第 38 卷 第 11 期
Vol.38 No.11

计 算 机 工 程
Computer Engineering

2012 年 6 月
June 2012

·开发研究与设计技术· 文章编号：1000—3428(2012)11—0268—03 文献标识码：A 中图分类号：N945

远程实时健康监护系统数据传输及安全性研究

陈苏蓉，王杰华，朱晓辉，邵浩然，何海棠

(南通大学计算机科学与技术学院，江苏 南通 226019)

摘 要：为实现传感器和数据中心间的双向数据传输，提出一种远程实时健康监护系统。设计包括微型生理信息采集器、数据传输系统和实时服务支撑平台的系统架构，使用蓝牙、GPRS 技术，并以智能手机为媒介实现数据双向传输，利用 IOCP 协议、动态密钥、数据验证、防恶意攻击等方法提高数据传输质量。实验结果表明，该系统具有较好的可靠性和安全性。

关键词：健康监护；数据传输；数据验证；数据安全；数据加密；IOCP 协议

Research on Data Transmission and Security for Remote Real-time Health Monitor System

CHEN Su-rong, WANG Jie-hua, ZHU Xiao-hui, SHAO Hao-ran, HE Hai-tang

(College of Computer Science and Technology, Nantong University, Nantong 226019, China)

【Abstract】In order to solve the problem of reliability and security for the two-way data transmission between sensor and data center, this paper presents a remote real-time health monitor system. It designs the system architecture which includes micro physiological information terminal data transmission system and real-time service support platform. It uses Bluetooth, GPRS technologies and smart phones as medium to realize two-way transmission of data, and enhances the data transmission quality by using IOCP protocol, dynamic encryption key, data validation, anti-malware attacks. Experimental results show that the system has good reliability and security.

【Key words】health monitoring; data transmission; data validation; data security; data encryption; IOCP protocal

DOI: 10.3969/j.issn.1000-3428.2012.11.081

1 概述

传统的健康监护系统主要包括 2 种[1-2]：(1)24 h 记录心电数据的 Holter 系统，它可以让病人随身携带，但无法进行实时诊断。(2)病房使用的床边监护系统，只能在医院固定地点使用。随着计算机技术、传感器技术及医疗器械技术的发展，利用微型传感器来对人体进行健康监护成为目前医疗仪器领域研究的重点[3-5]。美国麻省理工学院研发了指环传感器，可监测心脏活动数据，并利用无线传输数据。但由于其功能单一、造价昂贵，因此目前还处于实验室阶段。日本的 WIN Human Recorder 公司研制了一种只有 7 g 重量的体征信号采集系统 HRS-I[6]，但也存在采集数据单一，在生理数据异常时无法自动报警等问题。这些系统目前还处于实验研究阶段，因此，针对生理数据采集后数据远程传输过程中的可靠性及安全性等问题都没有做深入研究，目前还没有一套成熟有效并可真正投入商业运营的生理健康数据远程传输的解决方案。

本文利用光学传感、光谱分析及微型传感器等技术成功研发了一种便携式远程实时健康监护系统，重点研究如何实现生理数据的远程传输及传输过程中的可靠性和安全性问题。

2 系统架构

系统主要由微型生理信息采集器、数据传输系统和实时服务支撑平台 3 个部分组成，其架构如图 1 所示。系统基本工作流程为：微型生理信息采集器(以下简称 Device)佩戴于用户耳朵上并采集生理健康数据；数据通过蓝牙发送到用户智能手机(以下简称 Unit)；Unit 通过 GPRS 或 WCDMA 把数据远程传输到 Center 服务器；Center 服务器对数据进行必要的验证后存入数据库；用户及相关授权的医生、家人和朋友可以通过 Web 来查询个人生理健康数据；当用户生理健康数据异常时，Center 端通过数据库服务器向呼叫中心报警，呼叫中心按照一定的优先级别自动依次向用户本人、经授权的家人及朋友甚至用户当前所在地的 120 联系，请求及时的帮助和医疗救助。

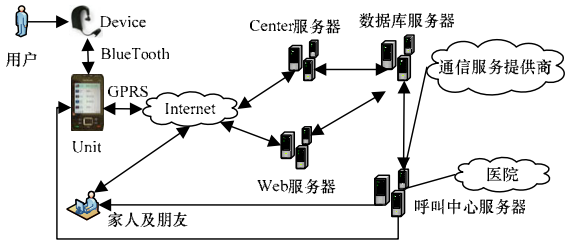


图 1 本文系统架构

基金项目：江苏省“六大人才高峰”基金资助项目(2010-WLW-006)；江苏省高校科研成果产业化推进基金资助项目(JHB2011-45)；江苏高校优势学科建设工程基金资助项目；南通市基础应用研究基金资助项目(K2010067, BK2011072, K2010028, BK2011025)；南通市科技公共服务平台计划基金资助项目(DE2010003)；上海市信息安全综合管理技术研究重点实验室基金资助项目(AGK2009006)；南通大学基础研究基金资助项目(10Z035)

作者简介：陈苏蓉(1977－)，女，讲师、硕士，主研方向：分布式软件开发，网络安全；王杰华(通讯作者)、朱晓辉、邵浩然，副教授、硕士；何海棠，讲师、硕士

收稿日期：2011-10-19 **E-mail：**firstemail@ntu.edu.cn

本文系统中各主要设备功能如下：(1)Device：是一个微型传感器，佩戴于用户耳朵上，内部集成了光电传感模块、数据采集与处理模块、蓝牙模块、驱动电池模块及运动传感模块。(2)Unit：是一个安装有专用数据传输程序的智能手机，作为数据的发送和接收的中间媒介。(3)Center 服务器：接受 Unit 传输来的数据，完成对数据的合法性验证后保存到数据库服务器，也可以向 Unit 发送指令，实现双向数据通信。(4)数据库服务器：存储生理参数数据。(5)WEB 服务器：为用户及其经过授权的医生、家人及朋友提供查询服务。(6)呼叫中心服务器：当用户生理健康数据发生异常时，Center 服务器自动截获并通过数据库服务器向呼叫中心发送报警，呼叫中心自动响应并以一定的优先级别依次与用户本人、用户授权的家人及朋友甚至用户当前所在地的 120 联系。

3　数据传输系统设计

整个数据传输系统包括 2 个部分：(1)Device 与 Unit 间的双向数据传输。(2)Unit 与 Center 服务程序间双向数据传输。系统中引入了智能手机作为数据传输的媒介来实现 Device 与 Unit 间的蓝牙数据通信，从而建立 Device 到 Unit 端的双向数据通信。同时利用手机 GPRS(WCDMA)技术来现实 Unit 到 Center 数据中心间的双向数据通信。

3.1　数据包格式

由于涉及到 Device、Unit 和 Center 三方的双向数据通信，因此需要制定统一的数据包格式，数据包分为包头和包体 2 个部分，包头结构如表 1 所示。

表 1　包头结构

范围/Byte	描述	取值
1~3	Start Marker	0XFF00FF
4~7	Device ID	Depend on Device
8	Chunck Type	无
9~12	Time Stamp	YY:MT:TT:TT
13	Total length of Data Chunks	无
14~15	Encrption Num	无
16~19	Checksum	无

包头结构前 3 Byte 是固定掩码，值为 OXFF00FF，表示包头的开始；4 Byte~7 Byte 表示 Device 蓝牙设备号，用来唯一表示一个 Device；8 Byte 表示数据包流向及具体功能；9 Byte~12 Byte 记录生理参数采集的时间；13 Byte 表示包体长度；14 Byte~15 Byte 是一个动态产生的随机数，用于对包体数据加密；16 Byte~19 Byte 是包头校验位。用于对 1 Byte~15 Byte 进行数据校验，在 Device 和 Unit 间数据传输时采用简单的累加计和方法生成校验位，在 Unit 和 Center 间进行数据传输时用 Hash 算法生成校验位。

包体结构主要包括掩码起始位、数据位及校验位构成。其中，1 Byte~3 Byte 表示掩码字段，表示包体开始；4 Byte~23 Byte 每个字节分别记录心率、体温、血氧饱和度等 20 个不同的生理参数；24 Byte~27 Byte 是校验位。

3.2　数据传输协议

由于 Device 与 Unit 之间是近距离的一对一通信，因此采用蓝牙技术来实现数据传输。而 Unit 与 Center 间的通信需要经过 GPRS(WCDMA)、Internet 等多个网络的传递，所以需要重点考虑数据传输的可靠性和安全性问题，同时还需要尽可能提升 Center 端服务程序的并发性能。

IOCP(I/O Completion Port)模型也叫完成端口，是一种高效的 I/O 模型，其最大优点在于用很少的服务器端线程就可以并发处理大量的网络连接和数据传输，大大减少 CPU 进行线程切换的工作，极大地提高了网络数据传输的并发性[7]，因此，项目中选用 IOCP 协议来实现 Unit 和 Center 间的双向数据传输。

4　数据传输系统实现

由于数据从 Device 端采集到传输到 Center 端接收过的程中需经过蓝牙、GPRS(WCDMA)、Internet 等多种不同的通信网络，因此数据传输过程中的可靠性和安全性显得尤为重要。这里通过对数据包进行必要的验证来确保数据传输过程中的可靠性。

4.1　Device 与 Unit 间数据完整性验证

受 Device 计算性能及电池容量限制，在 Device 端不适宜做大量的复杂计算。但考虑到蓝牙通信本身的不稳定性和易受干扰性，因此，需要通信双方对数据包做基本的数据完整性验证。这里采用对数据包进行累加计和方法来生成校验码，这样既可兼顾数据完整性要求，也充分考虑了 Device 端的计算性能的限制。数据完整性验证步骤如下：

(1)Device 采集生理参数，利用累加计和方法分别计算包头和包体校验码并填入各自的 Checksum 字段，然后向 Unit 发送数据包。

(2)Unit 接收到数据包后分解成包头和包体，并分别重新计算校验码。

(3)若新校验码和数据包中原来的校验码一致，说明数据在传输过程中没有改变，数据完整性验证结束，否则 Unit 丢弃该数据包并向 Device 发送一个请求消息包，请求 Device 重发数据包。

(4)若连续 3 次重发数据包都验证失败，则 Unit 向用户报警显示错误信息，并把该信息发送到 Center，由 Center 记录到日志文件中。

(5)重复步骤(1)。

同理，Unit 向 Device 发送数据包时的验证方法类似，这里不再赘述。

4.2　Unit 与 Center 间数据完整性验证

Unit 与 Center 间的远程数据传输需要经过 GPRS(WCDMA)、Internet 等多个网络，需进行更严格的数据完整性验证，因此系统采用 Hash 算法，其验证步骤如下：(1)Unit 对 Device 传来的数据包完成完整性验证。(2)Unit 利用 Hash 算法重新生成包头和包体验证码，并分别填入到各自的 Checksum 字段，然后 Unit 向 Center 发送数据包。(3)Center 接收到数据包后拆解成包头和包体 2 个部分，并用相同的 Hash 算法重新计算新校验码。(4)若新校验码和数据包中原来的校验码一致，则说明数据在传输过程中没有改变，数据完整性验证结束，否则 Center 丢弃该数据包并向 Unit 发送一个请求消息包，用于请求 Unit 重发该数据包。(5)如果连续 3 次重发数据包都验证失败，那么在 Unit 端向用户报警显示错误信息，并把该信息发送到 Center，由 Center 记录到日志文件中。(6)重复步骤(1)。

Hash 算法描述如下：

(1)定义 4 Byte 的 HASH 密码位 H=1，整型变量 r=4。

(2)依次取数据包中 1 Byte 的 B。

(3)H^=((*H*&63)+*r*)×((uint)*B*+(*H*<<8)。

(4)返回步骤(2)直到取完包中所有字节。

(5)把 H 保存到校验位字段并结束。

同理，Center 向 Unit 发送数据包时的验证方法类似，这

里不再赘述。

4.3 数据加密保护

Unit 与 Center 间的数据需要经过多种网络远距离传输，为防止恶意用户窃取数据，必须对数据进行加密。这里采用了 AES 对称加密算法，同时为了进一步增加数据包被破译的难度，系统采用了动态密钥技术。当 Device 开机后与 Unit 及 Center 三者间首先建立连接，并由 Center 进行设备合法性验证，然后由 Center 动态产生一个 2 Byte 随机数保存到包头中的 Encrption Num 字段并发送给 Unit。当连接建立后，Unit 即以该随机数作为加密密钥，用 AES 加密算法对包体中的生理健康数据进行加密，当 Center 接收到 Unit 传输过来的数据包时，利用同样的密钥对数据进行解密。这样使得用户每次开机时，加密密钥都是动态随机产生的，从而大大增加了破译难度，增强了数据在传输过程中的安全性。

4.4 数据防篡改验证

数据加密只能限制非法用户获取数据包中内容，但无法限制非法用户截获数据包并对数据包内容做修改后再转发给 Center 端服务程序，从而形成大量垃圾信息，因此，必须在 Center 端建立鉴别机制来判别数据是否被篡改。

在数据完整性验证中，系统采用 Hash 算法，因此，本质上在对数据完成完整性验证的同时也相应完成了数据的防篡改验证。因为当非法用户篡改数据包中的某个信息时，必然导致在验证过程中新生成的 Hash 结果和数据包中原来的 Hash 结果不一致。因此，Hash 验证算法在实现了数据完整性验证的同时也实现了数据防篡改的验证。

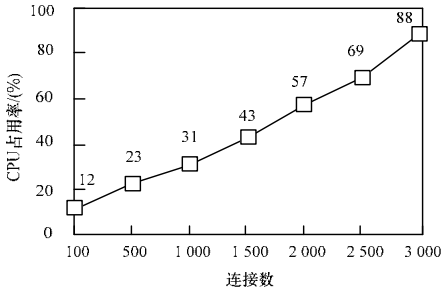
4.5 恶意攻击处理

由于数据远程传输的特性，因此很难避免数据包被恶意窃取。当恶意用户窃取数据包后，一方面可以利用多线程技术复制并向 Center 端服务器程序大量发送相同内容的数据包，从而导致 Center 服务器程序大量接收重复数据。另一方面也可以对数据包做恶意修改后再大量发送非法数据包，从而导致 Center 端服务器因需要对大量非法数据包进行验证而影响正常数据包的接收，无法为合法用户提供服务[8]，这也是 DDoS 攻击常用的手段。因此，需要在 Center 端服务器程序设立相应的防范机制。

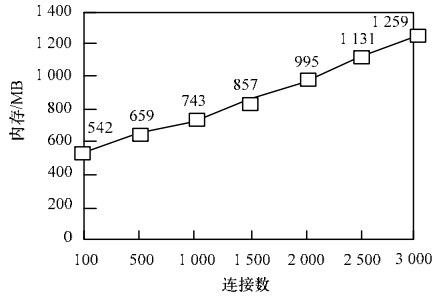
针对第 1 种情况，首先在 Center 服务器内存中保存所有 Device 的 ID 编号及该 Device 最后一次发送数据包的时间戳，并设定允许 Device 连续传送数据的最小时间间隔，在内存中保存以前进行过攻击的 Device 黑名单信息。采用 HashTable 结构在内存中存放 Device 的 ID 号以及该 Device 最后一次发送数据包的时间戳信息。采用 HashTable 结构的好处在于查找时间戳的时间复杂度为 $O(1)$，因此，可以大大提高数据查找的速度。当前后 2 个数据包的时间差小于系统允许的最小时间时，则可认为该数据包是一个恶意数据包，系统把该恶意包丢弃，并把该 Device 的 ID 编号记录到系统黑名单中，最后主动断开与该传感器的网络连接，从而不再接收该 ID 所发送过来的数据包。第 2 种情况的处理与第 1 种情况类似，当连续 3 次判断到同一个 Device 的数据包验证错误时，把该 Device 列入到黑名单中并主动断开与该 Device 的连接。

5 实验结果与分析

本文系统中开发的 Unit 数据传输程序基于 J2ME 平台，Center 服务器程序采用 C++及 IOCP 模型。实验测试环境如下：Center 服务器为 Xeon5420，8 GB 内存，RAID5 800 GB 硬盘，千兆带宽，Windows Server2003 R2；客户端机器硬件配置为 Intel 酷睿 2，4 GB 内存，ATA 640 GB 硬盘，千兆带宽，Windows XP。并开发了基于多线程的客户端测试程序，每个线程模拟一个 Unit 向 Center 服务器程序发送数据包，设定数据包发送的最小时间间隔为 2 s。正常数据测试结果如图 2 所示，其显示了在发送正常数据包情况下并发连接数和 CPU 及内存的之间的关系。



(a)连接数和 CPU 占用率

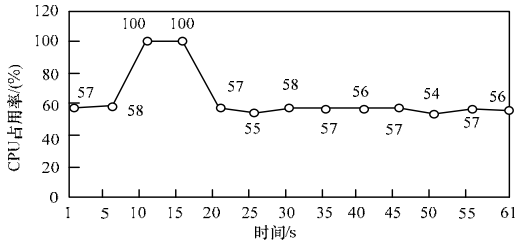


(b)连接数和内存

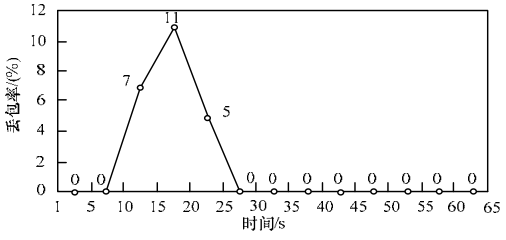
图 2 正常数据测试结果

由图 2 可知，随着并发连接数的增加，内存和 CPU 的资源占用率也称线性增长，Center 端服务器程序具有较高的并发性能，一台 Center 服务器即可支持 3 000 个左右的 Unit 进行并发数据的传输。

为测试 Center 端服务器程序遭受恶意攻击情况下的系统性能，在两组客户端机器上利用测试程序分别模拟 2 000 个 Unit 发送正常数据包进行正常数据传输和 3 000 个 Unit 发送非法数据包进行恶意攻击。首先运行正常的模拟程序 10 s，系统处于稳定的状态后，再向 Center 端发送非法数据包，测试情况如图 3 所示。



(a)CPU 占用率变化



(b)丢包率变化

图 3 恶意攻击测试结果

(下转第 273 页)

均错误率为 6.94%，此时正确率为 93.06%。

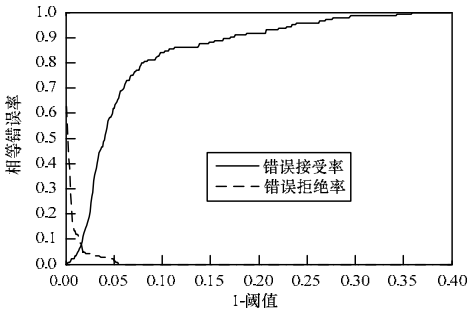


图 5　1-阈值与 FAR、FRR 的对应关系

表 2　相关系数阈值与 FAR、FRR 和 TER 的关系

阈值	FAR	FRR	TER
0.986	0.062 5	0.090 3	0.152 8
0.985	0.069 4	0.083 3	0.152 7
0.984	0.076 4	0.083 3	0.159 7

6　结束语

本文给出一种利用步态加速度进行疲劳状态检测的方法。介绍了步态加速度数据采集、基于相关系数的数据处理和疲劳检测方法。实验结果表明，该方法不依赖主观判断，不会给人的行动或者身体带来不便，具有较好的应用前景。但是，由于步态数据易受地面状况、鞋型、身体状况等因素的影响，因此仍需做进一步改进。

致谢　本文相关研究获得了清华大学——瑞萨电子联合实验室的大力支持，感谢清华大学老师的指导及所提供的设备与场地，感谢实验室师生的积极配合。

参考文献

[1] 詹发尚. 疲劳研究现状[J]. 中国行为医学科学, 2006, 15(2): 188-189.

[2] 王　颖, 赵梅雪. 石家庄市某校中学生作息与学习疲劳情况调查[J]. 中国学校卫生, 2001, 22(2): 158-159.

[3] 牛　杰, 沈晓峰. 疲劳状态监控系统中眼睛状态检测方法[J]. 计算机工程, 2009, 35(17): 195-197.

[4] Tsopanakis C, Tsopanakis A. Stress Hormonal Factors, Fatigue, and Antioxidant Responses to Prolonged Speed Driving[J]. Pharmacology Biochemistry and Behavior, 1998, 60(3): 747-751.

[5] Herlofson K, Larsen J P. Measuring Fatigue in Patients with Parkinson's Disease——The Fatigue Severity Scale[J]. European Journal of Neurology, 2002, 9(6): 595-600.

[6] Okuyama T, Akechi T, Kugaya A, et al. Development and Validation of the Cancer Fatigue Scale: A Brief, Three-dimensional, Self-rating Scale for Assessment of Fatigue in Cancer Patients[J]. Journal of Pain and Symptom Management, 2000, 19(1): 5-14.

[7] Hong Youlian, Li Jingxian, Daniel T F. Effect of Prolonged Walking with Backpack Loads on Trunk Muscle Activity and Fatigue in Children[J]. Journal of Electromyography and Kinesiology, 2008, 18(6): 990-996.

[8] Jorunn L, Helbostad S L. Physical Fatigue Affects Gait Characteristics in Older Persons[J]. Journal of Gerontology: Medical Sciences, 2007, 62(9): 1010-1015.

[9] 王　犇, 袁　涛, 梁　灿. 基于加速度特征点提取的步态身份认证[J]. 清华大学学报: 自然科学版, 2009, 49(10): 25-28.

编辑　刘　冰

(上接第 270 页)

由图 3 可知，Center 端服务器程序在前 10 s CPU 资源占用率为 57%左右，丢包率为 0%；受到非法数据包攻击后，第 10 s~第 20 s 内 CPU 资源占用率从 58%上升到 100%，然后逐渐下降，同时丢包率也从 0%先上升到 11%然后再下降到 0%；在 20 s 以后，CPU 资源占用率恢复到 57%左右，丢包率也恢复到 0%。原因在于前 10 s Center 处理 2 000 个并发的正常数据包，所以性能表现稳定；从第 10 s 开始，Center 端需要同时处理 2 000 个并发的正常数据包和 3 000 个并发的非法数据包，从而引起 CPU 资源占用率的提升，同时，因为系统来不及处理如此多的并发连接而出现数据丢包的情况，但由于 Center 服务器程序在发现非法数据包时会把该客户端列入到黑名单中，并主动断开相应的连接，因此客户端无法继续再向服务器发送数据包，在 20 s 以后系统性能又趋于稳定。以上可以看出，系统采用的防恶意攻击技术有效增强了 Center 服务器程序的安全性和稳定性，避免因受到恶意攻击而使系统崩溃。

6　结束语

本文提出一种远程实时健康监护系统。给出了数据传输系统设计，阐述了数据加密保护、数据篡改验证和恶意攻击的处理方法。实验结果表明，该系统能保证数据传输过程中的可靠性、安全性，并能有效阻止恶意用户对 Center 的攻击。今后需要重点研究如何提升 Center 端并发性能，实现分布式部署，从而进一步提升系统的稳定性和可靠性。

参考文献

[1] Zhang Ying, Xiao Hannan. Bluetooth-based Sensor Networks for Remotely Monitoring the Physiological Signals of a Patient[J]. IEEE Transactions on Information Technology in Biomedicine, 2009, 13(6): 1040-1048.

[2] Chow C, Herry C. Enabling Technologies for Wireless Body Area Networks: A Survey and Outlook[J]. IEEE Communications Magazine, 2009, 47(12): 84-93.

[3] 陈　真, 汪小燕, 王　钰. 智能网络关爱系统的设计与实现[J]. 微电子学与计算机, 2010, 27(9): 144-146.

[4] 鸿　强, 苗长云, 张龙宇, 等. 心电医疗监护物联网关键技术研究[J]. 计算机应用研究, 2010, 27(12): 4600-4603.

[5] 范晓武. 基于嵌入式设备的家庭健康监护系统的设计与实现[J]. 浙江工业大学学报, 2010, 38(3): 289-293.

[6] Shinichi K. Wearable Health Monitoring Sensor Debuts in Japanese Market[EB/OL]. (2010-11-21). http://techon.nikkeibp.co.jp/english/NEWS_EN/20100119/179393/.

[7] 陈怀松, 陈家琪. IOCP 写服务程序时的关键问题研究[J]. 计算机工程与设计, 2010, 31(17): 3793-3796.

[8] 张　洁, 秦　拯. 改进的基于熵的 DDoS 攻击检测方法[J]. 计算机应用, 2010, 30(7): 1778-1781.

编辑　刘　冰