^[13].但是,目前国内的泄漏电缆周界入侵探测系统基本仍停留在有无入侵的探测,少数具有定位功能的产品还存在定位精度不高等问题^[14-17].如王明吉等^[5]研究的单主机多域周界入侵探测系统的定位精度可以达到 20 m,文献^[11]研制的 FT-100 型辐射电缆周界防越探测设备的定位精度理论上能达到 9.7 m.

本文将泄漏电缆作为分布式传感器应用到周界入侵探测,将两根相距 1 m 左右的泄漏电缆平行浅埋于地下,利用主控板的 FPGA 处理模块实现泄漏电缆中信号的发送和处理.如果发生入侵,发射电缆在空间建立的电磁场将被扰动而发生变化,主机将此扰动信号与稳定的电磁场信号进行比较、分析和判断,最终利用测试软件实时显示当前探测状态并进行远程控制.经实地测试,该系统对入侵的定位精度达到了 5 m,克服了现有的周界入侵探测系统误报漏报率高的缺点,提高了入侵探测系统的定位精度.

1 系统组成及工作原理

泄漏电缆入侵探测系统主要由信号处理模块、泄漏电缆、终端匹配负载、电源和主控计算机组成,系统框图如图 1 所示.泄漏电缆是特殊设计的一种同轴电缆,具有信号传输和天线的作用,通过对外导体开口的控制,可将受控的电磁波能量沿线路均匀地辐射出去及接收进来,工作时其中一根要向周围的空间发射电磁场,另一根接收电磁场^[18-20].

该系统的基本工作原理是:FPGA 处理模块产生电磁信号经功率放大器馈入发送用的泄漏电缆中,并在电缆中传输.当能量沿电缆传送时,部分能量通过开槽漏入空间,在被警戒空间范围内形成一个大约宽 3 m,高 1 m 的电磁场防护区,其中一部分能量被安装在附近接收用的泄漏电缆接收,形成收发能量直接耦合.探测系统在埋地电缆周围产生不可见的空间电磁场,对移动目标的导电性、体积、移动速度进行探测.当入侵者进入两根电缆形成的防护区内时,这部分电磁能量受到扰动,引起接收信号的变化,这个变化的信号经低噪声放大和滤波处理后被送入 FPGA 模块进行处理,然后将处理得到的数据上报给主控计算机,最后利用上位机软件将入侵信号检测出来,并推动报警指示灯点亮,同时使继电器触点打开.

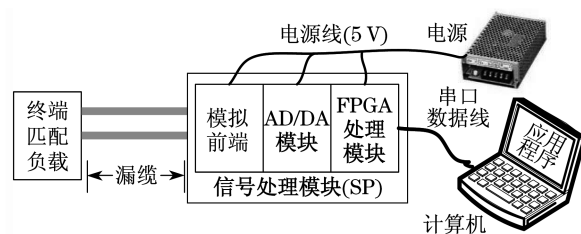


图 1 泄漏电缆入侵探测系统框图

Fig.1 Block diagram of the leaky cable intrusion detection system

2 系统硬件整体结构设计

系统硬件电路即泄漏电缆入侵探测系统的信号

处理模块,主要由 FPGA 处理模块、模拟前端和 AD/DA 模块组成.其中,FPGA 模块除了包含 FPGA 电路外,还涵盖了时钟和接口模块,接口包含了所有外部供电和数据传输接口.

FPGA 处理模块产生传递信息的数字中频信号,数字中频信号经过 AD/DA 模块的高速数字模拟转换器 DAC(digital to analog converter)转换成模拟信号,接着经过模拟前端的带通滤波器 BPF (band-pass filter) 和功率放大器 PA (power amplifier)完成信号的滤波和放大,最后将产生的中频信号馈入发送泄漏电缆中,完成激励.同时,泄漏电缆可以将报警信息反馈给主机,有效信号首先经过模拟前端的低噪声放大器 LNA (low noise amplifier)和带通滤波器完成信号的去噪、放大和滤波,接着经过 AD/DA 模块的高速模拟数字转换器 ADC(analog-to-digital converter)转换成数字信号,然后经 FPGA 处理模块对接收的数字中频信号进行处理,最后将这些数据通过数据接口上报给主控计算机.系统的硬件实现方案是消除误报漏报与提高灵敏度的关键,系统硬件的整体结构设计如图 2 所示.

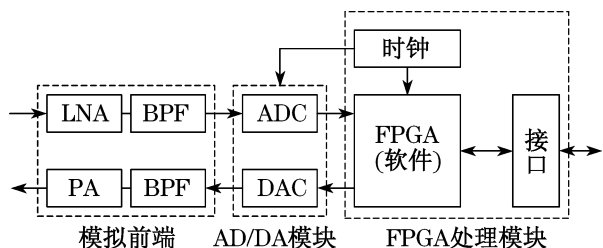


图 2 硬件的整体结构设计

Fig.2 Overall design of the hardware structure

FPGA 处理模块主要负责产生用于发送的数字中频信号,对接收的数字中频信号进行处理,并且将处理后的数据通过数据接口上报给主控计算机.模拟前端包括接收和发射两个支路,接收支路对泄漏电缆中的接收信号进行放大和滤波,主要包括一个低噪声放大器和一个带通滤波器,如果泄漏电缆中的接收信号功率过低,单级低噪声放大器增益不够,还可根据需要增加一级中放.AD/DA 模块包括高速 ADC、高速 DAC 和必要的时钟分配电路,该模块用于实现模拟信号到数字信号的转换以及数字信号到模拟信号的转换.从基本设计要求考虑,AD/DA 模块采用同源的时钟,并且能够全实时地将数据送给

后续 FPGA 处理模块.

3 软件设计

系统软件部分的主要功能是下发控制参数,实现对发射电缆的激励作用,并获取 FPGA 处理模块的上报数据,完成泄漏电缆场强数据及入侵状态数据采集与实时显示,然后根据对场强数据的分析,探测入侵的有无,并精确定位入侵的位置.同时系统具备探测数据保存、通用报表文件生成等功能.

信号处理模块中的软件部分即为下位机,系统上电后开始工作,首先将系统复位至明确的初始状态,进行系统设备的初始化配置和自检.在自检过程中进行设备合法性验证步骤,在初始化指令中下发所用设备的验证码信息(每个合法设备都设置了唯一的设备验证码),设备判断该验证码信息与设备是否匹配,若匹配则通过设备合法性自检,否则不通过,不能通过设备合法性验证的设备将无法通过自检.复位完成后,系统进入默认的参数设置模式,设置系统工作所需的各种参数,包括设备编号、分区检测门限等.然后启动校准工作模式,该模式下要求在一定时间内,1 个身高 1.7 m 左右、体重 60 kg 左右的人以约 1 m/s 速度按正常步态行走,从起始点沿部署线一直走到终止点,系统将该过程的测试数据上报给主机,主机根据这些测试信息统计获得校准所需的推荐参数设置值.接着根据校准结果,再次设置工作参数.最后,进入正常工作模式,系统按照一定的刷新频率上报入侵报警信息数据包,从而实现报警.整体控制流程图如图 3 所示.

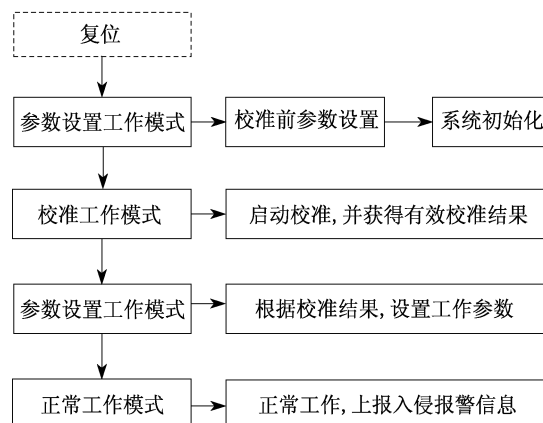


图 3 下位机工作流程图

Fig.3 Work flow chart of the slave computer

上位机是基于 Matlab 的人机界面,主要分为参数设置区、入侵显示区、记录与回放区。首先在参数设置区新建探测任务,然后初始化对应的通信链路,最后建立链接,实时显示探测状态,绘制探测波形。任务结束后,可根据需要生成通用报表文件及保存。

4 样机入侵检测及结果分析

为了验证这种泄漏电缆入侵探测系统是否达到设计要求,进行了相应的实验,通过测试入侵的位置和时间,来验证该户外入侵探测系统的准确性,以及误报漏报率。

对于埋地泄漏电缆入侵探测系统的测试,作者搭建了如下测试场景:在一家工厂的围墙外,将两根经过特殊设计的泄漏电缆以 1 m 的间隔平行埋入地下,埋地深度在 5 cm 左右,如图 4 所示(掩埋之前的照片)。两根泄漏电缆的两端分别连接匹配负载和信号处理系统,上位机控制信号处理系统发射、接收和处理信号,通过沿着平行和垂直泄漏电缆的方向随意走动来对入侵系统进行检测。利用 Matlab 编写的上位机软件查看后端报警情况,如图 5 所示。

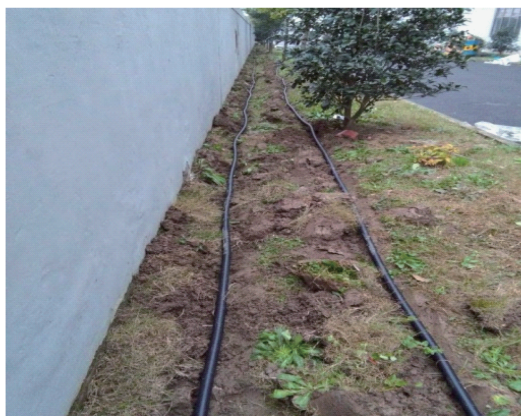


图 4 室外入侵探测实验场景

Fig.4 Experiments scene of the outdoor intrusion detection

图 6 为采用 100 m 长泄漏电缆入侵探测实验的测试结果,整个测试刷新周期为 2 s。图 6 上半部分为不同位置检测的信号功率水平。由图 6 可知,当有人入侵时,扰动信号功率远大于背景的信号功率。泄漏电缆上某处位置的入侵功率越大,说明该处越接近当前的入侵位置,即入侵功率的峰值所对应的泄



图 5 入侵探测实验的 PC 端报警监视

Fig.5 PC alarm monitoring of intrusion detection experiments

漏电缆位置处为当前的入侵位置,进而可以根据入侵功率的大小判断出入侵位置。图 6 下半部分为测试人员在埋地线缆附近以不同的速度沿线行走(从始端到末端,来回走动),不同时间所处入侵位置的报警提示。对入侵检测的定位精度实测达到了 5 m,经过埋地 4 个月测试,系统运行稳定可靠,仅出现过 3 次误报,无漏报。各项性能指标均达到设计和实际使用要求。

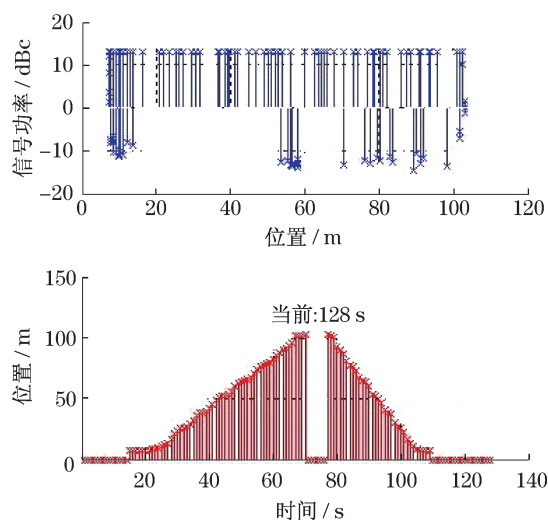


图 6 不同位置入侵报警提示

Fig.6 Different location intrusion alarm prompt

5 结 论

鉴于传统周界入侵探测系统误报漏报率高和定位精度不高的情况,本文使用经过特殊设计的泄漏

电缆和信号编码,设计了泄漏电缆周界入侵探测系统.本文从原理到系统硬件和软件设计介绍了泄漏电缆入侵探测系统,并对该探测系统进行测试.实验结果表明,当有人入侵泄漏电缆的防护区时,可以探测到入侵信号,对入侵的定位精度实测达到了5 m,减少了报警信息的误报漏报,提高了入侵监测的准确性,从而验证了该周界入侵探测装置的可行性.由此可见,本系统具有全隐藏安装、准确定位入侵位置和误报漏报率低的优点,在户外报警领域具有广泛的应用前景.

参考文献:

- [1] 王华杰,张晓娟,郑来芳.基于STM32的红外无线报警系统的设计[J].山西大同大学学报(自然科学版),2016,32(1):24-27.
- [2] 苏旭峰.分布式光纤振动传感系统的数据采集与处理[D].北京:北京邮电大学,2010.
- [3] 韦统安.基于泄漏电缆传感器的周界入侵探测技术[D].青岛:中国海洋大学,2012.
- [4] 樊治敏.张力式电子围栏周界防范报警系统设计原理及应用现状[J].中国安防,2008(3):42-45.
- [5] 王明吉,张勇,李玉爽,等.单主机高精度周界入侵探测报警系统[J].仪器仪表学报,2006,27(12):1718-1720.
- [6] 韦中超,廖浚宏,张准,等.主动红外对射式光电防盗报警器[J].光电技术应用,2013,28(2):1-4.
- [7] 田晓凤.基于振动传感器的周界围栏报警监控系统设计[D].沈阳:沈阳航空航天大学,2013.
- [8] 王维.激光对射系统在机场周界安防系统中的应用研究[J].智能建筑与城市信息,2010(3):79-85.
- [9] 李强,黄泽铤,徐雅芹,等.基于单模-多模-单模光纤模间干涉的传感系统[J].红外与激光工程,2014,43(5):1630-1636.
- [10] 岳剑锋.分布式光纤 φ -OTDR安防系统实用化研究[D].成都:电子科技大学,2009.
- [11] 乔宏章,张军.泄漏电缆周界监视技术研究[J].无线电工程,2013,43(3):43-46.
- [12] HARMAN K. Omnitrax ranging leaky coaxial cable sensor technology update [C]//Proceedings of the 43rd Annual 2009 International Carnahan Conference on Security Technology. Zurich, Switzerland: IEEE, 2009:216-220.
- [13] 王明吉,朱磊,李玉爽.泄漏电缆周界入侵信号检测方法及其仿真研究[J].信息技术,2013(10):81-84.
- [14] INOMATA K, YAMAGUCHI Y, YAMADA H, et al. Accuracy of 2-dimensional object location estimation using leaky coaxial cables[J]. IEEE Transactions on Antennas and Propagation, 2011, 59(6):2396-2403.
- [15] TSUJITA W, INOMATA K, HIRAI T. Development of dual leaky coaxial cable for intruder detection sensor [C]//Proceedings of the 2013 IEEE International Conference on Technologies for Homeland Security (HST). Waltham, MA, USA: IEEE, 2013:126-129.
- [16] 高松巍,杨洋.泄漏同轴电缆在周界报警装置中的应用[J].沈阳工业大学学报,2006,28(1):91-93,119.
- [17] 邵杰.基于泄漏同轴电缆的新型周界报警探测系统研究与实现[D].沈阳:东北大学,2012.
- [18] 朱磊.泄漏电缆周界入侵信号检测方法研究[D].大庆:东北石油大学,2013.
- [19] WANG J H. Research on the radiation characteristics of patched leaky coaxial cable by FDTD method and mode expansion method [J]. IEEE Transactions on Vehicular Technology, 2008, 57(1):90-96.
- [20] FENG L L, WANG Z, YANG X D, et al. Research on the radiation field of wide-band leaky coaxial cable [C]//Proceedings of the 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM). Chengdu, China: IEEE, 2010:1-4.

(编辑:石 瑛)