为普适健康而生的躯感网及其信息安全

鲍淑娣,陈萌

宁波工程学院电子与信息工程学院,宁波 315211

摘要　由人体生物传感器构成的躯感网是物联网在医疗健康领域的主要表现。本文从健康信息化国家战略出发,阐述躯感网技术及应用对健康信息化发展的重要意义,从通信技术层面分析了躯感网技术的发展现状及未来趋势,并重点论述了健康数据的安全及隐私保护机制。

关键词　健康信息化;物联网;躯感网;信息安全

健康信息化是新兴信息技术与医疗健康服务的有机结合,是促进医疗资源共享与充分利用、实现以人为本的个性化医疗保健服务的有效路径。自20世纪90年代以来,以医疗信息电子化与互通共享为核心的健康信息化技术发展迅猛,并在全球范围内受到广泛重视,中国医疗信息电子化紧密结合社区卫生信息化而取得了卓越进展。为进一步应对人口老龄化与改善慢病防控,2013年9月国务院发布《关于促进健康服务业发展的若干意见》(简称《意见》),提出要推进健康服务信息化,制定相关信息数据标准,加强医院、医疗保障等信息管理系统建设,充分利用现有信息和网络设施,尽快实现医疗保障、医疗服务、健康管理等信息的共享。《意见》还提出,到2020年,中国将基本建立覆盖全生命周期、内涵丰富、结构合理的健康服务业体系,健康服务业总规模达到8万亿元以上,成为推动经济社会持续发展的重要力量。为持续推进健康中国建设,全面提升人民健康素质,2016年10月国务院又印发了《"健康中国2030"规划纲要》,明确提出要创新互联网健康医疗服务模式,持续推进覆盖全生命周期的预防、治疗、康复和自主健康管理一体化的国民健康信息服务,实施健康中国云服务计划,发展智慧健康医疗便民惠民服务,加强健康医疗大数据应用体系建设,推进基于区域人口健康信息平台的医疗健康大数据开放共享、深度挖掘和广泛应用。中国健康信息化程度正以前所未有的速度推进。

从技术层面来说,健康信息化的核心是电子病历(electronic medical record,EMR)、电子健康档案(electronic health record,EHR)和个人健康档案(personal health record,PHR)的管理与应用。目前国内对于EHR和PHR还没有形成统一概念。依据美国食品药品管理局的表述,EHR记录的是符合信息标准的居民基本信息及其在医疗卫生机构内直接形成的具有保密备查价值的电子化历史记录。EHR与EMR的主要区别在于EMR往往局限于在某个医疗卫生机构内直接形成的电子化记录,而EHR则是个人在不同医疗卫生机构形成的EMR的综合。为便于医疗数据互通共享,国际标准组织制定了面向EMR的DICOM(digital imaging and communications in medicine)和面向EHR的HL7(health level 7)。与EHR不同,PHR是指可由个人自主管理的在院外(如社区、家庭、工作环境中)形成的电子化健康历史记录。以人体为中心、以可穿戴/植入式生物传感器为主而构建的躯感网(body sensor network,BSN)成为PHR的重要采集平台[1]。未来,如图1所示的医疗健康信息系统将实现个人健康档案与电子健康档案的充分整合,为真正实现个性化医疗健康提供服务平台,逐步形成以健康和预防为核心的卫生服务模式。

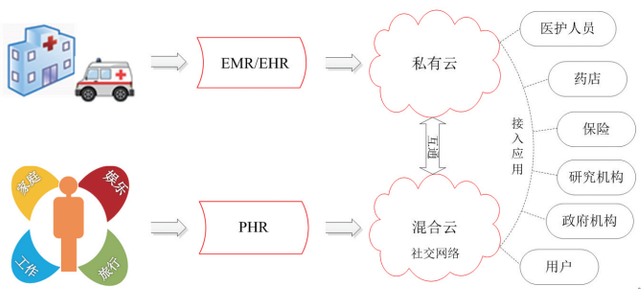

图1　以个人为中心的健康医疗信息系统示意

收稿日期:2016-11-02 ;修回日期:2016-12-13

基金项目:浙江省自然科学基金项目(LY14F010005);国家自然科学基金项目(61102087,61671260);宁波市自然科学基金项目(2016A610111);浙江省教育厅科技项目(Y201533194);中国科学院健康信息学重点实验室开放基金项目

作者简介:鲍淑娣,副教授,研究方向为移动健康、信息安全,电子信箱:shudi.bao@nbut.edu.cn

引用格式:鲍淑娣, 陈萌. 为普适健康而生的躯感网及其信息安全[J]. 科技导报, 2017, 35(2): 41-44; doi: 10.3981/j.issn.1000-7857.2017.02.004

1 躯感网及其通信技术

躯感网将与家庭、工作、医疗等环境无缝衔接,成为物联网在医疗健康领域的主要表现形式。典型的躯感网节点是穿戴于体表或植入于体内的集生理数据采集与处理、无线通信等功能于一体的生物传感器(图2)。根据其分布情况,可将躯感网节点大致分为3类:1)分布在人体体表或近体表的传感器节点,通常为可穿戴式设备,如手表式脉搏传感器、指环式心率感知器;2)植入人体内的传感器节点,如心脏起搏器、骶神经刺激器;3)活动于体内的传感器节点,如吞入式胃肠内窥镜。传感器节点之间的通信方式主要包括无线射频通信、电子织物、人体通信。

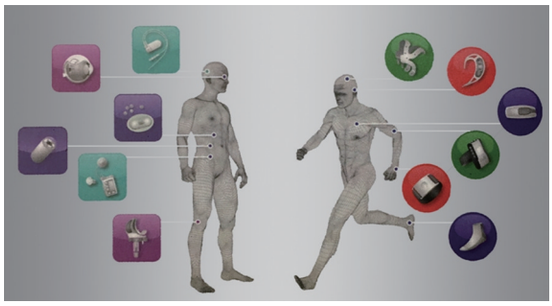

图2 面向医疗健康应用的穿戴式/植入式传感器(从神经刺激器到智能膝关节假体)示意

面向躯感网的无线射频通信技术主要包括体内通信和体外通信两大类型。目前国际上普遍采纳的体内通信协议是植入式医疗通信服务(MICS),其工作频段403~405 MHz,包括若干个带宽为300 kHz的子频段,上限功率为25 μW。人体作为一种通信介质,其产生的阻抗会随着年龄、体重甚至姿势的变化而变化,具有不可预见性[2]。加上个体的差异性,想要准确分析体内通信链路的性能显得极为困难。近年来,适用于躯感网的体外通信技术得到长足发展。IEEE 802.15工作组先后发布了多个短距离无线通信技术,包括IEEE 802.15.1(蓝牙Bluetooth)、IEEE 802.15.3(超宽带Ultra Wideband, UWB)、IEEE 802.15.4(ZigBee)以及最新的IEEE 802.15.6(Wireless Body Area Network,WBAN)[3]。无线通信技术在躯感网应用中依然存在多个技术难点,包括:1)超低功耗设计及供能问题;2)通信可靠性和安全性问题;3)人体各类状态下的网络服务质量稳定性问题。

电子织物是由体积微小、价格低廉的简单芯片、功能纤维和互联部分组成的"特殊"分布式系统。由于资源有限,单个节点一般仅能处理简单计算任务,并且需要系统各组件协作以完成应用任务。另一方面,由于系统织造、使用过程中引入的裁剪、拉扯或者磨损等,容易导致节点之间的通信链接、节点与电源之间的能量路由路径以及节点本身等多方面的故障率[4]。人体通信技术利用人体作为通信的传输介质,通过电容耦合或者电流耦合的方式进行数据传输。简言之,人体通信即是将人体当作数据线进行数据传输。目前,人体通信的理论传输速度为10 Mbit/s,但实际环境中,由于人体不同部位传输速率不同,不同人体的物理特性存在微妙差异,加之环境噪声等因素影响,数据传输速度达不到理论极限值。中国科学院深圳先进技术研究院近来年已制造出可供体验应用的人体通信原型机,并针对人体体表的不同物理特性,在寻找数据传输速度最快、最稳定的表皮信道方面已取得一定进展。人体通信技术未来发展的重要方向包括植入式设备的人体通信、人体通信无线供能和磁场耦合式人体通信[5]。

综上可见,无线射频通信技术仍将是躯感网的主流通信技术,而无线通信所带来的数据安全及用户隐私保护问题将随着躯感网在医疗健康领域的广泛应用而日益突显。

2 数据安全与隐私保护

由躯感网采集的个人健康档案PHR与医疗信息系统中的电子病历EMR、电子健康档案EHR进行互通整合,必将带来巨大的数据安全与隐私保护问题。发达国家在医疗健康信息安全保护方面意识较强,起步较早,相关法律体系也较为健全。例如,美国于1996年通过并于2003年正式实施了HIPAA法案,明确了适用实体、受保护医疗信息类型、医疗信息安全、医疗隐私、数据泄露告知等细则。为推动医疗信息化进程,美国于2009年底进一步提出HITECH法案,为电子健康档案的全面发展保驾护航[6]。

尽管国内外已经在医疗信息化解决方案方面实施了较多研究项目,但针对开放环境中个人健康档案的获取、管理与应用,及其数据安全与隐私保护等问题仍有待广泛研究和积极探索[7]。图1所示的健康信息系统中,健康医疗信息(尤其是个人健康档案)在传输、存储和应用等各环节都存在安全隐患。尤其是躯感网与健康云平台的安全问题正引起人们的关注并逐渐成为研究热点。

作为健康信息系统的安全薄弱环节,无线躯感网的通信安全问题已得到较为深入的研究。美国电子电气工程师协会(IEEE)于2012年公布了无线躯域网(wireless body area network, WBAN)物理层/链路层通信标准,即IEEE 802.15.6[3]。其通信安全方案利用AES-CCM实现数据完整性和加密保护,其中AES(高级加密标准)是高效且安全的对称分组加密算法,CCM是将计数器(CTR)和CBC-MAC(cipher block chaining-message authentication code)模式相结合的分组密码操作方式,用于密码块消息验证;通信双方采用基于椭圆曲线公钥密码的Diffie-Hellman密钥交换算法,生成主密钥。

作为无线躯域网的通用低层通信标准,IEEE 802.15.6的密钥管理机制并不完全适用于躯感网。首先,躯感网节点往往不具备良好的操作界面,凡符合标准的任意两个节点都可以协商生成主密钥而进行通信,从而易遭到冒充攻击。其

次,该方案无法解决因传感器共享而带来的安全问题。实际应用时,一群用户(如家庭成员)可能需要共享可穿戴传感器,在无意识情况下可穿戴传感器的交叉误用情况也可能发生。如果不支持网络节点识别,健康数据来源易被混淆,进而可能导致医疗事故的发生。

2.1　节点动态识别机制

躯感网与其他网络最显著的区别在于,网络节点附着于人体,而人体具备自身的通信传输系统。由于人体通道相对于其他传输通道而言具备充分的安全性,因此将人体通道与无线信道有机结合而发展出来的一种新型生物测定系统有望用于躯感网的密钥共享过程。其基本思想可以表述为:由于同一躯感网的生物传感器依附于同一人体,在人体通道的作用下,同网节点同步检测到的生理信号在某些方面具备高相似性,而异网节点检测到的生理信号却存在显著差异。在这里,生理信号被用于鉴别躯感网节点的网络归属。从本质上来说,生理信号可被认为是一种利用生物测定方法实现身份识别的生物特征源。与一般的生物测定学特征(例如指纹、虹膜)不同,生理信号是一种非稳态的时变信号,具有动态随机性,因而可以被考虑用于网络密钥管理[8-9]。但是,在实际应用时上述方法具有较大的局限性,因为其应用条件是通信双方必须同时具备相应的生理信号检测功能,例如,双方均具备心电图或脉搏波检测功能。

2.2　数据源认证机制

在健康医疗系统中,如果能对躯感网所采集的健康传感数据的来源(包括传感器和用户)进行认证,那么就可以解决因为共享或交叉误用生物传感器而带来的健康数据误存或误用问题。解决数据源认证的传统方法是数字签名和消息认证码。对于很多系统(包括躯感网)而言,数字签名机制因其计算成本过高而不实用;而消息认证码属于链路层方案,对密钥管理有较高要求。

考虑躯感网健康传感数据的特殊性,有较多现有研究利用其生物识别特性而实现数据源用户认证。所涉及的健康传感数据包括心电图[10-11]和脑电图[12-13]两种生理信号。与传统生物识别技术相比,利用心电图/脑电图进行身份识别具有两方面优点:一为活体识别而不易被其他设备模拟,二为时间序列而易于处理。此外,心电图和脑电图为躯感网采集的主要生理信号,相关采集技术发展迅速。

关于心电信号,研究人员提出了多种可用于身份识别的心电信号时频域特征参数,如QRS波三角形角度/面积/周长等时域特征、信号频率倒谱系数、经小波变换和奇异值分解的特征参数等。这些特征普遍适用于恒定的心电波形,在心率变异较大情况下的识别或鉴别准确率会显著降低。为最大限度保留心电信号特征信息,Yang等提出直接利用心电周期波形进行分类或识别[10]。

利用距离或幅度差异来计算测试样本与模板样本之间的匹配度是一类常用识别方法。其中,动态时域归整[11,14]是一种把时间归整和间距测量计算结合起来的非线性归整技术,可以得到具有最大相似性的弯曲路径。另一类方法是基于支持向量机分类器或神经网络分类器或隐马尔可夫模型[15]等对心电信号进行分类,通过规模样本数据的学习训练来估计参数。这类需要预学习的分类方法普遍要求对样本信号进行较长时间的训练,若训练样本数受限,则存在推广能力较差的问题从而导致识别准确率降低。

值得注意的是,虽然不同导联/体位采集到的心电信号存在显著差异,大多数现有研究将源自不同数据库不同导联的心电数据混用而作为性能分析的实验数据。此外,心电身份识别还存在数据时间跨度较小、仅针对静态心电信号以及用户容量受限等有待进一步解决的问题。

2.3　数据静态安全

躯感网所采集的健康传感数据在包括云平台在内的各存储环节也面临着严重的安全威胁[16],因此健康数据的静态安全问题也亟待解决。

解决静态数据安全的主流方法是采用数据加密机制。例如,Mat Kiah等针对电子病历安全问题提出采用高级加密标准AES和安全散列算法SHA-1相结合的加密方法[17]。Huang等提出将电子健康档案分成可识别用户信息和非可识别信息两类,对前一类EHR采用公钥密钥体制进行加密保护,对后一类EHR则采用去标识和假名化方法解决隐私保护问题[18]。Lin等综述了健康云平台的数据安全与隐私保护方法,包括可搜索加密机制、全同态加密机制、基于公钥密码体制的身份基加密机制和属性基加密机制等[19]。

现有研究中针对躯感网静态数据安全的研究较少。Ren等提出一种将健康数据隐藏到非敏感数据的方法,即先对健康数据进行无损压缩后,采用一种随机处理方法将健康数据与非敏感数据进行简单异或操作完成数据隐藏[20]。该方法有两方面主要不足:一是健康数据必须与非敏感数据捆绑,二是非敏感数据量必须远远大于健康数据量。可见,该方法在实际应用中具有很大局限性。Bao等提出的一种健康数据分离自加密方案,初步探讨了云环境中健康数据静态存储安全问题[21]。此外,考虑躯感网节点的低能耗设计需求,不建议采用传统加密算法实现静态数据保护。一个好的设计思路是在对健康传感数据进行压缩的同时融合加密方法。

3　结论与展望

本文从通信技术层面分析了躯感网技术的发展现状及未来趋势,并重点介绍了健康数据的安全及隐私保护机制。可以预见,随着躯域网技术的发展与应用,在医院外形成的、可自主管理的个人健康档案将呈现爆发式增长,健康信息化也将由此进入新的发展阶段;在个性化健康医护需求日益增加的将来,以人为核心、以健康监测和辅助诊断为主要应用的躯感网将在移动医疗系统中发挥更加显著的作用;而以低成本、易操作、广覆盖和个性化为特点的移动医疗系统必将

积极推动医疗服务模式由现在的以治疗为主的集中模式,逐步转变到以预防为主的医院、社区、家庭和个人相结合的分布模式。

参考文献(References)

[1] Yang G Z. Body sensor networks[M]. 2nd ed. Berlin: Springer, 2014.

[2] 林伟兵, 雷声, 韦彩虹,等. 体域网传感器节点和无线通信技术研究进展[J]. 生物医学工程学杂志, 2012, 29(3): 568—573.

[3] IEEE Standards Association. IEEE standard for local and metropolitan area networks-part 15.6: Wireless body area networks[J]. IEEE Standard for Information Technology, IEEE, 2012, 802(6): 1-271.

[4] 郑能干, 吴朝晖, 林曼, 等. 电子织物研究进展[J]. 计算机学报, 2011, 34(7): 1172—1187.

[5] 汪啸尘, 张广浩, 霍小林. 人体通信技术研究进展[J]. 中国生物医学工程学报, 2015, 34(3): 345-353.

[6] Blumenthal D. Launching HITECH[J]. The New England Journal of Medicine, 2011, 362(5): 382-385.

[7] Senor I C, Aleman J L F, Toval A. Personal health records: New means to safely handle health data[J]. Computer, 2012, 45(11): 27-33.

[8] Poon C C Y, Zhang Y T, Bao S D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health[J]. IEEE Communications Magazine, 2006, 44(4): 73-81.

[9] Bao S D, Poon C C Y, Zhang Y T, et al. Using the timing information of heartbeats as an entity identifier to secure body sensor network[J]. IEEE Transactions on Information Technology in Biomedicine, 2008, 12(6): 772-779.

[10] Yang M X, Liu B, Zhao M M, et al. Normalizing electrocardiograms of both healthy persons and cardiovascular disease patients for biometric authentication[J]. Plos One, 2013, 8(8): e71523-e71523.

[11] 卢阳, 鲍淑娣, 周翔, 等. 基于动态心电信号的实时身份识别算法[J]. 计算机应用, 2015, 35(1): 307-310.

[12] 刘泉影, 毛承胜, 聂碧娟, 等. 普适环境下基于脑电的身份及上下文状态识别[J]. 东南大学学报(自然科学版), 2010, 40(增刊2): 263-266.

[13] Campisi P, Rocca D L. Brain waves for automatic biometric-based user recognition[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(5): 782-800.

[14] 杨立才, 沈君, 鲍淑娣, 等. 基于PLR-DTW 的ECG 身份识别方法[J]. 生物医学工程学杂志, 2013, 30(5): 976-981.

[15] Rabhi E, Lachiri Z. Biometric personal identification system using the ECG signal[C]//Proceedings of IEEE Computing in Cardiology Conference. Zaragoza: IEEE, 2013: 507-510.

[16] Caldeira J M L P, Rodrigues J J P C, Lorenz P. Toward ubiquitous mobility solutions for body sensor networks on healthcare[J]. IEEE Communications Magazine, 2012, 50(5): 108-115.

[17] Mat Kiah M L, Nabi M S, Zaidan B B, et al. An enhanced security solution for electronic medical records based on AES hybrid technique with SOAP/XML and SHA-1[J]. Journal of Medical Systems, 2013, 37(5): 1-18.

[18] Huang L C, Chu H C, Lien C Y, et al. Privacy preservation and information security protection for patients´ portable electronic health records[J]. Computers in Biology and Medicine, 2012, 39(9): 743-750.

[19] Lin H, Shao J, Zhang C, et al. CAM: Cloud-assisted privacy preserving mobile health monitoring[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(6): 985-997.

[20] Ren J, Wu G, Yao L. A sensitive data aggregation scheme for body sensor networks based on data hiding[J]. Personal and Ubiquitous Computing, 2013, 17(7): 1317-1329.

[21] Bao S D, Lu Y, Chen M, et al. A data partitioning and scrambling method to secure cloud storage with healthcare applications[C]//Proceedings of IEEE International Conference on Communications. London: IEEE, 2015: 2075-2079.

Body sensor network and its security concerns for pervasive healthcare

BAO Shudi, CHEN Meng

School of Electronic and Information Engineering, Ningbo University of Technology, Ningbo 315211, China

Abstract The body sensor network contains wearable and/or implantable biosensors and serves as an important front-end platform for Internet of Things in the healthcare domain. From the point of view of the national health information development strategy, this paper discusses the importance of the body sensor network technology and its applications in the development of health information. The current status and future trends of the body sensor network technology are reviewed from the perspective of communication technology, with emphasis on security and privacy mechanisms of sensitive health data.

Keywords health information; internet of things; body sensor network; information security

(责任编辑 刘志远)