

物联网核心技术及应用演进

薛小平, 王 骞*, 张 芳

(同济大学 电子与信息工程学院, 上海 200092)

(*通信作者电子邮箱 wangqiantails@163.com)

摘 要:针对物联网概念、关键特征、体系结构及核心技术进行研究。在关键特征与核心技术方面,深入研究并讨论了物联网的泛在性、特定环境下的智能标识与感知技术、数据的不确定性、数据表示方法、海量数据的信息传播、安全和隐私等问题,并给出了开放性的研究内容。针对未来物联网应用的泛在性,进一步提出了物联网的研究发展方向。

关键词:物联网;泛在网络;体系结构;核心技术;智能技术

中图分类号: TP393.1 **文献标志码:** A

Key technologies and application evolution of Internet of things

XUE Xiaoping, WANG Qian*, ZHANG Fang

(School of Electronics and Information Engineering, Tongji University, Shanghai 200092, China)

Abstract: The concept and architecture of the Internet of Things (IoT) were introduced. Key characteristics and technologies, which included the ubiquity of the IoT, intelligent identification and sensing technologies, uncertainty of data, representation methods of data, information propagation towards massive data, security and privacy were discussed in detail, and related open issues were presented. Based on the future ubiquitous applications, the research directions of the IoT were put forward.

Key words: Internet of Things (IoT); ubiquitous network; architecture; key technology; intelligent technology

0 引言

互联网从20世纪80年代的纯学术网络开始,至今已发展为全球信息共享平台,直接影响着社会经济、政治和文化。目前,互联网正从固定网络转向移动互联网,接入互联网的设备也由传统的计算机,扩展到诸如移动电话、掌上电脑、全球定位系统(Global Positioning System, GPS)跟踪器等泛在化和智能化设备。在互联网实现了信息传递和共享后,人们期望各种实物的描述信息也可传递和共享,“物联网(Internet of Things, IoT)”^[1]正是在这种情况下提出的。

物联网是未来互联网的重要组成部分。未来互联网将不仅是现有互联网的简单演化,为适应未来应用,更需要有新的体系结构、接口、数据管理方式、能异构地接入各种不同互联网实体(包括设备、服务、物体和人)及传感器等。未来对象均为可标识、可通信、可移动、可交换、可创建和销毁的智能化可信实体,若干对象可建立通信网络,这种网络又可与本地甚至全球的其他网络连接,且可为各种用户提供所需服务。

近年来,物联网已受到学术界和业界的高度关注,人们试图通过物联网实现无处不在、无时不在的泛在计算。

本文主要探讨物联网的相关概念、网络体系结构、核心技术及其应用演进。

1 物联网概念

物联网最初由麻省理工学院 Auto-ID 研究中心^[2]提出,其含义是把所有物品通过射频识别(Radio Frequency Identification, RFID)等信息传感设备与互联网连接,实现智

能化识别和管理,试图以 RFID 为基础,构建全球性的 RFID 网络架构,以实时跟踪和监视物品。

国际电信联盟(International Telecommunication Union, ITU)^[3]对物联网概念进行了扩展,提出物联网的基本含义:通过射频识别、红外感应器、全球定位系统、激光扫描器等信息传感设备,按约定的协议,把任何物品与互联网连接起来,进行信息交换和通信,以实现智能化识别、定位、跟踪、监控和管理的一种网络。强调任何时间、任何地点、任何物体之间,通过泛在网络和普适计算互联,除 RFID 技术外,传感技术、纳米技术、智能终端等技术也将得到广泛应用。

物联网中的交互实体是时间或空间上可移动的物理或虚拟物体,采用近场无线通信(Near Field Communication, NFC)、无线传感与执行网络(Wireless Sensor and Actuator Network, WSN)与 RFID 等技术的融合,连接物理世界与虚拟世界^[5-6]。在物联网中,物体参与商业、信息和社会的活动,进行交互和通信;并感知环境,与环境交换数据和信息^[7]。

近年来,正在兴起的未来互联网^[4]研究认为,未来互联网集媒体互联网、服务互联网和物联网于一体,基于标准通信协议将多种网络集成为一个互通的全球信息平台。物联网作为未来互联网的组成部分,定义为可自我配置的动态全球网络基础设施,基于可互操作的标准通信协议,将有身份、物理属性、虚拟特性及智能接口的物理或虚拟物体,无缝地集成于同一信息网络。

针对未来网络的演化,有学者认为信息物理系统(Cyber-Physical System, CPS)^[8-9]是未来网络的发展方向。CPS 是信息领域的网络化技术、信息化技术与物理系统中控制技术、自

收稿日期:2013-04-22;修回日期:2013-06-07。 基金项目:国家自然科学基金资助项目(60972036)。

作者简介:薛小平(1963-),男,江苏金坛人,教授,博士,主要研究方向:物联网、可信计算、路由理论;王骞(1990-),男,江苏江阴人,硕士研究生,主要研究方向:物联网、射频识别;张芳(1971-),女,浙江嵊泗人,讲师,博士,主要研究方向:图像处理。

动化技术的融合。CPS通过嵌入物理世界的传感器与计算节点,将之与信息世界相连接,实现物理世界和信息世界的相互作用与深度协作,提供实时感知、信息反馈和动态控制等功能,以构成高效、智能的物理世界。

CPS强调计算技术与控制技术的融合,为把虚拟世界与物理世界连接,CPS需把已有的、处理离散事件的、不关心时间和空间参数的计算技术,与现有的、处理连续过程的、注重时间和空间参数的控制技术融合起来,使得网络世界可以采集物理世界与时间和空间相关的信息,进行物理装置的操作和控制。

未来网络演化是物联网还是CPS,尚存在争议。文献[10]指出,物联网与CPS的区别同因特网和电信网的区别类似;两者基本技术如无线传感器网络、射频识别、高效低功耗嵌入式系统等方面是一致的,而CPS更强调循环反馈的概念,强调感知物理世界之后,再通过通信与计算对物理世界做出某种调整。

2 物联网关键特征及体系结构

2.1 关键特征

大量的研究表明,与传统的互联网相比,物联网具有以下基本特征:

1) 融合物理实体。物理实体可融合射频识别与传感技术,应具有可标识、可感知、可通信、可控制的安全智能体^[11]的特征,但并非所有的物理实体均要实现全部功能,有些实体仅需实现可标识、可通信等部分功能。依据实现功能及智能体智能度的差异,物理实体有以下几种情形:①获取标识(RFID网络)^[2];②获取标识和状态量(RFID与传感网络的融合,是典型的物联网)^[3];③获取标识、状态量以及受控执行机构(远程控制与人机交互)^[12];④标识、状态量、智能计算和执行机构(机器人)^[13]。

2) 异构化特征。智能标识与感知技术由标识与传感技术融合而成,本质上具有异构性^[4],且不同环境下的智能标识与感知体采用不同技术实现,具体表现为不同标识及传感器的底层实现技术各不相同^[14],如特定环境下的标识技术不同,实现技术也不同;同样,不同环境下的传感技术也呈现出差异化;标识技术和方法的不统一,如目前广泛应用的条码技术,EPCGlobal(国际物品编码协会和美国统一代码委员会的合资公司)建议采用产品电子码(Electronic Product Code, EPC)编码,而有学者也提出采用IPv6进行编码^[15],或采用特定技术的标识进行编码,如表面超声波技术;异构化还表现在获取信息表示方法的差异性,由于不同厂商遵守的标准不一、方法不一,造成信息表示的差异性,进一步影响系统的可扩展性。

3) 海量信息的存储、共享、传播及管理。网络承担数据存储、共享、传播及管理的功能,研究表明:物联网所产生的数据量巨大,以采用RFID技术的超市供货系统为例,其每天需处理的RFID数据高达太比特级^[16]。海量数据的存储、共享、传播及管理,给网络提出了新的挑战,需要适当的体系结构来满足海量数据的传播、存储和共享问题。

4) 泛在性与普适计算相结合。物联网中,通过将物理实体与射频识别、无线传感等技术相融合,通信对象扩展到日常生活用品,实现人与物及物与物之间的通信,从而使信息与通信技术获得一个新维度^[3],将任何时间、任何地点连接任何人,扩展到任何物体之间的信息交换;普适计算建立在分布式

计算、通信网络、移动计算、嵌入式系统、传感器等技术之上。物联网中,其与泛在网络相结合,实现信息空间与物理空间的无缝连接,人们可随时、随地、自由地享用计算能力和信息服务。

2.2 体系结构

EPCGlobal定义的EPC体系结构^[17-18]如图1所示,由EPC编码体系、射频识别系统及信息网络系统3部分组成,具体包括EPC编码体系、EPC标签、阅读器、EPC信息服务(EPC Information Service, EPCIS)软件、对象名解析服务(Object Naming Service, ONS)、EPC中间件6个部分^[17,19]。

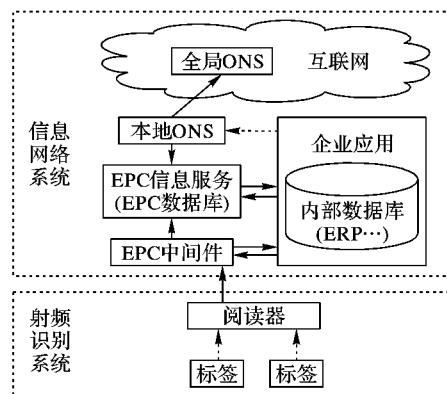


图1 EPC体系架构

EPCIS是数据库与应用间通信的“翻译器”,提供标准化的、到EPC网络其他部分的接口,从而获取EPC相关信息并对这些信息进行处理;ONS的作用类似域名解析服务^[20],可把EPC翻译成统一资源定位器(Uniform Resource Locator, URL),并将对象信息服务器中的关于产品信息的URL与带有唯一编码的被标记对象相联系;EPC中间件位于标签阅读器及企业应用之间,可处理大量来自阅读设备的标签数据或传感数据。

EPC中间件中最重要的部分为应用层事件(Application Level Event, ALE)规范^[21]。ALE层处于应用业务逻辑和原始标签读取层之间,定义了RFID中间件基本功能:收集与过滤,将原始数据处理为应用层事件,以此减少原始数据的冗余度,并从大量数据中提炼出有效的业务逻辑。

EPCGlobal定义的体系结构,主要针对RFID应用,网络构架中并未体现物理信息感知、表示、管理、传播等核心内容,无法构成通用、完整的物联网体系结构。为实现物联网异构信息之间的互联、互通与互操作,未来的物联网应是开放的、分层的、可扩展的网络体系结构。ITU在文献[22]中描述了泛在传感网络(Ubiquitous Sensor Network, USN),将物联网分为识别感知层、通信网络层、数据管理层和应用服务层四个层次,如图2所示。

1) 识别感知层主要负责数据采集与感知,主要用于采集物理世界中发生的物理事件和数据,包括各类物理量、标识、音频、视频等数据,涉及传感器、RFID、多媒体信息采集、二维码和实时定位等技术,是物联网的关键和核心;

2) 通信网络层主要负责可靠、安全地信息传递和处理,将传感器网络技术、移动通信技术、互联网技术等相融合;

3) 数据管理层包括网络和数据管理中心、信息中心和智能处理中心等;

4) 应用服务层则是物联网与行业专业技术的深度融合,用于支撑跨行业、跨应用、跨系统之间的信息协同、共享、互通,服务于包括智能交通、智能医疗、智能家居、智能物流、智

能电力等行业应用,与行业需求结合,实现行业智能化。

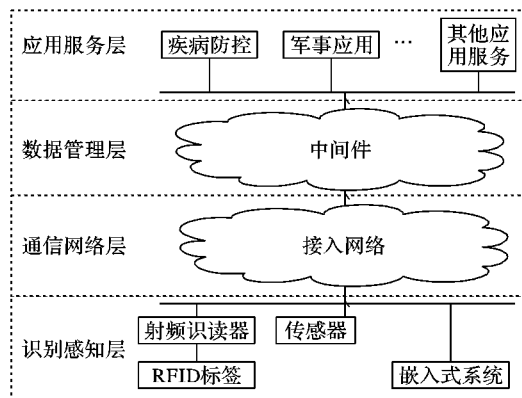


图2 物联网分层结构

目前,针对物联网体系结构的研究还在不断地深入,但未来物联网至少应具备感知和标识任何对象的能力;具备海量数据管理、存储、处理及传播的能力;具备将物理世界的数据可视化地呈现给应用的能力。

云计算^[4,23]作为海量信息存储、处理的一种方法,近来受到了研究人员的关注。云计算通过在一个服务器上部署多个虚拟机和应用,可提高资源的利用率,对信息进行高效存储、共享和传播。有学者针对物联网内数据信息的动态性和应用的不确定性,提出采用基于事件的信息传播机制^[20,24-25]。

目前,物联网体系结构的研究还有很多问题^[4]有待解决,包括:

- 1) 分布式开放架构,具有端到端传输、互操作性、异构性、明确的分层结构及有效防御物理网络中断等特性;
- 2) 基于对等节点的分布式自主架构;
- 3) 云计算技术,基于事件驱动的架构,无连接操作和同步;
- 4) 网络边缘的智能化,实现数据分布式计算与存储。

到目前为止,学术界和业界尚未实现真正可用的基于分布式技术的网络体系结构,但研究人员给出了物联网体系结构的一些核心特征^[3-4]:

物联网是泛在网络与普适计算的融合,可实现任何时间、任何地点、任何人与物的相互连接;基于开放式架构,以最大限度满足异构系统与分布式资源之间的互操作性;明确定义了抽象数据模型、接口和协议,并可支持第三方技术,如可扩展标记语言(eXtensible Markup Language, XML), Web Services等,以满足多编程语言与操作系统;支持物联网节点自主组建动态对等网络,支持语义搜索、发现;为应对海量数据,物联网边缘应具有过滤、模式识别、机器学习与决策能力,可在数据源端或网络云处智能化处理分布式信息数据,并满足智能体之间、智能体与非智能体之间信息与服务共享;支持事件处理、路由、存储和检索等;支持数据流的有效缓存、预定位与同步请求、更新等。

3 物联网的核心技术

3.1 特定环境下智能标识与感知技术

传统研究中,传感技术和标识技术是分离的,如采用RFID标识某个特定对象,而采用传感器技术来感知此对象的物理状态量。物联网中的智能标识与感知技术须将标识技术和传感技术进行融合。

针对特定对象的智能标识与感知技术,对象可用标识和

状态量来表示,即 $O = \{ID, D_1, \dots, D_n, L, Timestamp\}$,式中 ID 表示对象的唯一标识, D_1, \dots, D_n 为对象的状态量,包括对象温度、湿度、某种物质的含量等, L 表示位置, $Timestamp$ 表示信息获取的时刻。

目前,所采用的标识技术^[26]包括条码(一维、二维和三维条码)技术、RFID技术等;表示各种状态信息的状态量的获取,通常采用传感器,如温度传感器、压力传感器等;位置信息通常采用GPS或特定的位置估计技术来获取;时间的获取方法则相对简单,通常在获取信息时加入其获取时间,但针对开环应用,需要有全球统一的时间同步。

针对特定类型应用的智能标识与感知技术,呈现出差异性。例如在对集装箱的标识和状态量获取时,需采用抗干扰的有源电子标签,获取用户感兴趣的状态量,如箱内温度、车门的开关状态等,而事实上,针对集装箱内物品的不同,用户感兴趣的状态量也有所差异。

全球物联网应用种类呈现出多样性,这种多样性给智能标识与感知技术提出了新的挑战,包括:

1) 电子标签和传感器的低价格、低成本、小型化和纳米技术,如供应链中,标识香烟、记事簿等海量且小体积商品的电子标签。传统上采用条码技术,价格十分低廉,而电子标签无法做到如此低的价格,需在用户承受范围之内,与被标识对象相比,价格需做到1%甚至更低。特定应用下,如电子医疗中采用的人体皮下注入电子标签技术,需同小型化和纳米技术相结合^[3]。

2) 特定环境的标识技术。如水环境下,工作的电子标签需满足特定防水等级,且随被标识对象距水面距离加深,现有的基于反向散射、感应耦合的方法将无法工作,需要特殊的通信和感知方法;又如高温环境下,很多电子设备无法正常工作,同样需特殊的对象标识技术等。此外,标识技术也受到标识对象的影响,如某些物品体积小且形状不规则,要求电子标签体积小,且能高效通信。

3) 特定环境的传感技术,如水污染、高速列车轨道间的平衡性检测、漏水、管道漏气等特定应用场合下的传感技术。

4) 电子标签和传感器的销毁问题。电子标签均采用电子器件,已作废的电子器件处理不好,会带来电子污染。因此,在设计和制造电子标签和传感器时,需考虑销毁问题,尤其在大规模应用时,这一问题更加重要且不易解决。电子标签的销毁还会带来标签编号的回收问题,否则,若每个物品都保留原有标识编号,则电子标签编号资源将很快被耗尽。

5) 电子标签和传感器需要解决数据存储、电源供电、能源存储与节约及安全防伪等问题。此外,由于很多应用场合,读写器信号作用范围内可有多多个标签存在,需采取防碰撞技术^[12],以减少数据冲突,达到快速准确识别多个标签的目的。

6) 智能标识与感知网络化问题^[7]。智能标识与感知网络节点作为一个微型化的嵌入式系统,在感知物理世界的同时,应具有局部信号处理功能及足够的抗干扰能力;智能标识与感知网络中存在大量节点,网络拓扑结构在节点发生故障时,应具有自组织能力、自动配置能力及可扩展能力。

7) 智能标识与感知网络中节点的定位问题。节点的准确定位是物联网应用的重要条件,如目标监测与跟踪、智能交通、特殊区域无线传感器等特定应用要求网络节点预先知道自身的位置^[27]。定位包括二维定位、三维定位。受物联网节点大规模、低成本和低计算能力的制约,需寻求合适的定位算法,在提高节点定位精度的同时,降低节点能量消耗,延长网

络的生存周期^[28]。

3.2 数据的不确定性处理及表示

物联网应用中,因其射频技术无线通信的特点,系统前端获取信息的原始数据流具不可靠性与不确定性,表现为数据信息的冗余、错误^[29]等,称之为脏数据^[30]。脏数据会浪费网络资源、影响后台处理的正确性,甚至还会带来更为严重的后果,如错误告警。

研究人员针对数据的不确定性进行了研究,希望减少和消除物联网中的脏数据,主要的方法包括基于网络前端硬件特性的标识与感知可靠性改进方法,以及基于软件的数据清理方法。前者包括抗碰撞算法^[31]、天线设计等;后者包括平滑及流水线方法^[32-34]、基于完整性约束的数据清理方法^[35]等。

在抗碰撞的研究方面,目前已基本成熟,主要有基于ALOHA^[36-37]与二进制树^[37]的抗碰撞算法。其中:ALOHA算法实现较简单,但存在错误判决问题,且其信道利用率较低,不适合大量标签应用场合;二进制树算法识别率较高,不存在错误判决的问题,但时延长,安全性较差。具体应用中,需在防碰撞算法识别率、识别速度、信道利用率及安全隐私等问题方面进一步研究和改进。

在数据清理方面,文献[33-34]提出了采用流水线数据清理的框架结构,以支持普适环境中的应用,称为可扩展的传感器数据流处理(Extensible Sensor stream Processing, ESP),它根据阅读器所获得数据在时间和空间上具有的相关性对数据进行处理。数据清理过程是由点处理、平滑处理、合并处理、判决处理和虚化处理5个阶段组成的数据清理流水线。

在此基础上,有学者引入了数据质量^[38]的概念,针对物理实体数据的不可靠和不确定性,在向应用提供数据时,对其数据质量即清洁度进行评估,应用程序在采用这些数据时可参考数据质量,以给出更为可信的结论。尽管如此,在物联网中,要彻底完全地消除脏数据是不可能的,研究人员还在进一步研究降低数据不可靠性的技术和方法。

在数据表示方面,物联网中数据具有不同异构性,包括结构异构、语法异构、系统异构和语义异构^[39]。目前已有许多技术被开发用来解决不同类型的异构问题,如XML作为公共的语言标准被广泛使用后,由于其所具有的通用语法格式,使得数据源之间能够采用统一的数据模型信息,有效地解决了数据集成中数据共享的问题,但语义异构的问题仍未有效解决。

为此,研究人员提出基于Ontology的数据表示方法^[40-41]。Ontology既准确描述了概念的含义,又描述了概念之间的内在关联,可通过逻辑推理获取概念之间蕴涵的关系,具有很强的表达概念语义和获取知识的能力。同时可采用某种编码语言,如资源描述框架(Resource Description Framework, RDF)、RDF Schema(RDF模式)与本体论Web语言(Ontology Web Language, OWL)等表示Ontology,使之具有较强的推理能力。

3.3 海量数据下的信息传播

物联网的应用将会产生海量的数据,对这些数据的有效管理、处理、存储及传播的方法,是物联网发展所需解决的问题之一。

针对海量数据,有学者提出将数据存储于物体;有学者认为要将数据存储于网络,如中央数据库服务器;也有学者提出“在源附近消化数据”^[42],即在靠近网络前端处,将原始数据

进行处理、过滤和聚合,仅传输有意义的复合事件至中央系统,使之免受来自前端海量低层数据的洪泛。

信息的传播是物联网信息共享的重要内容,针对RFID应用,EPCGlobal认为RFID数据应采用事件的方式表示,不仅可以有效消除数据冗余,减轻网络负载,而且可以通过消息通告系统的方式来方便地传播与共享。文献[16]提出了基于网格的数据挖掘模型,如图3所示。

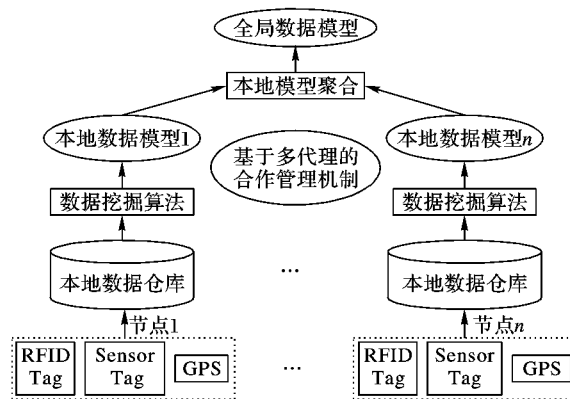


图3 基于网格的数据挖掘模型

在该模型中,局部节点接受来自各种网络前端的原始数据,经数据过滤、抽取、压缩等预处理,存储到本地数据仓库;在本地数据仓库,数据经过滤、合并后形成复杂事件;复杂事件经全局控制节点的聚合操作,存储到全局仓库,以用于不同的应用。其中局部节点之间通过基于多代理的合作管理机制,可共享对象数据与知识。

基于网格的分布式数据模型可解决局部节点的数据存储问题,通过利用网络前端智能体自身的智能计算、语境感知及远程操作能力,在一定程度上满足了物联网的高性能、高存储及高计算能力,物联网可以看作一个大规模信息系统,由于其前端在对物理世界感应方面具有高度并发的特性,并将产生大量引发后端深度互联和跨域协作需求的事件。网络中的事件并非仅发送给某一个应用,如在集装箱运输管理过程中,事件需发送至海关、货代、货主等若干方,且包括事件发生的时间、位置及状态等。传统的一对一、一对多的通信方式无法满足应用需求,需有新型通信机制,以满足事件通信,同时需考虑面向异构基础信息的网络构架问题。

实时感应、高度并发、自主协同等特征对物联网计算的研究提出了新的挑战,需要有针对性地研究物联网特定的应用集成问题、体系结构及标准规范,特别是大量高并发事件驱动的应用自动关联和智能协作问题。

3.4 安全和隐私问题

安全与隐私问题是物联网技术应用与推广的挑战性技术之一。

系统应用中主要安全问题^[43]包括两方面:

1) 电子标签或传感器本身的访问缺陷^[44-45]。由于电子标签或传感器本身的成本所限,自身很难具备足够的安全能力,极易被攻击者操控。在没有足够可信任的安全策略保护下,标签或传感器中数据的安全性、有效性、完整性、可用性、真实性都得不到保障。另外,物联网前端系统中,大量使用射频无线通信技术,无线传输的信号本身是开放的,这就给非法用户的侦听提供了方便。

2) 未来信息传播网络中的安全问题。物联网前端产生的大量数据信息,需在后端网络构架中传播、处理和控制在满足不同应用的需要,这些信息的安全需要采用各种认证与

加密方法来保证。

系统安全问题以保证数据存储和数据传输的安全为目的,完善的系统安全解决方案应当具备机密性、完整性、可用性、真实性和隐私性等基本特征。

系统应用中主要面临两类隐私问题^[46]:位置隐私和信息隐私。电子标签和传感器可跟踪用户运动、生活习惯等信息,携带电子标签和传感器的任何人都可在公开场合被自动跟踪,位置隐私含有高度的个人特征。如商家可利用消费者在超市某一地点或货架的位置信息,或根据消费者商品标签中所接收到的信息资料,去推断消费者的消费习惯,进而结合对象数据库,实时或定期地提供一定的商品推销。

相对于安全的概念,隐私包含了政策、法律等多领域的多元因素。物联网的广泛应用,应在采取合理、有效的安全机制的同时,通过制定相关法律、法规,使隐私权得到切实保护。

4 物联网的应用演进

受终端价格、接受程度、信息安全、应用规模及成熟度等因素的影响,物联网可分为闭环应用和开环应用,或称泛义物联网和本义物联网(国际物联网)。

泛义物联网,即物联网的闭环应用中,技术和方法具有独立性,它包括基于本地的局域网物联网、基于跨区或跨行业的封闭物联网,如门禁、校园一卡通等。

本义物联网,即物联网的开环应用基于公众服务,实现物品与生产、仓储运输、公众服务相关联、物品与生活便利相结合的开放型应用体系,这种服务需要有统一的设备接入、数据模型、事件传播和共享机制、安全和隐私等。

目前,国内外物联网应用处于闭环阶段,如停车场、智能小区、铁路的信号系统等,但物联网最终需要从闭环物联网向开环物联网发展过渡。目前,实现全球统一的开环物联网仍存在很多挑战,主要是核心技术、标准规范、安全与隐私保护以及国家的产业政策、推广应用等技术方面与管理方面的问题^[7,47]。

1)核心技术有待突破。目前处于物联网关键技术研发和规模化应用的初始阶段,关键在于尽快突破核心技术:实现泛在电子标签与传感器的融合;解决特定应用领域与环境下,可靠的智能标识与感知技术;研发易于推广的低能耗、低成本的网络前端等。

2)统一的协议、标准、规范有待制定。参与物联网通信的智能体与非智能体的多样性与差异性,及构成网络的异构性、泛在性,决定了需在全球的范围内制定统一的通信协议、泛在网络标准体系、异构网络互控制与互操作协议、智能化物联网设备标准、物体交互语言规范、安全与隐私标准等。

3)安全与隐私技术有待进一步发展。物联网中的物与物、物与人之间互联,使用大量的信息采集和交换设备,信息安全和保护隐私成为亟待解决的问题,需建立低成本、高安全与高性能的安全标识、认证系统。

4)需政府制定相关政策,参与管理。开环物联网的开放、泛在特性,使得物联网的管理问题凸显,需各国政府积极参与,包括频谱资源管理,为隐私保护立法及实现可持续资源能源消耗等等。

可以预期,物联网最终将成为全球统一的开放和泛在分布的、基于标准协议和接口的、可靠和可信的网络体系结构。

5 结语

物联网的发展,目前呈现出与互联网发展不同的途径,表

现为由局部的、闭环的应用为驱动,逐步形成开放的、全球统一架构的物联网。在未来的应用中,将从单一的对象标识技术,发展为集对象标识、传感、控制和执行于一体的智能执行体,物联网终将是智能体之间、智能体与非智能体相关通信、信息共享的全球一体化网络。

本文描述了物联网的概念、体系结构、核心技术、开放性研究问题以及应用的演进趋势。目前,关于开放性物联网的理论、方法及核心技术仍处于研究阶段,而闭环的物联网应用可在局部范围内实现,但不可避免地会带来标准、方法的不统一。在物联网从闭环向开环不断演进过程中,为避免资源的重复建设和浪费,要兼顾具体应用的特殊要求与各行业应用的共性技术特点,制定统一的面向公众应用的标准。

参考文献:

- [1] HOURCADE J-C, NEUVO Y, POSCH R, *et al.* Future Internet 2020: Visions of an industry expert group[M]. Brussels: European Commission, Information Society and Media Directorate-General, 2009.
- [2] Auto-ID Labs [EB/OL]. [2013-02-10]. <http://www.autoidlabs.org/>.
- [3] ITU Internet Reports 2005: The Internet of Things – Executive Summary [EB/OL]. [2010-07-05]. http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf.
- [4] VERMESAN O, FRIESS P, GUILLEMIN P, *et al.* Internet of things-strategic research roadmap[R]. Brussels: European Commission-Information Society and Media, 2009.
- [5] JEONG S, KIM S H, HA M, *et al.* Enabling transparent communication with global ID for the Internet of things[C]// Proceedings of the 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. Piscataway: IEEE, 2012: 695 – 701.
- [6] CONTI J P. The Internet of things[J]. Communications Engineer, 2006, 4(6): 20 – 25.
- [7] Internet of Things in 2020: Roadmap for the future [EB/OL]. [2010-07-05]. <http://www.smart-systems-integration.org/public/internet-of-things>.
- [8] KANG K D, SON S H. Real-time data services for cyber physical systems[C]// Proceedings of the 28th International Conference on Distributed Computing Systems Workshops. Piscataway: IEEE, 2008: 483 – 488.
- [9] LEE E A. Cyber physical systems: design challenges[C]// Proceedings of the 11th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing. Piscataway: IEEE, 2008: 363 – 369.
- [10] KOUBAA A, ANDERSSON B. A vision of cyber-physical Internet [C]// Proceedings of the 8th International Workshop on Real-Time Networks. Piscataway: IEEE, 2009: 1 – 6.
- [11] ENGELS D W. The reader collision problem[EB/OL]. [2010-07-05]. <http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH-007.pdf>.
- [12] KORTUEM G, KAWSAR F, SUNDRAMOORTHY V, *et al.* Smart objects as building blocks for the Internet of things[J]. IEEE Internet Computing, 2009, 14(1): 44 – 51.
- [13] KRANZ M, HOLLEIS P, SCHMIDT A. Embedded interaction: interacting with the Internet of things[J]. IEEE Internet Computing, 2010, 14(2): 46 – 53.
- [14] XIA F, MA L, DONG J, *et al.* Network QoS management in cyber-physical systems[C]// Proceedings of 2008 International Con-

- ference on Embedded Software and Systems. Piscataway: IEEE, 2008: 302–307.
- [15] JARA A J, ZAMORA M A, SKARMETA A F G. An architecture based on Internet of things to support mobility and security in medical environments[C]// Proceedings of the 7th Consumer Communications and Networking Conference. Piscataway: IEEE, 2010: 1–5.
- [16] SHEN B, LIU Y, WANG X Y. Research on data mining models for the Internet of things[C]// Proceedings of the 2010 International Conference on Image Analysis and Signal Processing. Piscataway: IEEE, 2010: 127–132.
- [17] ARMENIO F, BARTHEL H, DIETRICH P, *et al.* The EPCGlobal architecture framework [EB/OL]. [2010-07-05]. http://www.epcglobalinc.org/standards/architecture/architecture_1_2-framework-20070910.pdf.
- [18] YAN B, HUANG G. Supply chain information transmission based on RFID and Internet of things [C]// Proceedings of the 2009 ISECS International Colloquium on Computing, Communication, Control and Management. Piscataway: IEEE, 2009: 166–169.
- [19] ROBERTS C M. Radio Frequency Identification (RFID) [J]. Computer & Security, 2005, 25(1): 18–26.
- [20] EPCGlobal Inc. EPCGlobal Object Name Service (ONS) 1.0.1 [EB/OL]. [2010-07-05]. http://www.epcglobalinc.org/standards/ons/ons_1_0_1-standard-20080529.pdf.
- [21] EPCGlobal Inc. The Application Level Event (ALE) 1.0 [EB/OL]. [2010-07-05]. http://www.epcglobalinc.org/standards/ale/ale_1_0-standard-20050915.pdf.
- [22] ZHILBERT T. Ubiquitous Sensor Networks (USN) [R]. Geneva: ITU-T, 2008.
- [23] MELL P, GRANCE T. Draft NIST working definition of cloud computing [EB/OL]. [2010-08-30]. <http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>.
- [24] HE M, ZHENG Z, XUE G X, *et al.* Event driven RFID based exhaust gas detection services oriented system research[C]// Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing. Piscataway: IEEE, 2008: 1–4.
- [25] EUGENE W, YANLEI D. High-performance complex event processing over streams[C]// Proceedings of the 2006 ACM SIGMOD International Conference on Management of Data. New York: ACM, 2006: 407–418.
- [26] QUACK T, BAY H, VAN G L. Object recognition for the Internet of things [C]// Proceedings of the 1st International Conference on the Internet of Things. Heidelberg: Springer, 2008: 230–246.
- [27] BULUSU N, HEIDEMANN J, ESTRIN D. Density adaptive algorithms for beacon placement in wireless sensor networks, UCLACS-010013[R]. Los Angeles. University of California Los Angeles, 2001.
- [28] 曾凡仔, 孙正章, 罗娟, 等. 无线传感器网络的节点定位方法[J]. 通信学报, 2008, 29(11): 62–66.
- [29] ELNABRAWY E, NATH B. Cleaning and querying noisy sensors [C]// Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications. New York: ACM, 2003: 78–87.
- [30] 周傲英, 金澈清, 王国仁, 等. 不确定性数据管理技术研究综述[J]. 计算机学报, 2009, 32(1): 1–16.
- [31] LI R Z, NEJAD M B, ZHUO Z, *et al.* Future RFID and wireless sensors for Ubiquitous intelligence[C]// Proceedings of 26th Norchip Conference. Piscataway: IEEE, 2008: 142–149.
- [32] GONZALEZ H. Warehousing and analyzing massive RFID data sets [C]// Proceedings of the 22nd International Conference on Data Engineering. Piscataway: IEEE, 2006: 83.
- [33] JEFFERY S R, ALONSO G, FRANKLIN M J, *et al.* A pipelined framework for online cleaning of sensor data streams[C]// Proceedings of the 22nd International Conference on Data Engineering. Piscataway: IEEE, 2006: 140–153.
- [34] JEFFERY S R. Declarative support for sensor data cleaning[C]// Proceedings of Pervasive'06. Heidelberg: Springer, 2006: 83–100.
- [35] INOUE S, YASUURA H, HAGIWARA D. Systematic error detection for RFID reliability[C]// Proceedings of the 1st International Conference on Availability, Reliability and Security. Piscataway: IEEE, 2006: 280–286.
- [36] BORDER L A. RFID multiple access methods [EB/OL]. [2010-07-11]. http://www.vs.nf.cthz.ch/ccu/SS2004/DS/reports/06_rfid-mac_report.pdf.
- [37] ISO/IEC FCD 15693-3. Identification cards-Contactless integrated circuit(s) cards-Vicinity cards-Part 3: Anti-collision and transmission protocol [S]. Geneva: ISO, 2000.
- [38] JEFFERY S R, GAROFALAKIS M, FRANKLIN M J. Adaptive cleaning for RFID data streams[C]// Proceedings of the 32nd International Conference on Very Large Databases. New York: ACM, 2006: 163–174.
- [39] SHETH A P. Changing focus on interoperability in information systems: from system, syntax, structure to semantics[C]// Interoperating Geographic Information System. Boston: Kluwer Academic Publishers, 1998: 5–29.
- [40] WANG W, TOENJES R, REETZ E, *et al.* A comprehensive ontology for knowledge representation in the Internet of things[C]// Proceedings of 2012 IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Piscataway: IEEE, 2012: 1793–1798.
- [41] TAMMA V, AART C, MOYAUX T, *et al.* An ontological framework for dynamic coordination[C]// Proceedings of the 4th International Semantic Web Conference. Heidelberg: Springer, 2005: 638–652.
- [42] PALMER M. Seven principles of effective RFID data management [EB/OL]. [2010-07-05]. <http://www.objectstore.com/docs/articles/7principlesrfidmgmt.pdf>.
- [43] SHAO X W. Study on security issue of Internet of things based on RFID[C]// Proceedings of the 4th International Conference on Computational and Information Sciences. Piscataway: IEEE, 2012: 566–569.
- [44] ZUO Y. Survivable RFID Systems: Issues, challenges, and techniques systems[J]. IEEE Transactions on Man and Cybernetics, Part C: Applications and Reviews, 2010, 40(4): 406–418.
- [45] SARMA S, WEIS S, ENGELS D. RFID systems and security and privacy implications [C]// CHES 2002: Workshop on Cryptographic Hardware and Embedded Systems. Heidelberg: Springer, 2002: 454–469.
- [46] JUELS A. RFID security and privacy: a research survey[J]. IEEE Journal of Selected Areas in Communications, 2006, 24(2): 381–394.
- [47] 王保云. 物联网技术研究综述[J]. 电子测量与仪器学报, 2009, 23(12): 1–7.