doi:10.11959/j.issn.2096-3750.2017.00015

智能硬件发展的若干关键技术

孙玲玲[1]，苏江涛[1]，黄汐威[1]，金洁[1]，李文钧[1]，王小军[2]
（1. 杭州电子科技大学射频电路与系统教育部重点实验室，浙江 杭州 310018；2. 都柏林城市大学电子工程学院，都柏林 爱尔兰）

摘 要：智能硬件一般是指基于平台性的底层软硬件构建的具备智能感知、智能信息处理、数据连接以及人机交互能力的新型智能终端与系统。阐述了智能硬件的内涵和构架，针对芯片技术、传感器技术、软硬件协同平台和安全技术等若干智能硬件发展的关键技术，分析了其面临的挑战和机遇，希冀促进国内智能硬件相关的研究发展。

关键词：智能硬件；感知；连接；软硬件协同平台；安全
中图分类号：T-1 **文献标识码**：A

Key technologies for the development of intelligent things

SUN Ling-ling[1], SU Jiang-tao[1], HUANG Xi-wei[1], JIN Jie[1], LI Wen-jun[1], WANG Xiao-jun[2]
(1.Key Lab of RF Circuits and Systems, Ministry of Education, Hangzhou Dianzi University, Hangzhou 310018, China;
2. School of Electronic Engineering, Dublin City University, Dublin 9, Irealand)

Abstract: Intelligent things are intelligent terminals and systems based on software-hardware integrated platforms which are capable of smart sensing, smart processing, smart connection, and smart human-computer interaction. The key technologies for the development of intelligent things, including integrated circuit technology, sensor technology, software-hardware integrated platform, and security technology were discussed, together with opportunities and challenges, to promote the research and development of intelligent things.

Key words: intelligent things, sensing, connection, joint software-hardware platform, security

1 引言

智能硬件（intelligent things）一般是指基于平台性的底层软硬件构建的具备智能感知、智能信息处理、数据连接以及人机交互能力的新型智能终端与系统[1]。近年来，随着移动互联网、物联网（IoT, Internet of Things）、云计算、大数据等新一代信息技术的发展及其与社会生产、生活的深度融合，智能硬件在医疗、金融、交通、智慧城市建设等领域的应用日益深化，在智能穿戴设备、智能车载设备等领域已经形成规模化的产品，对传统设备的智能化改造也在加速[1]，如图 1 所示。为了进一步提升终端产品智能化水平，加快智能硬件应用普及，2016 年 9 月，工信部与发改委共同印发了《智能硬件产业创新发展专项行动（2016-2018 年）》，预计到 2018 年，我国智能硬件产品可服务的总体市场规模可以达到 5 000 亿元，到 2020 年可以达到万亿元的水平[2]。

智能硬件可以看作是多层次的，具备智能感知、处理、学习、执行和互联等能力的，结合软硬件的复杂系统或设备。智能硬件不仅是将传统硬件

收稿日期：2017-06-30；**修回日期**：2017-08-20
通信作者：孙玲玲，sunll@hdu.edu.cn
基金项目：国家自然科学基金资助项目（No.61331006, No.61501156）；浙江省自然科学基金资助项目（No.LY17F010016）；浙江省公益性技术应用研究计划基金资助项目（No.2017C31064）；爱尔兰国际战略合作科学基金资助项目（No.SFI/13/ISCA/2845）
Foundation Items: The National Natural Science Foundation of China (No.61331006, No.61501156), The Natural Science Foundation of Zhejiang Province (No.LY17F010016), Public Welfare Technology Application Research Plan of Zhejiang Province (No.2017C31064), Science Foundation Ireland (SFI), International Strategic Cooperation Award (ISCA) (No.SFI/13/ISCA/2845)

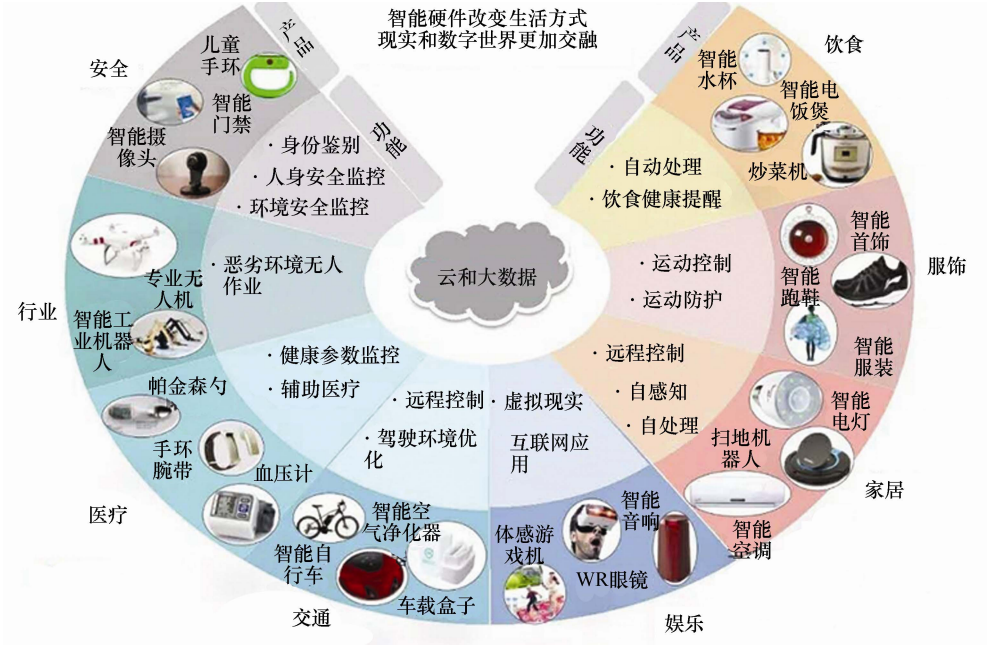

图 1　智能硬件与社会生产生活的融合

添加了新的能力，更将人工智能嵌入硬件，构成了大数据的源头和云计算服务的入口[3]；它是连接线上云平台和线下现实场景的跨界点，更是反映了人工智能和物联网发展的必然趋势。基于智能硬件形成的软硬件一体、线上线下互动、云端结合的物联网新型服务模式甚至生态环境，具有极其广阔的发展前景[4~6]。

本文从智能硬件内涵架构及特点角度出发，对其发展所需要的若干核心技术进行阐述，分析其面临的挑战和待解决的问题，希冀促进国内智能硬件相关的研究发展。

2　智能硬件的内涵与架构

作为蓬勃发展的新兴事物，对于智能硬件的内涵与架构并无严格一致的规定。然而从智能硬件的核心要求出发，一般认为智能硬件应满足如下基本条件。

1) 智能性。智能硬件应该有自我学习和感知的能力，即主动的感知外部环境的变化，做出自己的决策。在未来，多种智能硬件必将成为内容展示的众多载体，智能购物、智能出行、智能娱乐等内容将融合在智能硬件的使用场景中，单一的智能化将不再出现。例如，亚马逊最新推出的智能音箱 ECHO，突破了传统音箱的概念，不仅能够主动接受用户指令，用语音控制音响，连接到灯光、恒温器等，成为家庭的控制中心；更加可以主动进行婴儿监护、行程智能安排、家庭必需品采购等行为，已经初步具有自我学习和判断能力[7]。人工智能技术的发展将大大推进智能硬件产业的发展。

2) 独立处理复杂信息的能力。智能硬件应能综合多主体、多因素、多变量、多主体，建立信息处理决策系统。这既可包括多种信息的融合，如声音数据、图像数据、毫米波太赫兹等电磁波数据等，又包括多信息单元间的耦合和判断，即判断什么是大因素，什么是小因素，进而做出最优决策。一个典型的无人驾驶汽车需要具备至少数十个不同类型的传感器，包括毫米波传感器、激光传感器、CMOS 图像传感器等；又需要定位算法、建图算法、感知算法、预测算法、决策算法、控制算法等的综合应用以在当前的感知置信度、感知结果的情况下给出最优的车辆轨迹、速度等控制信息，同时考虑效率、安全和舒适性[8]。

3) 无时不在、无处不在的高互联性。智能硬件要求既能实现设备与设备互联，又可实现人机物互联；既可在狭小空间通信，又可在大空间进行连接；既可通过有线方式连接，又可通过无线方式（如 5G 等），也可以突破传统传播介质，采用包括电力线载波、可见光通信等方式进行连接。通过高互联能力，多个智能硬件可以进一步构成多主体、互为输出输入的一个超系统，多主体/子系统/单元间有高

度相互依赖性。依托这种高互联性，近年来，集群智能（swarm intelligence）理论被广泛进行研究，这种理论可以实现多平台分布式自组织（self-organizing）控制，采用自底向上的数据驱动和建模策略，将简单对象构成大集合，通过简单智能主体的聚集协同来实现全局的智能行为[9]。而美国国防部在《无人机系统路线图 2005~2030》指出，到 2025 年以后，无人机将具有集群战场认知能力，实现完全自组织作战[10]。

4) 本地化计算能力和云计算能力的统一。在具有独立智能决策能力和高互联性的基础上，智能硬件一方面可以作为云计算的补充，充分利用本地计算能力，进行模式识别和人工智能决策，并进一步作为云计算平台的数据来源和检验系统；另一方面，可依靠云计算的强大计算力量，开展深度机器学习，弥补本身计算能力的不足。汽车无人驾驶系统，就是本地化计算能力和云计算能力统一结合的一个很好的例子：在车辆行驶过程中，固然需要云计算提供路况分析计算、大规模车辆路径规划、智能交通调度、基于庞大案例的车辆诊断计算等，但是车辆本身必须要随时根据车流量、车速、路口拥堵情况、交通标志牌等实时进行计算，作为无人驾驶的首要依靠信息。

5) 具有低功耗、高能效特性。为了满足长时间待机的互联需求和本地计算需求，在电池技术以及环境能量回收技术未获得重大突破之前，智能硬件本身必须具备集成化和低功耗的特点。因此，越来越多的智能硬件区别于传统芯片集成的概念，不仅仅是将天线、传感器等核心互联器件集成至芯片中，而是直接将数据处理和存储芯片集成至传感器等部件中，进一步减小功耗和器件尺寸；同时，智能芯片的功耗管理也变得智能化，在外部环境不发生改变的情况下，可以长时间保持待机状态，进一步减小功耗；在外部通信协议上，随着基于蜂窝的窄带物联网（NB-IoT）、低功耗蓝牙（BLE）等低功耗通信协议的开发，智能硬件专有通信协议与传统的高速互联网协议界限日益分明，从而减小了器件的尺寸[11]。

6) 安全与隐私：智能硬件无时不在、无处不在的互联性固然带来连接的便利，但同时也使智能硬件时时暴露在网络下，容易受到安全入侵和隐私泄露；而随着智能硬件的广泛应用，一旦安全问题受到威胁，带来的经济损失和社会影响则不可计数。目前智能硬件的发展并没有深入的考虑安全与隐私问题，导致其安全事件频发。例如，2014 年 7 月，安全软件开发巨头赛门铁克公司发现，代号为“蜻蜓”的黑客组织攻击了 1 000 多家能源企业的工业生产控制系统[12]；2016 年 10 月，黑客组织通过互联网控制了超百万台包括网络摄像头在内的智能终端设备，利用设备登录弱口令等漏洞，操纵它们对 DNS 服务器进行大规模 DDoS 攻击，致使美国大面积网络中断。智能硬件的安全性，主要体现在智能设备与云端交互数据、设备本身操作系统内部以及智能硬件芯片内部 3 部分，因此，目前主流的智能硬件安全方案，目的都在实现从 CPU 到 SoC，再到操作软件的一体化可信执行平台，从底层构建夯实的可信环境，为智能硬件安全保驾护航。在此方面，例如芯片公司 ARM 对网络安全公司 OffSpark 公司的收购，智能硬件公司 NanoTag 与网络服务提供商 Vodaphone 的合作，无不在体现这一软硬件结合和协同安全保障趋势[13,14]。

3　智能硬件的核心技术与挑战

为进一步推进智能硬件发展，需要从其核心技术进行突破。基于智能硬件的内涵架构，智能硬件的核心技术主要包括先进集成电路（芯片）技术、传感器技术、软硬件协同设计以及安全技术等。集成电路是信息技术的基础和核心，是智能硬件的“心脏”；传感器是智能硬件感知外部环境的直接手段；软硬件协同平台是基于集成电路、传感器形成的具备信息采集、处理、控制和连接能力的智能硬件软硬件解决方案；安全技术是基于集成电路、传感器、信息处理和连接上形成一整套软硬件安全机制。这几项核心技术服务于智能硬件内涵上有差异也有联系，须以集成电路芯片与传感器协同推进核心技术突破，以平台技术支撑智能硬件产品集成创新，以安全技术支撑智能硬件安全应用。

3.1　芯片技术

智能硬件的复杂性和多功能性要求芯片设计时需考虑多层次的优化、平衡和验证。具体而言，需要如下的技术突破。

1) 智能信息处理与交互芯片

针对智能硬件中集成电路芯片感知与处理信号的大数据量、微弱性等特性，为了满足智能硬件的智能化、低功耗、云互联、高能效比、高性能的目标需求，必须研发基于新结构新算法的智能信息

处理与交互芯片，并在硬件和算法间建立桥梁。研究可包括人工智能（类脑）处理芯片、面向 IoT 终端和工业控制的低功耗智能微控制器芯片、高性能图像处理和语音交互芯片、AR/VR 芯片、高速高性能硬件加速芯片等；并研发与之相配合的微弱信号处理的接口电路、调制解调电路及模数转换电路等关键硬件电路。这方面以谷歌最近推出的 TPU (tensor processing unit)芯片，即专门为加速深层神经网络运算能力而研发的一款 ASIC 芯片为代表，将机器学习拓展到芯片级，实现低功耗的智能计算[15]。在语音识别、人脸识别等面向下一代用户界面与用户体验的智能硬件方面，新型的基于卷积神经网络和深度学习的处理器也被开发[16,17]。

2) 高速无线数据传输与通信芯片

智能硬件内部模块之间、各种智能硬件之间的高速无线传输是制约数据处理与交换瓶颈的问题。因此，高速无线数据传输集成电路芯片的研究具有重要意义。如硅基毫米波/太赫兹频段的高速无线数据传输，包括毫米波/太赫兹核心芯片电路、片上集成化天线、无线大数据量传输等，突破基于硅基集成电路工艺的毫米波/太赫兹集成电路芯片设计技术，实现高工作频率、低噪声和高输出功率的毫米波/太赫兹集成电路核心芯片，通过高频率、宽频带的毫米波/太赫兹通信传输芯片以期实现智能硬件的感知与处理间的交互，从而形成系统化集成[18]。

3) 低功耗芯片技术

智能硬件中所采用的微电子芯片愈来愈小型化，计算能力愈来愈强，同时消耗功率也越来越低。但这种通过减小器件尺寸来提高芯片性能的方法，正面临物理和经济上的发展的一个转折点。因此，一方面要对 FinFET（鳍式场效晶体管）等先进垂直器件工艺进行研究，探究在晶体管尺寸不再减小的条件下，增加芯片性能的方法；另一方面，要研发可对先进器件电路进行建模、设计和实现的开发工具，要开展系统、模型—工艺与 EDA 工具的协同设计研究[19]。

3.2　传感器技术

为了满足不同智能硬件的功能需求，传感器的种类丰富多样。环境传感器如气体、气压、湿度、温度传感器，常用于空气净化器、家装毒气、工业废气等的检测；惯性传感器用于智能手环、智能手表等可穿戴设备，可监测佩戴者的运动情况；磁性传感器用于智能家用电器仪表盘的转角检测；模拟类传感器用于心电图信号感知等智慧医疗设备；图像传感器用于可见光、红外图像探测，实现扫地机器人自动避障等；化学生物传感器，如场效应纳米孔器件、栅控纳流道器件，用于环境、生物医疗检测[20]。

针对智能硬件的发展要求，传感技术的突破主要应集中在 2 个方面。第一，向微型化、低功耗、高精度、高可靠性方向发展，以达到更高效、持久、敏感的信息感知，同时降低成本，或通过发现新的敏感机理提高性能。例如，目前全球最小的三轴加速度计是博世公司在 2014 年发布的 BMA355，采用晶圆级封装，尺寸仅为 1.2 mm×1.5 mm×0.8 mm，功耗极低，工作电流仅为 130μA[21]。第二，随着 CMOS 兼容的 MEMS 技术、CMOS 集成技术与微处理技术的发展，新型的同时具备信息感知、处理、判断、通信功能及标准数字化输出于一体的智能传感器成为发展趋势，以替代传统的仅提供表征待测物理量的模拟信号的传感器。同时，单片集成多种感知能力的传感器、多感知数据的融合分析，都是智能硬件传感技术发展的新方向。例如，2016 年，欧洲微电子研究中心（IMEC）与三星电子共同研发了一种内置了并发心电（ECG）、生物阻抗（BIOZ）、皮肤流电反应（GSR）以及光电容积描记（PPG）脉搏波传感器，实现了多参数生理信号同步采集，可以为可穿戴电子产品提供更精确、可靠和广泛的健康评估[22]。

3.3　软硬件协同平台

智能硬件软硬协同平台（以下简称“平台”）主要依托高性能的嵌入式处理单元和智能嵌入式操作系统，以及丰富的数据接口。平台对下可以兼容多种传感器和设备（如毫米波传感器、激光雷达、视觉传感器等），完成数据采集和处理，设备和传感器的添加可定制可重构；对上可联网传输数据到远程数据中心，为各种智能的运算和控制等提供现场传感器和设备数据；并且还能根据数据类型和重要性，定制现场处理数据的应用（如机器学习、智能控制算法），使数据的端处理能力大幅提升，降低数据中心的处理压力和数据传输的带宽负荷。

智能硬件的系统硬件和软件应解决 3 个核心问题，即控制、计算和网络。这 3 部分技术模块相互独立又同时互相关联，构成了智能硬件的个体智能和组网智能。在这些方面，应重点研究通过高阶控制理论，可在智能硬件上运行的控制算法，如自适

应 PID、滑膜控制等，以解决智能硬件对控制系统的实时性、控制精度、系统稳健程度的高要求。如无人机需要通过飞行传感器的反馈信息进行电机控制，使系统对环境做出自适应调整，姿态控制误差范围需要保持在小于 0.1° 以下，具备一定抗风能力。同时要着重研究连接云端和本地计算关键技术，实现联网传输所有数据到远程数据中心，为人工智能的运算提供现场传感器和设备数据。并且还能根据数据类型和重要性，定制现场处理数据的应用（如机器学习、智能控制算法），使数据的端处理能力大幅提升，降低数据中心的处理压力和数据传输的带宽负荷。这样，平台在功能和性能上就能够很好的平衡本地“雾”计算和远端“云”计算，并具有开放性和可重构性。

3.4　安全技术

智能硬件的安全技术主要包括设备本身的安全以及连接的安全，涉及监控、加密、隔离、存储等多方面。一方面，随着随时随地无线互联的要求，智能硬件时刻暴露在互联网中，也时刻存在着被攻击的危险；另一方面，智能硬件的传感器增多，类型多样，带来更多的被攻击和隐私暴露的风险。一旦智能硬件以及智能硬件系统的一个偶然的漏洞被攻击者利用，就很有可能带来巨大的、使用者隐私全盘暴露的风险[23]。针对物联网安全问题，斯坦福、伯克利和密歇根大学的研究人员正开展 SITP（Secure Internet of Things Project）项目，希望能从基础研究角度实现新的物联网安全技术[24]。

在智能硬件安全技术上，目前尚未形成统一的标准和流程，缺乏可靠性、安全性测试评估方法，未建立完善的安全防护体系。目前，可行的思路包括：让智能硬件拥有自主学习能力，可以自行升级代码，并且与网络云计算平台相联系，自动检测威胁并防御[25]；智能硬件包括自我学习能力和自我修复能力，在一旦受到威胁后，可以自我修复[26]；智能系统的设计包括一定的冗余，使在遭受攻击时具有较强的抵抗力和恢复能力[27]。

对攻击的抵御，体现在及早发现攻击意图，判断攻击目标，以及采取反制对策和修复措施。由于智能硬件本身的轻体量性，无论是中央处理器的计算能力，还是内存的大小都无法具备独自抵御攻击的能力。因此，低功耗的集成电路芯片技术，特别是在芯片内部集成安全防御电路的技术[28]，以及结合大数据云计算平台的本地雾计算技术[29]，将是未来智能硬件安全技术领域重要的研究方向。

实际上，除了抵御攻击问题之外，隐私保护技术也是智能硬件安全范畴下的一个重要课题。在这个问题上，已经涌现多种技术如“私有钥匙”，将智能硬件本身的芯片特征作为网络传输加密验证的公钥，而实际传输的数据经过加密，作为网络节点的智能硬件只能获得与本地芯片相符合的数据[30]。

4　结束语

智能硬件的发展，已经远远超出了一个“概念”范畴。通过多种传感器件的应用，并结合自身学习、处理能力的增强，智能硬件可以在很大程度上为人们的日常生活提供便利，并为智能制造、工业 4.0 的发展提供坚实的基础。然而，智能硬件的发展，在芯片技术、传感器技术、软硬件协同平台以及安全技术上仍然有很长的道路要走。未来的研究必须充分考虑到这些挑战，集中力量在这些技术上取得突破，从而更好更快地发展智能硬件。

参考文献：

[1] 智能硬件产业创新发展专项行动（2016-2018 年）[EB/OL]. http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c5259332/content.html.

[2] 中国信息通信研究院. 2016 智能硬件产业全面解析[EB/OL]. http://chuansong.me/ n/1372551551352.

[3] BONOMI F, MILITO R, ZHU J, et al. Fog computing and its role in the internet of things[C]// Edition of the MCC Workshop on Mobile Cloud Computing. 2012: 13-16.

[4] ELEONORA B. The Internet of Things vision: key features, applications and open issues[J]. Computer Communications, 2014, 54: 1-31.

[5] GRIECO A, RIZZO A, COLUCCI S, et al. IoT-aided robotics applications: technological implications, target domains and open issues[J]. Computer Communications, 2014,54: 67-83.

[6] AL-FUQAHA A , MOHSEN G , MEHDI M, et al. Internet of Things: a survey on enabling technologies, protocols, and applications[J]. IEEE Communications Surveys & Tutorials, 2015,17(4): 2347-2376.

[7] WEBER A, ALEXA A, ECHO A. Amazon echo: the best user guide to learn Amazon echo and get benefits from Amazon prime membership [M]. Create Space Independent Publishing Platform, 2016.

[8] Novak. Google self-driving car[EB/OL]. https://en.wikipedia.org/wiki/Google_self-driving_ca.

[9] BENI G, WANG J. Swarm intelligence in cellular robotic systems [M]// Robots and Biological Systems: Towards a New Bionics?. 1993:703-712.

[10] 王明月. 美国公布《“下一代”无人机系统研究、发展和验证路线图》[J]. 装备学院学报, 2012(3):43-43.

[11] HEYDON R. Bluetooth low energy[M].Prentice Hall, 2013.

[12] 俄罗斯黑客组织红蜻蜓攻击了西部一千多家能源公司[EB/OL]. http://server.chinabyte.com/170/12843170.shtml.[2014-7-17].

[13] ARM buys OffSpark the IOT security company[EB/OL]. http://www.machinetomachinemagazine.com/2015/02/09/arm-buys-offspark-the-iot-security-company/.
[14] JORGE G， EDMUNDO M，JORGE S S. Security for the Internet of Things: a survey of existing protocols and open research issues[J]. IEEE Communications Surveys & Tutorials，2015, 17(3):1294-1312.
[15] JOUPPI N P, YOUNG C, PATIL N, et al. In-datacenter performance analysis of a tensor processing unit[J]. arXiv:1704. 04760.
[16] PRICE M, GLASS J, CHANDRAKASAN A P. A scalable speech recognizer with deep-neural-network acoustic models and voice-activated power gating[C]//ISSCC. 2017.
[17] BONG K, CHOI S, KIM C, et al. A 0.62 mW ultra-low-power convolutional-neural-network face-recognition processor and a CIS integrated with always-on haar-like face detector[C]// ISSCC. 2017.
[18] SADHU B, TOUSI Y, HALLIN J, et al. A 28 GHz 32-element phased-array transceiver IC with concurrent dual polarized beams and 1.4 degree beam-steering resolution for 5G communication[C]// ISSCC. 2017.
[19] BLAAUW D, SYLVESTER D, DUTTA P, et al. IoT design space challenges: circuits and systems[C]// VLSI Technology. IEEE, 2014:1-2.
[20] 尤政.智能传感器技术的研究进展及应用展望[J]. 科技导报，2016，34(17):72-78.
YOU Z. Research progress and application prospect of smart sensor technology[J]. Science &Technology Review, 2016, 34(17): 72-78.
[21] COLIN R J. Bosch unveils consumer MEMS [EB/OL]. http://www.eetimes.com/document.asp? doc_id=1262945.
[22] KONIJNENBURG M, STANZIONE S, YAN L, et al. 28.4 A battery-powered efficient multi-sensor acquisition system with simultaneous ECG, BIO-Z, GSR, and PPG[C]//IEEE International Solid-State Circuits Conference, 2016: 480-481.
[23] JACOB W, TADAYOSHI K, SHORT D, et al. WearFit: security design analysis of a wearable fitness tracker[C]// IEEE Cybersecurity, 2016.
[24] Secure Internet of Things Project [EB/OL]. http://iot.stanford.edu.
[25] DENG J, HAN R, MISHRA S. Secure code distribution in dynamically programmable wireless sensor networks[C]// ACM/IEEE Int. Conf.Inf. Process. Sens. Netw. (IPSN), 2006: 292-300.
[26] SALEHI S A, RAZZAQUE M A, NARAEI P, et al. Security in wireless sensor networks: issues and challenges [C]// IEEE International Conference on Space Science and Communication. IEEE, 2013: 356-360.
[27] AGRAWAL V. Security and privacy issues in wireless sensor networks for healthcare[C]// International Internet of Things Summit. Springer International Publishing, 2014:223-228.
[28] KAABOUCH M, COCQUEN E L. Bi-processor architecture for secure systems[P]. US7984301. 2011.
[29] KERMANI M M, SAVAS E, UPADHYAYA S J. Guest editorial: introduction to the special issue on emerging security trends for deeply-embedded computing systems[J]. IEEE Transactions on Emerging Topics in Computing, 2016, 4(3):318-320.
[30] TAN C, et al. Body sensor network security: an identity-based cryptography approach[C]//WiSec ’08, 2008:128-133.

作者简介：

孙玲玲（1956-），女，杭州电子科技大学教授，主要研究方向为微波毫米波集成电路与智能系统设计。

苏江涛（1981-），男，杭州电子科技大学讲师，主要研究方向为微系统与集成电路设计。

黄汐威（1987-），男，杭州电子科技大学副研究员，主要研究方向为集成传感器与微分析系统。

金洁（1986-），男，都柏林城市大学博士生，主要研究方向为网络化控制系统与网络安全科研工作。

李文钧（1977-），男，杭州电子科技大学副教授，主要研究方向为集成电路设计与物联网技术。

王小军（1964-），男，都柏林城市大学副教授，主要研究方向为信息与网络安全。