物联网系统安全与可靠性测评技术研究

李 维,冯 钢,刘 冬,苗 勇,汤业伟,胡 滨
(工业和信息化部 计算机与微电子发展研究中心(中国软件评测中心),北京 100048)

摘 要:如何保障物联网系统在各种应用环境下的安全与可靠性,是制约物联网技术大规模应用的瓶颈之一。研究符合物联网特征的安全与可靠性测评技术,研发专用测评工具,发现存在于系统中的风险隐患,是建立物联网系统安全与可靠性保障体系的重要基础。文中在分析物联网各层风险环节的基础上,结合物联网质量保障的共性需求,提出了物联网安全与可靠性内涵,研制了测评体系,并针对无线传感器网络安全性测试需求,开发了安全性渗透测试工具。

关键词:物联网;安全性;可靠性;测评;无线传感器网络
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2013)04-0139-05
doi:10.3969/j.issn.1673-629X.2013.04.034

IOT System Safety and Reliability Testing Technology Research

LI Wei, FENG Gang, LIU Dong, MIAO Yong, TANG Ye-wei, HU Bin
(Research Center for Computer and Microelectronics Industry Development, MIIT, Beijing 100048, China)

Abstract: How to protect IOT security and reliability in various environments is one of the bottlenecks which are restricting the large scale IOT application currently. It is the important basis of IOT security and reliability protection system to study testing and evaluation technology, specific testing tool and to find out the risks and potential hazards in system. Outline content of IOT security and reliability according to risk analysis of IOT layers and IOT quality demand. Meanwhile, it shows a IOT security and reliability testing system and a security penetration tool for wireless sensor network.

Key words: Internet of Things; safety; reliability; testing; WSN

0 引 言

物联网是一个系统的系统(System of Systems),由感知、传输、应用以及控制多个子系统构成,每一个子系统又包括若干小的系统,涉及众多技术领域;物联网的应用场景千差万别,对系统的安全性与可靠性提出较高要求;另一方面,物联网系统因其解决方案的差异性、管理的复杂性以及需求的多样性等特征,使既有的硬件可靠性、软件可靠性、网络可靠性、信息安全等技术不能很好满足物联网系统端到端安全与可靠性保障需求。

因此,研究符合物联网特征的安全与可靠性测评技术,研发专用测评工具,发现存在于系统中的风险隐患,是建立物联网系统安全与可靠性保障体系的重要基础。下面将分析物联网各层风险环节,并结合物联网质量保障的共性需求,提出物联网安全与可靠性内涵,研制测评体系,同时针对无线传感器网络安全性测试需求,开发安全性渗透测试工具。

收稿日期:2012-04-26;**修回日期**:2012-07-29
基金项目:国家物联网发展专项资金项目(财企(2011)64 号);电子信息产业发展基金(财政部财建(2011)879 号,工业信息化部财函(2011)506 号)
作者简介:李 维(1982-),女,博士,中国软件评测中心副总工程师,研究方向为物联网、信息安全、可靠性技术。

1 物联网系统面临的安全与可靠性挑战

真实环境中部署的物联网系统往往由多个异构网络互联起来的传感器设备、网关设备、通信设备以及计算机等电子设备组成。电子设备中任何一个元器件或焊点发生故障都将导致系统发生故障。另一方面,在物联网系统的感知层通常有 RFID、各类传感器等终端设备采集数据,这些与应用环境结合最紧密的组件面临高低温、冲击、震动和辐射等条件,使产品的可靠性受到影响。同时物联网应用物理环境的恶劣可能导致通信信道受到严重干扰,使决策系统软件发生误判或者失效。目前物联网安全性和可靠性已成为人们关注的焦点。

研究物联网安全性和可靠性,要先从缺陷和薄弱环节入手。表 1 小结了物联网各层存在的安全缺陷和薄弱环节[1,2]。在此需要特别指出的是:隐私泄露问题在物联网领域面临的形势非常严峻。从感知层到应用

表 1 物联网各层的典型安全缺陷与薄弱环节

层级	安全缺陷	说明	风险级别
感知层	物理安全	传感网容易遭到物理破坏而失效;节点结构简单,加密手段较弱,易于伪造	高
	链路安全	有限的数据加密机制;碰撞攻击和拒绝服务攻击	低
	路由安全	虚假路由,脆弱的路由协议	中
	恶意攻击	Sinkhole 攻击、Sybli 攻击、Wormholes 攻击、HELLO flood 攻击等	高
	物理破坏	通过物理手段取出芯片封装,使用微探针获取敏感信号,进而进行对 RFID 标签的重构	中
	信息泄露	无线信号广播,易被窃听	高
	无线干扰	干扰广播、阻塞信道	高
	安全协议攻击	扫描 RFID 标签和响应识别器,寻求安全协议、加密算法弱点,进而删除 RFID 标签的内容或篡改可重写 RFID 标签内容	中
	隐私保护	涉及到个体隐私问题的数据在物理层泄露	高
网络层	异构接入	物联网采用 Wi-Fi、WiMAX、3G/LET/4G 等各种无线接入技术,异构网络的复杂性给管理和安全带来了新的挑战	低
	无线网络开放性	无线信道的开放性使信道窃听、干扰容易实现,数据信息被篡改、插入、删除、截获的风险增大	高
	核心网络安全性	网络地址空间短缺,巨大的信息量,网络带宽的有限性,传统的基于互联网络的协议的有效性	中
	网络拥塞	大量以集群方式存在的物联网节点,在数据传输过程中,会导致网络产生“洪水”效应,造成网络拥塞甚至瘫痪	高
	隐私保护	涉及到个体隐私问题的数据在网络层泄露	中
应用层	恶意代码和设计缺陷	来自传统应用层的恶意代码、病毒和系统自身的设计漏洞	高
	海量数据处理	物的数量极其庞大,信息量远比“互联网”时代巨大	中
	云计算安全性	物联网依赖于云计算强大的处理和存储能力作为支撑	高
	数据分级管理	不同安全级别的数据需要分级存储、访问和管理,及与之对应的身份认证问题	低
	隐私保护	大量涉及个体隐私的信息(如身份信息、财产、位置信息等)会因为未实行有效的保护,面临被非法窃取、篡改、泄露的风险	高

表 2 物联网各层的典型可靠性缺陷与薄弱环节

物联网	漏洞	漏洞说明	共性可靠性问题
感知层	易于伪造	结构较为简单,非常易于伪造	物联网架构技术标识和解析技术网络管理技术
	信息泄漏	无线通信的广播特性	
	易受环境干扰	工作环境复杂;信号弱,易受外界影响	
	数据采集失效	节点本身容易遭到影响与破坏;多节点协作进行数据采集	
	节点能耗	节点能源受限,应降低能耗	
	无线链路不稳定	信号弱,易受外界影响;节点差异性	
网络层	低功耗路由问题	限于能耗问题,路由信息的播送就不能很频繁	
	多跳通信问题	多跳通信导致链路不稳定,增加系统能耗	
	异构网络融合	支持多种通信协议	
	服务质量(QoS)	不可靠的平台提供可靠的服务	
应用层	设备备份与恢复	避免单点故障	
	海量数据存储和处理	算法不仅要高效而且空间复杂度还必须很低	
控制层	无线信道易受影响	节点信号弱,易受外界影响	
	通信协议简单	控制器自身结构简单,无法采用较复杂协议	

层,各层都存在着隐私泄露的环节。目前保护隐私的各种技术尚未成熟:现有的各种系统并不是针对资源受限访问型设备而设计的,但物联网恰恰是这种类型的系统。

表 2 小结了物联网各层存在的可靠性隐患。

2 国内外安全与可靠性评测技术研究现状

2.1 信息安全评测技术

近年来,伴随信息技术的发展,信息安全的内涵也从 20 世纪 80 年代的通信保密,发展为目前以“风险管理”为主的信息安全。为加强物联网信息安全风险检测与防范,国际研究机构纷纷开展专业物联网安全测试工具的研制。美国加州大学洛杉矶分校、澳大利亚新南威尔士大学、德国不莱梅大学分别开发出用于物联网信息安全测试的 SenSec[3],用于传感网蛀洞攻击的测试网络 BANAID[4],用于物联网信息安全仿真与验证的 TAP-SNS[5]。这些测试工具目前只能针对几种典型漏洞进行测试,且多停留于网络层面,需要更加紧密结合物联网的应用特征才能更有效地应用于物联网安全检测。

2.2 软件可靠性评测技术

目前,软件可靠性研究主要包括软件可靠性需求与分配、软件可靠性分析、软件可靠性设计、软件可靠性度量和软件可靠性测试等方面[6]。软件可靠性测试是为了满足用户对软件的可靠性要求,通过对软件进行测试并发现和纠正软件中的缺陷,提高软件的可靠性水平,并验证它能否达到用户可靠性要求的一种软件测试方法。国外,马里兰大学、纽卡斯尔大学等在软件可靠性领域发表了不少研究成果。国内的北京航空航天大学等研究单位研发了可靠性设计分析技术及软件工具,并在一些项目中得到应用。但目前国内对于软件可靠性模型的研究多集中在软件的研制阶段,很少有涉及测试与评估阶段的可靠性模型。

2.3 硬件设备可靠性评测技术

硬件设备可靠性技术方面,对于产品和模块级等电子产品的可靠性研究主要集中在可靠性设计、可靠性预计与可靠性试验几方面[7,8]。其中,硬件产品可靠性试验目的是了解产品,验证产品的可靠性水平,通过试验—改进—再试验,反复提高产品可靠性水平。对不同的产品,有不同的可靠性测试方法,如环境试验、寿命试验、筛选试验、现场使用试验和鉴定试验等。

2.4 网络可靠性评测技术

网络可靠性研究早期主要集中于通信网络领域。伴随 Ad-Hoc 等复杂网络的发展以及网络应用场景和规模的复杂化,传统网络可靠性分析技术面临严峻挑战[9,10]。伴随通信网络规模的迅速扩张,网络拥塞和

延时逐渐成为了网络可靠性主要考虑的因素。目前国外从事网络可靠性研究的学术机构主要有美国弗吉尼亚大学计算机学院、英国利兹大学交通研究所等。国内对网络可靠性分析系统的研究主要着眼于网络安全与故障维修方面,研究机构有北邮、北航等,但是国内缺少应用于实际网络的可靠性评测系统。

综合上述的关于软件可靠性、硬件设备可靠性以及通信网络可靠性的研究,一般研究者是把三者作为独立不相关的组成部分,分别进行研究。而物联网系统的可靠性不仅包括软件可靠性、硬件设备可靠性以及通信网络可靠性,而且包括三者之间的互相影响及作用。

3　物联网系统安全与可靠性内涵

3.1　物联网系统安全性内涵

物联网安全性是指在满足功能、性能要求的前提下,物联网系统保护硬件、软件及数据,防止其因偶然或恶意的原因使系统遭到破坏,数据遭到更改或泄露等的能力,分为技术安全性和管理安全性两大类。其中,技术安全性包括物理安全性(如电磁防护和能耗控制等)、网络安全性(如入侵防范与安全审计)和应用安全性(如数据安全与备份、隐私保护)。

3.2　物联网系统可靠性内涵

物联网系统可靠性(关于物联网系统可靠性定义与详细内涵请见本作者的另一篇文章[11])是指物联网在业务量增消变化的运行过程中,在各种破坏性因素共存的条件下,物联网对用户服务需求持续满足的能力。这一定义体现了物联网“以用户为中心”的服务宗旨。这里,“对服务需求的满足能力”是物联网可靠性的测度,它包括两个维度:从能力内涵看,既包含物联网系统的生存能力,也反映了系统对用户需求的适应能力;从研究内容看,既研究系统固有属性(如拓扑设计、路由设计、资源管理机制等)的可靠性,也研究系统运行属性的可靠性,是对系统可靠性的综合测度。

对比传统的系统可靠性要素内涵,物联网系统可靠性五要素的内涵分别为:

· 对象是指物联网系统,包括固有属性和任务属性;

· 规定条件是指物联网运行环境中的各种破坏性因素(即各种影响物联网高效可靠运行的因素),既包括人为或自然破坏因素,也包括业务量变化、系统自身故障等因素;

· 规定时间是指系统设计时规定的运行生命周期;

· 规定功能是指用户需求,即系统功能;

· 能力是指满足用户需求的能力,即系统性能。

根据物联网系统可靠性内涵,物联网系统可靠性的研究需要考虑以下几个方面的问题:

· 在无外界破坏环境下,系统在业务量变化、自身故障和人为正常操作等因素下,仍能保持运行的能力;

· 系统在随机性破坏作用下,保持有效运行的能力;

· 系统在人为、自然灾害破坏下,仍能保持运行的能力;

· 系统抗各种安全攻击的能力;

· 系统运行管理能力。

从上述定义可以清晰发现,物联网系统可靠性是硬件可靠性、软件可靠性、通信网络可靠性的内容高度集成和综合运用。研究物联网系统可靠性,需要将硬件、软件和网络作为一个有机整体,考量其在各种测试条件下,满足用户服务需求的能力。物联网系统可靠性具有端到端、系统级、与应用环境紧密结合的特征,这也是区别于传统的系统可靠性的本质特征。

4　物联网系统安全与可靠性测评模型

4.1　物联网系统安全性测评模型

对物联网系统的安全测评是以保障系统的高效可用为前提条件的,测评模型的输入为系统功能、系统性能、系统管理、感知层信息安全、网络层信息安全、应用层信息安全。以上输入因素在实际的应用及测评过程

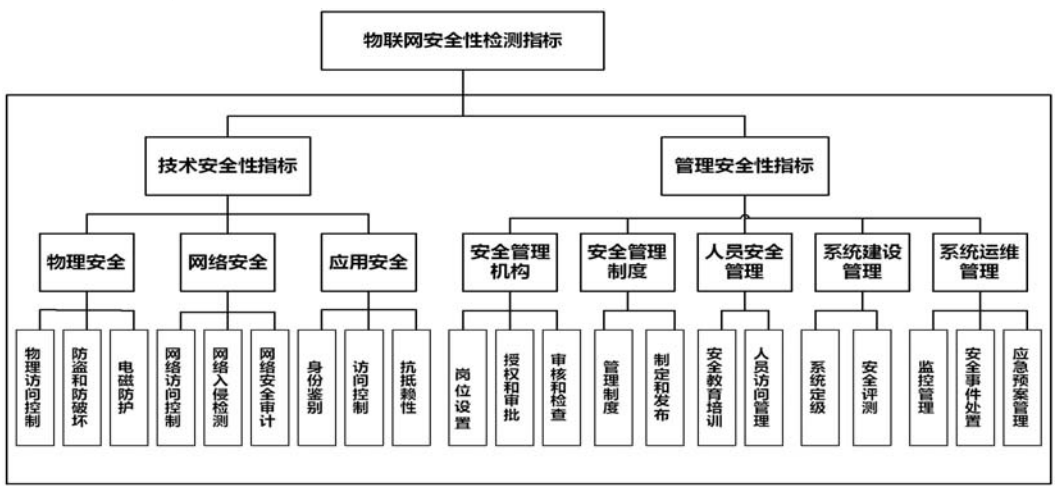

图 1　物联网系统安全检测模型

中都会互相影响,通过物联网安全检测系统模型的后台运算,输出被测物联网系统各层的安全性、功能、性能、管理方面的量化数据,同时输出目标系统这几方面目前的相互关系情况。可以帮助用户或企业更直接地找出系统的薄弱环节,并进行修改。图 1 为物联网安全测评模型。

4.2 物联网系统可靠性测评模型

在研究分析物联网安全与可靠性内涵的基础上,研制了由检测指标、条件指标和判定指标三部分组成的测评指标体系。其中,检测指标(见图 2)用于确定检测项,条件指标用于确定实施测评的外界条件等级,判定指标用于判定检测指标在各种测试条件下是否符合既定功能性能指标的要求,分为系统级判定指标和子系统级判定指标(见图 3)。其中,系统级判定指标用于判定被测物联网系统的安全性与可靠性等级,子系统级判定指标用于确定系统缺陷或漏洞的位置,以改进系统设计方案或指定预警应急方案。

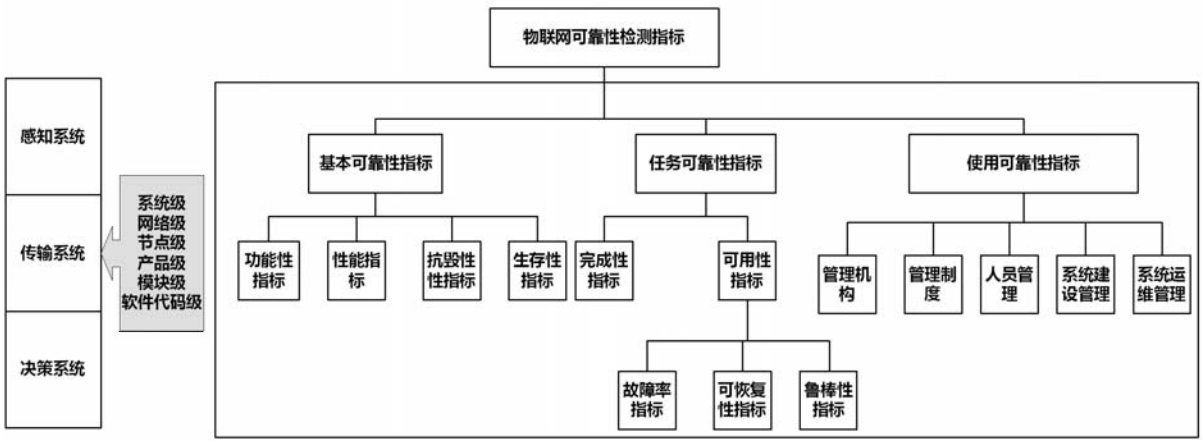

图 2 物联网系统可靠性测评检测指标模型

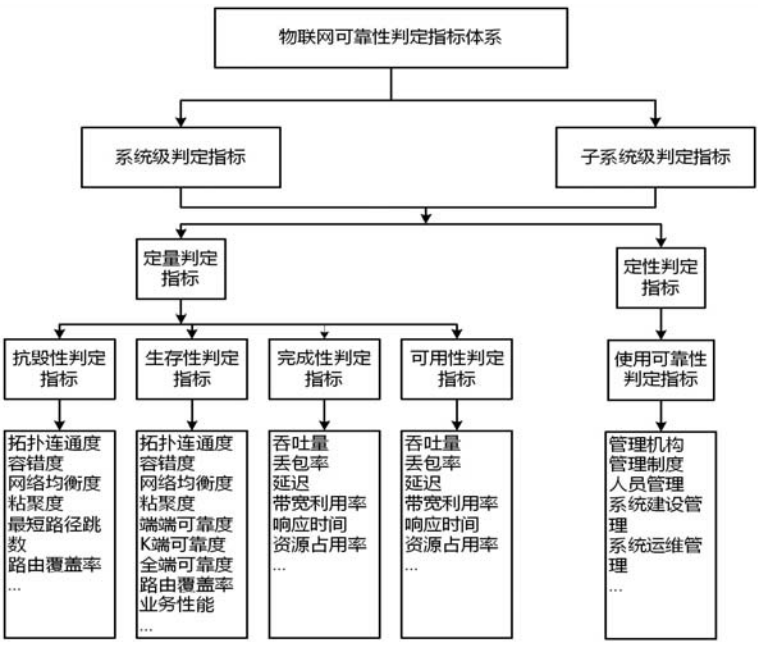

图 3 物联网系统可靠性测评判定指标模型

5 一种基于 TOSSIM 的无线传感器网络安全性测评工具

无线传感器网络作为物联网感知层的重要组成部分,在文物保护、环境监测、安防等领域已得到广泛应用,并普遍采用 TinyOS 作为传感网节点操作系统。但是 TinyOS 为了尽量降低能耗,舍弃了经典操作系统常用的内存管理和安全机制,这就使 TinyOS 在恶意攻击面前非常脆弱。当前很多已经商业化的测试仿真工具并不适合对 TinyOS 进行安全仿真与检测。

针对这一问题,中国软件评测中心自主开发了一套基于 TOSSIM (TinyOS Simulator 是 TinyOS 携带的仿真器,可仿真一个完整的基于 TinyOS 操作系统的传感网络)无线传感器网络安全性测评工具,能够提供从数学仿真到物理仿真的多层次仿真测试环境,可以为无线传感网提供信息安全方面的先期概念演示、解决方案筛选与验证、传感网安全专项任务模拟与测量等服务。

5.1 工具架构

工具主要由节点接口模块、采样模块和用户端控制模块三大基本部分组成。

1)节点接口模块。

节点接口模块用于获取节点内部变量、无线通信数据等信息。当基于 Zigbee 协议帧格式的数据在节点转发时,通过侦听接口,工具可以获取节点通信数据;模块也可以在待测节点程序中按照一定的格式调用接口命令,以获取节点内部数据。

2)采样模块。

本工具支持 USB 端口和串口两种作为数据传输口的传感器节点。采样模块的作用相当于是一个数据收集和控制网关。一边通过 USB 或者串口连接传感器节点,一边通过 SPI 总线连接到用户的控制模块。采样模块通过节点接口模块可以获取节点内部变量以及通信数据等信息,并将这些数据信息通过总线传输给用户控制模块。其中,采样模块的硬件载体是自主研发的基于 ARM11 的采集板。

3)用户控制模块。

用户控制模块具有信息处理与人机交互功能,由 SRES(Security & Reliability Emulation System)[12] 仿真系统组成。其中 SRES 是在 TOSSIM 基础上开发的仿真系统[12]。SRES 系统结构与工作流程图见图 4。

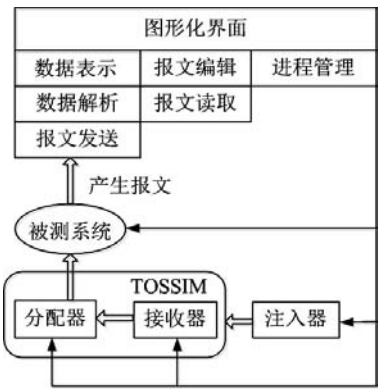

图 4　SRES 系统结构与工作流程图

5.2　工具功能设计

本工具采用模块化设计,可适用于大规模的无线传感器网络应用,能够实时收集网络中被测节点的运行情况并进行记录和分析;在不影响系统正常工作及无需对网络进行拆装的情况下,可对大量传感器节点程序进行升级。为物联网的测试提供了真实的软硬件基础平台和物理环境,提供了脚本形式的接口与多种可视化用户接口。

6　结束语

物联网是无线通信技术、海量信息处理技术、异构网络接入技术等信息技术的高度集成运用。物联网的应用所带来的安全风险是对传统信息安全技术和防范措施的巨大挑战,只有不断完善检测技术手段,才能为物联网的大规模应用构建起安全屏障。

参考文献:

[1] 武传坤. 物联网与信息安全[R]. 出版地不祥:出版者不详,2010.

[2] 武传坤. 物联网信息安全架构初探[J]. 中国科学院院刊,2010(4):411-419.

[3] Wang Yitao. Scalable emulation of tinyos applications in heterogeneous network scenarios[C]//IEEE 6th International Conference on Mobile Ad-hoc and Sensor Systems. Macau, China:[s. n.],2009:140-149.

[4] Alzaid M, Abanmi S. A sensor network test-bed for wormhole attacks[C]//AusCERT. Gold Coast, Australia:[s. n.], 2008.

[5] Gorecki C, Behrens C, Westphal D, et al. TAP-SNS - A test platform for secure communication in wireless sensor networks for logistic applications[C]//12th International Sensor Conference. Hannover:[s. n.],2005:335-340.

[6] 熊　健. 基于场景的构件软件可靠性测试技术研究[D]. 长沙:国防科技大学,2005.

[7] AGREE. Reliability of Military Electronics Equipment:Report[M]. Washington, D C:US Government Printing Office,1957.

[8] 白广忱,黄洪钟. 机械系统可靠性的多目标模糊优化设计[J]. 机械设计,1998(1):12-13.

[9] 丁开盛,张学渊,梁雄健. 通信网可靠性的定义及其综合测度指标[J]. 通信学报,1999,20(10):75-78.

[10] 武小悦,沙基昌,党晓玲,等. 系统可靠性预计与分配集成系统的设计与实现[J]. 计算机工程与应用,1999,35(11):44-46.

[11] 李　维,苗　勇,汤业伟,等. 物联网系统可靠性检测与评估技术[J]. 软件,2012,33(4):1-4.

[12] 李　维,刘　冬,骆俊瑞. 一种面向 TinyOS 的物联网系统信息安全测评工具[J]. 软件,2012,33(2):1-4.

(上接第 103 页)

[8] 兰　陵. 关注视频服务器[J]. 微电脑世界,1999(44):58-59.

[9] 黄淼英. 远程视频传输控制和硬盘录像系统的软件设计[D]. 南京:南京理工大学,2005.

[10] 梁永全,邓隆兴. 多媒体数据存储[J]. 计算机世界,1998(37):152-154.

[11] 蔡　明,任绮念,易剑光. 视频监控系统中的视频存储系统的设计与实现[J]. 江南大学学报,2003(2):115-118.

[12] 谢建国,陈松乔. 视频存储技术发展综述[J]. 计算机工程与应用,2002(9):17-19.

[13] 张明亮,张宗杰. 浅析 FAT32 文件系统[J]. 计算机与数字工程,2005(1):56-59.

[14] 何　炬,袁　宇. 基于 SAN 的视频监控存储文件系统设计[J]. 电视技术,2011(13):98-101.

[15] 何　炬. 基于 IP-SAN 的视频监控存储系统关键技术研究[D]. 上海:上海交通大学,2011.