物联网名字服务关键技术研究

刘 阳[1,2],李馨迟[1,2],田 野[1],毛 伟[1]
(1.中国科学院计算机网络信息中心,北京 100190;2.中国科学院大学,北京 100080)

摘 要: 随着物联网的高速发展,各种异构的物理实体被连入网络形成海量的虚拟资源,从而在性能和功能两个方面都为名字服务带来了新的挑战.本文首先从性能角度对物联网名字解析服务和发现服务通过层次式DNS技术、扁平式DHT技术以及混合使用这两种技术实现的架构方案进行了深入的分析比较;然后从功能角度,针对异构兼容、对等解析、隐私保护等三个关键性的需求,梳理了物联网名字服务的最新研究进展;最后探讨了物联网名字服务在未来可能的发展趋势.

关键词: 物联网; 名字服务; 命名; 寻址; 解析; 发现
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2014) 10-2032-08
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.10.025

Research on Key Technology of Name Service for the Internet of Things

LIU Yang[1,2],LI Xin-chi[1,2],TIAN Ye[1],MAO Wei[1]
(1. *Computer Network Information Center,Chinese Academy of Sciences,Beijing* 100190,*China*;
2. *University of Chinese Academy of Sciences,Beijing* 100080,*China*)

Abstract: With the rapid development of Internet of Things(IoT),heterogeneous physical entities have been connected to the network to form massive virtual resources,which bring many new challenges to the name service in both performance and functionality. From a performance point of view,we firstly give an in-depth analysis and detailed comparison among different resolution services and discovery services which are based on hierarchical DNS technology,flat DHT technology or mixing the two technologies. Then from a functionality point of view,we describe the latest research for the purpose of addressing three key issues: compatible for heterogeneity,equitable and federated resolution,and privacy protection. Finally,we summarize the development trends of name service and indicate the future research directions.

Key words: Internet of Things; name service; naming; addressing; resolution; discovery

1 引言

物联网通过自动识别和感知技术获取物品自身以及周边信息,基于网络通信技术完成物品组网及其与互联网、电信网、广播电视网的融合,借助类似互联网中域名系统的名字服务来发现和检索相关信息,利用普适计算技术使得人们能够在任何时间、任何地点、以任何方式处理这些信息,最终达到对现实世界的智能化决策和控制.物联网是对现有网络的拓展和延伸,从而将实体对象连接入网络中,再通过网络获取信息和管理资源.这里所提到的名字服务,其研究范畴通常包括命名(Naming)和寻址(Addressing)两部分.通过从一种名字到另一种名字的映射转换,名字服务可提供更加直接或更加丰富的名字映射关系及其附加属性信息.

1983年发明的域名系统(Domain Name System,DNS)[1]经过将近三十年的发展,至今仍是互联网中最为核心的名字服务.但DNS并不是一种放之四海而皆准的万能解决方案.特别是在物联网中,从性能角度看,要求名字服务在数据量大、查询量大的情况下仍需保持较快的响应速度;从功能角度看,产生了兼容异构标识、公平对等解析、安全需求增强等新的挑战.为了在物联网环境下设计合适的名字服务,研究人员做出了大量工作,但还有很多问题尚未得到有效的解决.本文力图对物联网名字服务研究的整体进展进行梳理,通过分析各种关键技术的发展趋势,为相关研究提供参考.

2 名字服务命名机制研究

物联网资源是指任何可以被寻址或者引用的物联网主体对象,而名字就是用来唯一识别资源的抽象标识符.命名机制所要研究的就是如何设计合理的编码规则

收稿日期:2013-07-08;修回日期:2014-03-31;责任编辑:李勇锋
基金项目:国家发改委物联网技术研发及产业化专项(物联网标识管理公共服务平台);中国科学院计算机网络信息中心主任基金(No.Y313041105);中国科学院一三五规划重点培育方向专项(No.CNIC_PY_1403)

来标识资源.

2.1　名字分类

现有物联网体系结构通常分为感知层、网络层、应用层等三个层次. 如图 1 所示,也可以相应的根据识别目标和应用场景将名字划分为三类: 用于识别各种实体资源的对象标识,用于识别具备通信能力的网络节点的通信标识,用于识别物联网各项应用服务组成元素的应用标识.

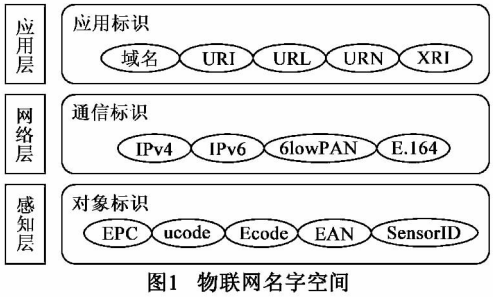

图1　物联网名字空间

此外,名字还有其它多种分类方式[2]. 根据作用范围,可以分为全局标识和局部标识; 根据区分粒度,可以分为对象标识和单品标识; 根据长度是否固定,可以分为定长标识和可变长标识; 根据结构是否分段,可以分为扁平式标识、层次式标识和混合式标识; 根据功能,可以分为身份标识和地址标识; 根据描述的实体类型不同,还可以分为用户标识、设备标识、服务标识和数据标识.

2.2　名字特征

目前,不同国家、不同组织都为其所管理的物联网资源对象设计了大量的命名规则. 但是总结起来,所有的物联网资源名字都具有以下共性特征:

唯一性　在一定范围内,应能毫无歧义的区分不同的资源对象.

多样性　名字的存在形态、分配方式、编码结构等均可有多种具体实施机制.

扩展性　名字应该可以通过一定的扩展机制来应对由于时间推移、产业发展以及其它新需求不断出现造成的变化.

关联性　一个资源可以拥有多个名字,供不同的应用和业务来识别; 反之则不然,一个名字必须唯一的对应一个实体对象或者逻辑对象.

3　名字服务寻址机制研究

名字服务中的寻址是一种在不同名字间进行映射信息转换的查询过程. 根据查询目标的资源记录所采用存储方式的不同,寻址机制可以分为集中式和分布式两类. 前者将所有资源记录存储在唯一的名字服务器上,而无需考虑多个名字服务器之间的数据同步问题,网络结构简单,但是不适应物联网作为大规模分布式网络的性能和安全需求; 后者则将资源记录分散存储在多个名字服务器上,它们之间可能是主从关系,也可能是对等关系.

对于分布式寻址网络,根据索引分布方式的不同,又存在层次式和扁平式两类设计风格. 层次式主要基于分级的树状形式组织名字服务器的体系架构,以域名系统 DNS 最为突出; 扁平式主要基于对等的环状结构组织名字服务器的体系架构,以分布式散列表(Distributed Hash Table,DHT) [3] 的形式最为常见. 除此之外,近年来也有许多学者提出兼有层次式和扁平式两种设计思想的混合式服务.

图 2 在忽略寻址服务网络的具体拓扑结构情况下,给出了一个抽象的物联网名字服务寻址架构,包括注册器、解析器、名字服务器和信息服务器等组成元素. 这里需要区分的是资源记录和信息记录,前者反映了物联网资源名字之间的绑定关系,也包含记录类型、生存时间等辅助信息; 而后者则是以文本、图片、音频、视频或其它数据形式存在的物联网信息资源本身.

除了为保证寻址稳定和高效而设置镜像/备份服务器外,互联网中传统的名字服务会将资源记录存储在指定的唯一名字服务器上. 即使针对同一名字,可能有多条不同类型的资源记录,但是信息来源基本上都是单一的,通常只由该名字所唯一标识资源的管理者提供. 而物联网中的情况则大不一样:

资源多粒度性导致寻址目标的数量不同; 资源可移动性导致寻址目标的位置不同.

以 RFID 网络为例,采用不同粒度的电子标签编码标识,可以为批次粒度的商品关联商品名称、产地等静态信息; 也可以为单品粒度的对象关联物流历程等动态信息. 基于前者寻址的目标通常只是生产商,而基于后者寻址的目标可能会涉及生产商以及商品在物流途中所经历的多个信息节点. 因此,物联网中的名字服务寻址机制又可进一步分为解析服务(Resolution Service,RS) 和发现服务(Discovery Service,DS) [4] 这样两种模式,其区别如表 1 所示. 下面将分别对其研究现状进行总结和归纳.

3.1　解析服务

互联网中的解析服务相对单一,最主要的就是 DNS 域名系统. 而在物联网中,随着标识种类的增加和标识获取设备移动性的增强,标识使用变得更加灵活. 特别是由于查询的入口往往是不可直接进行寻址的对象标识,所以解析往往需要经历多个阶段. 本节将分别介绍层次式、扁平式和混合式等三种模式的解析服务架构.

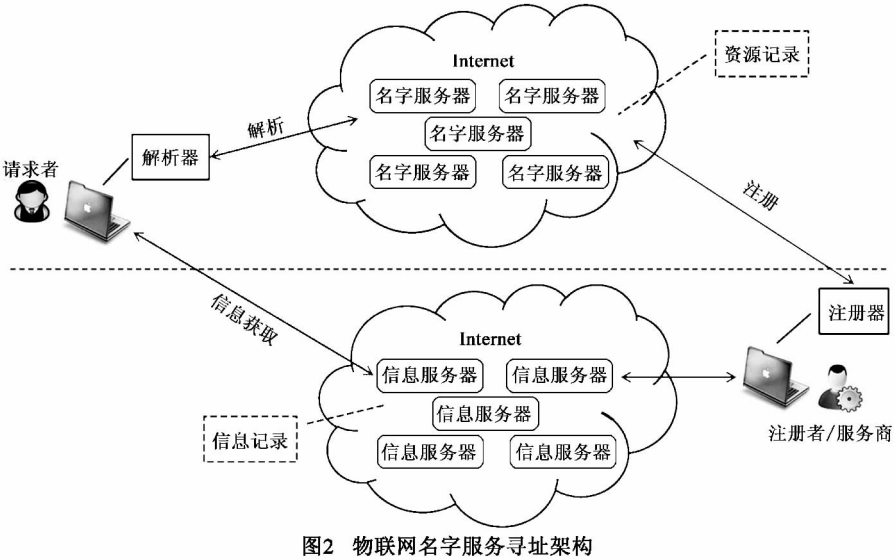

图2 物联网名字服务寻址架构

表1 解析技术和发现技术的区别

	解析服务	发现服务
信息来源	来源单一，通常是初始管理者，如物品的生产厂商	可能是物品全生命周期中经历的不同管理者，需要多源信息的整合
解析特征	共性解析，查询标识和信息源地址是一对一的映射关系	特性解析，查询标识和信息源地址是一对多的映射关系
查询粒度	批次粒度的一类商品	单品粒度的具体对象
访问控制	通常是公开服务，无需访问控制	通常是私有服务，涉及到用户隐私，在可信任用户间共享信息

3.1.1 层次式的解析服务

互联网中的长期应用实践证实了 DNS 系统的成功，因此类似的解决方案也被运用到物联网中. 美国麻省理工学院 Auto-ID Labs 提出的对象名字服务(Object Name Service，ONS)[5]是目前物联网中应用最为广泛的标识解析服务. 标准化组织 GS1 已将 ONS 用于构建全球化的 EPCglobal 网络[6]，实现对贸易单元的自动识别和跟踪，以增强供应链的信息透明度与可视性来提高物流管理水平，从而降低管理成本.

ONS 的应用场景主要局限于采用 EPC 编码的 RFID 系统. 电子标签中存储的 EPC 编码可以为其所附着的对象提供全球唯一标识，而详细的对象属性信息中则存储在生产商、经销商、销售商等信息提供者的 EPC 信息服务器内. ONS 解析服务首先将 EPC 编码转换为完全合格域名的形式，再借助标准 DNS 查询获取对应的 EPCIS 地址等映射信息.

具体工作流程如图 3 所示.

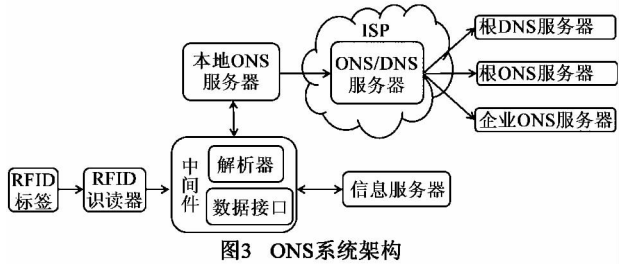

图3 ONS系统架构

3.1.2 扁平式的解析服务

也有学者认为基于 DNS 的局部改进方案无法彻底解决树状层次式结构中因根节点集中控制所带来的瓶颈等诸多缺点，提出设计新型名字服务体系架构. 典型方法就是基于 DHT 构建这样的对等分布式服务体系，将资源记录存储在扁平的环状结构中，并提供相应的环节点定位和查询功能. 由于 DHT 更适应节点的动态加入或者退出，存储和查询都被均匀分布给所有节点，所以在扩展性、鲁棒性、隐私性等方面都具有很大优势.

Benjamin Fabian 等人所提出的 OIDA 对象信息分布式体系架构[7]，成功的将 DHT 思想用于构建物联网中的名字服务. 其中，每个参与者部署自己的名字服务器节点，所有节点组成 P2P 覆盖网络. 每当有新的名字服务器加入网络，就通过加密哈希函数将服务器名字映射为 DHT 网络中的节点标识. 然后每个节点托管一部分名字空间的标识解析服务，不同节点间通过基于密钥的路由实现寻址. 典型的工作流程如图 4 所示. 文献[8]对 OIDA 理论模型进行了验证，采用 Bamboo 算法构建 DHT 系统，并在全球性开放式测试平台 Planetlab 上通过 350 个节点仿真模拟证实了 OIDA 的有效性.

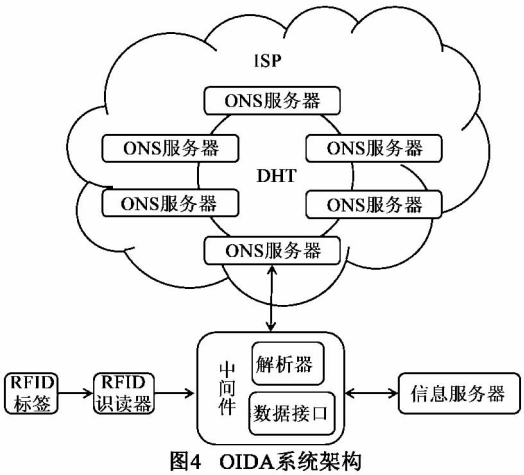

图4　OIDA系统架构

3.1.3　混合式的解析服务

基于 DNS 技术构建层次式的解析服务或者基于 DHT 技术构建扁平式的解析服务各有优缺点. 为了扬长避短,既能利用两种方式的优点,又能避免其缺点,研究者先后从三个角度提出了同时混合使用 DNS 技术和 DHT 技术构建的解析服务体系.

(1) DHT-DNS

当前域名系统,根服务器一般存储到二级域名的资源记录,三级以上则存储在权威服务器中. 为了兼顾根服务器的公平对等和权威服务器的自治管理,HDNS 系统[10] 将域名空间划分为两级,上部基于环状 DHT 扁平式处理,下部基于 DNS 层次式处理.

(2) DNS-DHT

文献[10] 则认为底层解析网络更需要借助 DHT 技术提高扩展性和稳定性,因此提出了一种截然相反的混合思路. 即在无需大规模改动现有基础设施的前提下,通过 DHT-DNS 转换器允许 DNS 树状结构下层可挂接 DHT 环状结构的权威服务器组.

(3) 多级 DHT

为了提高扁平式单级 DHT 网络的查询效率,还可根据环上不同节点的特性将其聚集为子环,从而形成多级嵌套的 DHT 网络. 例如文献[11] 中针对中国国情提出的名字编码方案就包含了国家/地区/城市等地域信息. 在此基础上,同一地域的名字服务器将被组织在一起形成小组作为下级解析网络,每个组选择一个超级节点,所有的超级节点再组成上级网络. 该方法不同于前两种混合方案,而是将层次化的思想直接作用于扁平化的设计方案. 既能将逻辑网络与物理网络更大程度的结合,减少本地数据异地存储的现象; 又能保证数据管理的自主性,使得数据拥有者仍能最大程度的管理自己的数据.

3.2　发现服务

发现服务是对解析服务的一种延伸,在静态的批次粒度映射信息查询基础上,又增加了动态的单品粒度映射信息查询,所以相对解析服务而言更加复杂,需要考虑寻址的动态性、准确性和完整性.

3.2.1　层次式的发现服务

EPCglobal 最早提出发现服务的需求,在完成 ONS 标准后即着手展开 DS 相关研究. 其基本思想是以基于对象标识通过 ONS 解析首先查询到发现引擎地址,再将查询转移到发现引擎继续. 通过参与欧盟 BRIDGE 项目,GS1 共提出八种可能的发现服务查询模式[12] ,并认为其中目录服务模型和请求传播模型等两种方案最具参考价值. 虽然 GS1 至今尚未推出具体的标准和规范,但可以推测其发现服务的体系架构仍是类似于 DNS/ONS 的层次化设计.

3.2.2　链式的发现服务

由供应链追踪管理这一实际应用所启迪产生的链式发现服务,是指随着物品在不同供应链节点间的流通,为其在同一层次的节点之间建立指针性的链接关系,从而通过正向或者逆向的遍历链表来实现发现服务查询.

例如 IBM 研发的 Theseos 系统[13] 就是基于这样的思想,将信息服务器和名字服务器融为一体,在每个信息服务器上安装搜索引擎来存储本地的名字资源记录. 查询时首先在本地进行检索,若无法命中,则重写该查询请求并递归的转发给其它信息服务器. 但这种无结构化 P2P 网络的组织形式导致查询时延往往很长.

3.2.3　扁平式的发现服务

基于供应链追踪的模式过分依赖于信息服务器所组成的信息链条,无论是在链条构建阶段还是查询阶段,如果发生断裂都会严重影响查询效果. 基于 DHT 的结构化分布式网络可以有效解决这一问题[14] . 但是这种直接将物联网资源对象的名字空间与名字服务器的节点标识空间相互关联的方式,需要所有供应链参与方的绝对信任才能实施,不能很好的符合实际需求. 为此,文献[15] 提出每个行业、组织或者公司设置各自的发现服务器,分别负责一定编码规则的发现服务或者指定公司码空间内的发现服务,而所有的发现服务器按照 DHT 算法组成逻辑环. 此外,基于 DHT 算法构建名字服务[16] 也普遍面临查询延迟时间过长的问题.

3.3　对比分析

名字服务是物联网资源管理的必经步骤,但并不是物联网服务的主体本身,所以衡量标准首要考虑的就是查询效率. 选路可用是衡量多跳转发的查询请求是否能够成功,查询时延是衡量在选路可用的前提下查询所需的全部时间,有效缓存也是提高查询效率的重要参数. 同时,名字服务又是一种公共服务,负载均

衡是能够在整个物联网范围内提供服务的前提. 因此，本文从选路可用、查询时延、有效缓存、负载均衡等四个方面来进行对比分析.

(1) 选路可用

根据 DNS 的冗余机制，每一个主名字服务器都应该有若干从名字服务器. 假设 DNS 树状结构中，第 i 层有 n_i 个这样的备份节点，则成功选路最多有 $\prod n_i$ 种. 因为不同备份节点都保存有完全相同的区文件，所以只要一层中有一个备份节点可达，选路就可以继续向下一层开展. 而 DHT 系统中，每一个逻辑节点都维护着含有若干后继节点信息的路由表，节点间存在多种冗余连接. 不失一般性的以 Chord 算法为例，N 个节点组成的 DHT 网络中任意两个节点间最多有 $(\log N)!$ 种成功选路[17]. 但实际上，只要选路中某一步所途径的逻辑节点失效，那么整次选路都将宣告失败，可见 DHT 并不能充分利用所有的冗余路径.

(2) 查询时延

不考虑缓存的情况下，在选路成功后，名字服务的查询时延主要取决于查询所经过名字服务器的平均跳数. 假设 DNS 树状结构中，树高为 h 层，则平均跳数最多不会超过 $O(h)$. 而 N 个节点组成的 DHT 网络中，平均跳数在 $O(\log_a N)$ 左右. 随着网络规模的增大，查询时延呈现对数增长，成为制约扁平式名字服务发展最重要的原因. 多层 DHT 网络增加了跨层转发而带来的时延，但组内的本地查询会相对更快.

(3) 有效缓存

缓存是提高名字查询效率的重要途径. DNS 机制在解析器和递归名字服务器都设置了相应的缓存机制，来保存最常访问或者最近访问的查询记录. 缓存有效性只取决于本地/局部查询请求的历史，独立于网络中的其它节点. 而 DHT 系统中缓存的记录通常是源自所有查询请求的统计分布，各节点将保存整个系统中最为流行的查询记录.

表 2 不同体系架构下名字服务的性能比较

(+：良好；o：中等；−：差)

		选路可用	查询时延	有效缓存	负载均衡
层次式方案		+	+	+	−
扁平式方案		−	−	−	+
混合式方案	DHT-DNS	o	−	−	+
	DNS-DHT	+	o	o	+
	多级 DHT	−	o	o	+

(4) 负载均衡

DNS 的树状拓扑结构，使得各层域名服务器的重要性大不相同，尤其是金字塔架构顶端的根名字服务器、顶级名字服务器都需要承受巨大负载压力. 上层名字服务器的负载又不能合理的分配给其他名字服务器分担，一旦上层域名服务器发生故障就可能会导致大量名字解析失败. 基于 DHT 的扁平结构自动通过散列方式将查询负载很好的分布到全部对等的名字服务节点上，可以有效解决这一问题.

4 物联网时代的新挑战

从互联网拓展和延伸出来的物联网，由于把海量的物理实体联入网络，所以不仅携带了原来互联网所存在的一些缺陷，还面临诸多新的问题，这对名字服务也带来了新的挑战. 接下来，本文将从异构兼容、对等解析、隐私保护等三个方面重点介绍针对物联网标识服务的最新研究进展.

4.1 异构兼容

物联网的终极目标是实现各种资源统一寻址和互联互通，不会局限于为某一种应用而在一定的国家或者组织内部使用单一的组网技术、命名手段和解析服务来构建封建闭环. 因此，异构多编码的兼容性解析成为物联网名字服务的重要研究方向.

4.1.1 URNS

URNS 体系[18]采用协议名作为区分，包含 URI 中心网络和 P2P 逻辑子网两部分. 前者采用 URI 解析机制，无需客户端的解析器做任何改动；后者则基于 Chord 算法分别组织各异构的 P2P 逻辑子网. URI 中心名字服务器的资源记录只保存各异构 P2P 逻辑子网的入口服务器地址，然后通过 URI 协议名将名字解析请求转发给相关逻辑子网的入口服务器，在逻辑子网内部按照 Chord 算法查找名字资源记录.

4.1.2 ID@URI

赫尔辛基大学在 DIALOG 系统中使用了 ID@ URI 名字服务[19]，将对象标识分为 ID 和 URI 两个部分，由“@”隔开. URI 部分由 DNS 提供解析，ID 部分格式则由本领域管理者自行规定，只需要在给定范围内是唯一的就可以保证整个对象标识的全球唯一性. 如果 ID 选用产品序列码，URI 选用信息服务器的域名标识，这种机制就与 ONS 相似. 不同之处在于，ID@ URI 机制可以完全使用现有的 DNS 解析服务，ID 部分不一定使用 EPCglobal 分配的 EPC 编码，更无需先将 EPC 编码转换为 URI 格式，再进行新的 ONS 解析. 该方案的缺点在于 ID@ URI 标识一经分配就难以修改，URI 部分无法实时动态更新.

4.1.3 RNS

文献[20]最早提出为解决任意物品编码标准共存问题采用多次迭代寻址模型的思路. 文献[21]中采用两段式物联网资源命名机制的 RNS 名字服务体系则是对该思路的进一步探索. 由国家、组织所定义的标准标

识,用来规范一定的编码结构语义; 由企业、个人所定义的资源标识,用来唯一标识物品资源本身. 前者是一类物品资源获取名字服务的入口,可能被频繁解析,而且是一种公共资源,需要开放给不同的国家、组织共享; 后者则是特性资源,可能只有特定物品资源的所有者才会查询,属于内部资源. 因此,RNS 中建议采用 DHT 网络来组织标准标识服务器,可保证其对等公平性; 采用 DNS 网络来组织资源标识服务器,来保证其解析效率和个性化管理.

4.1.4　小结

长远来看,兼容多种异构标识的根本思路还是设置分级的编码方案,可能是类似于 RNS 的两段式,也可能是更多层级的迭代寻址,但这一问题的根本性解决目前还存在两个关键的阻碍: 第一,标准标识的选择. 什么样的标准标识能够为各国家、各标准组织所接受,由谁来负责维护此类标识的分配和管理,都值得进一步商榷. 第二,标准标识的使用. 现有的各种命名机制中并没有预先分配标准标识,解析器往往也不能支持预先进行标准标识解析. 即使未来的技术能够全面支持这些改进,如何兼容现有编码方案会非常困难.

4.2　对等解析

出于主权安全以及商业竞争的目的,世界各国、各组织都希望能够管控与其所拥有物联网资源相关的名字服务. 以 ONS 为代表的集中式控制体系势必造成根节点单极化的问题,影响名字服务作为一个公共服务的可用性和可靠性. 对等解析就是试图在根层级上,将单根服务器分解为多个对等的服务器,保证每一个对等根的权级相同. 从而实现不同名字服务系统间的互联互通,从根本上保障安全性.

4.2.1　MONS

MONS(Multipolar Object Name Service) [22] ,是对现有 ONS 体系的修改,通过在多个地区备份根服务器的副本并由不同的独立实体维护,再依据查询发起者的身份将解析请求分散到本地根节点完成. 提高了解析查询的对等性,但需要在多个根节点之间同步完整的根区文件,而物联网名字服务中的根区文件又远远超过了互联网 DNS 系统的根区文件大小,所以同步所带来的网络通信开销会很大. 同时,由于同步的信息来源仍然是由 EPCglobal 所维护和发布,所以并不能实现真正的对等解析.

4.2.2　FONS

AFNIC 提出的 FONS(Federated Object Name Service) [23] ,则提议建立多个对等的根服务器,不同的根之间通过“国家码-国家域”映射表进行合作. 参考现有 DNS 系统的管理体系,建立“全球根服务器-洲际根服务器-国家/地区层级服务器-本地服务器”的四级 ONS 管理体系,不同的解析请求将按照对象标识中的国别码,通过 DNAME 资源记录被重定向到本地区的名字服务器完成. 目前,包含这一解决方案的相关草案已经被提交给 GS1 标准组织,并成为新的 ONS 2.0 标准的一部分.

4.2.3　小结

公平、对等的解析环境对自治性很强的物联网而言至关重要,在保证名字服务可以处理跨越多个自治子网的资源定位和信息检索并助力于物联网实现真正互联互通的同时,又能保证资源拥有者对资源的自主控制权,自行维护和管理本地的名字服务设施. 虽然 FONS 中的根节点映射表和 DNAME 重定向资源记录可以有效解决这一问题,但仍然需要进一步考虑如何将根节点映射表分布式存储,以及通过多权威共同签名等方式保证根节点映射表内信息的真实性和可靠性.

4.3　隐私保护

以互联网为依托的物联网,不可避免的也会遇到互联网中原有的各种安全隐患 [24] ,最突出的就是隐私保护问题. 一方面是名字资源记录发布者的权益,另一方面则是名字资源记录查询请求者的权益.

4.3.1　注册信息的隐私保护

互联网的名字服务是一种完全公开的基础服务,所有资源记录都可被任意用户自由查询用来定位资源. 管理者只关心资源记录的完整性和真实性,而并不关心谁可以获取这些资源记录. 但物联网将物理实体连入网络的同时也将金融、军事等敏感信息传入网络. 针对这种敏感资源,物联网名字服务就需要进一步增加对访问控制的考虑.

针对这一问题的早期研究主要是参照互联网的模式,不对名字服务查询行为本身进行访问控制,而是将接入认证完全寄托于内容供应商提供的信息服务器. 但这种基于细粒度的访问控制 [25] 过多依赖于信息服务器的具体情景,不适合大型网络的信息共享. 为此,SecDS [26] 将访问控制由信息服务器转移到了名字服务器来处理,并对名字资源记录的发布者开放接口,可以编辑基于属性的安全策略. 但是名字服务器也不是绝对可信的,文献 [27] 提出采用一定的认证体系对名字服务器本身进行授权和认证.

4.3.2　请求信息的隐私保护

除了注册名字资源记录的信息发布者的权益需要通过访问控制的形式予以保护外,由于敏感信息查询记录也可能泄露查询请求者的经济状况、地理位置、兴趣爱好等个人隐私信息,所以如何更好地保护请求者的个人隐私也是一个关键的问题. 鉴于现有名字服务的查询报文基本上都是明文传输,所以第一种方案就是使用加密的策略. 例如通过扩展 DNS 协议和第二代洋葱路由协议实

现的安全 ONS 查询机制[28]. 第二种方案是可以基于临时化的身份分配. 例如文献[29]中名字服务的查询请求将由本地名字服务器转发. 可信的第三方认证服务器在注册阶段就首先为各本地名字服务器分配一个临时的身份信息,既完成了对本地名字服务器的身份合法性验证,又保证了请求者的匿名性. 第三种方案是基于匿名化的数据发布和查询. 匿名化方法的基本特征是通过泛化和抑制操作对数据进行扭曲、扰乱和随机化,但维持其真实信息的一致性. 目前最主要的匿名化技术手段是 k-匿名[30]和 l-多样化[31],文献[32]基于此类方法设计了匿名化的 RFID 数据发布平台.

4.3.3 小结

名字服务作为一种向整个物联网开放的公共第三方查询服务,在提供信息共享的同时,个人隐私的保护也是一个巨大的挑战. 任何单一角色都无法完全解决这一问题,需要名字服务架构中的名字服务器、信息服务器、解析器、注册器等各种组成元素都参与进来,才能构建一个完整的安全体系,充分保障用户在信息发布、信息查询等各个环节的隐私安全. 同时,各种隐私保护机制还需要与服务质量、信息损失、查询多样性和运行时间进行权衡. 因此,如何定义可动态灵活变化的安全策略,以及研究时间复杂度更低的隐私保护算法等都具有重要意义.

5 总结和展望

物联网名字服务作为一项关键的基础服务,是联通用户、资源和设备的重要纽带[33],也是构建整个物联网体系架构的一种切实可行的模式. 本文首先介绍了物联网名字的分类和特征,然后从性能和功能两个角度分别综述了物联网中名字服务的主要研究进展. 在未来,名字服务的发展方向可能是: 第一,面向混合式名字服务体系架构的探索. 鉴于 DNS 的层次式设计和基于 DHT 的扁平式设计各有优缺点,都无法满足物联网对名字服务的需求. 综合使用这两种技术的混合式解决方案值得进一步探索,并可通过真实环境的实际部署探索其有效性. 第二,名字服务在更多异构子网间的推广. 目前,发现服务最主要的应用场景是基于 RFID 技术的供应链管理. 但实际上,物联网中的其它自治网络环境下也同样存在这样的需求. 例如 WSN 中针对传感器节点的名字查询,信息可能来自传感器制造商、加工商、销售商,也可能来自传感器当前所属的网关服务器,或是传感器数据汇集的中心服务器. 第三,固定名字服务向灵活搜索服务的演变. 传统的名字服务(如 DNS)都是采用固定的报文格式和单一的名字资源记录,无法满足物联网在灵活性方面的需求. 根据查询者所处的上下文环境,选择查询区间[34];当直接标识无法获取时,基于时间属性或空间属性等间接标识[35];支持区间标识的查询、多关键字查询、部分关键字查询等其它形式的名字服务[36]等问题,在物联网环境下都值得进一步研究和探索.

参考文献

[1] Mockapetris P. Domain names - concepts and facilities [S]. RFC 1034, IETF, 1987.

[2] 曹锐,吴建平,等. 互联网命名问题研究[J]. 软件学报,2009,20(2):363-374.
Cao Rui, Wu Jianping, et al. Research on Internet naming [J]. Journal of Software, 2009, 20(2): 363-374. (in Chinese)

[3] Urdaneta G, Pierre G, et al. A survey of DHT security techniques [J]. ACM Computing Surveys, 2011, 43(2): 800-849.

[4] Beier S, Grandison T, Kailing K, et al. Discovery services-enabling RFID traceability in EPCglobal networks [A]. Proceedings of COMAD'06 [C]. Delhi, India, 2006. 214-217.

[5] EPCglobal. EPCglobal Object Name Service(ONS), Version 1.0.1 [S]. The EPCglobal Standards Development Process, 2007.

[6] EPCglobal. The EPCglobal architecture framework, Version 1.4 [S]. The EPCgolbal Standards Development Process, 2010.

[7] Fabian B, Gunther O. Distributed ONS and its impact on privacy [A]. Proceedings of the ICC'07 [C]. Glasgow: IEEE, 2007. 1223-1228.

[8] Fabian B. Implementing secure P2P-ONS [A]. Proceedings of ICC'09 [C]. Dresden: IEEE, 2009. 1-5.

[9] Yiting Song, et al. Study on a hybrid P2P based DNS [A]. Proceedings of CSAE'11 [C]. Shanghai: IEEE, 2011. 152-155.

[10] Yusuke Doi, Wakayama S, Ishiyama M, et al. On scalability of DHT-DNS hybrid naming system [J]. Lecture Notes in Computer Science(LNCS), 2006, 4311: 16-30.

[11] 刘学洋,赵文,等. 基于 P2P 的 RFID 编码解析网络结构与算法研究[J]. 电子学报,2008,36(12A):102-108.
Liu Xueyang, Zhao Wen, et al. Research on P2P based RFID code resolution network architecture and algorithm [J]. Acta Electronica Sinica, 2008, 36(12A): 102-108. (in Chinese)

[12] BRIDGE project. BRIDGE WP02-high level design for discovery services [R]. BuildingRadio Frequency Identification Solutions for the Global Environment(BRIDGE), 2007.

[13] Cheung A, et al. Theseos: A query engine for traceability across sovereign, distributed RFID databases [A]. Proceedings of ICDE'07 [C]. Istanbul: IEEE, 2007. 1495-1496.

[14] Manzanares-Lopez P, Munoz-Gea J P, Malgosa-Sanahuja J, et al. An efficient distributed discovery service for EPCglobal network in nested package scenarios [J]. Journal of Network and Computer Applications, 2011, 34(3): 925-937.

[15] Lorenz M, Mueller J, et al. A distributed EPC discovery service based on peer-to-peer technology [A]. Proceedings

of RFID SysTech'11 [C]. Dresden: VDE, 2011. 1 - 7.

[16] Cox R, Muthitacharoen A, Morris R. Serving DNS using a peer-to-peer lookup service [A]. Proceedings of IPTPS'02 [C]. London, UK: Springer-Verlag, 2002. 155 - 165.

[17] Gummadi K, Gummadi R, et al. The impact of DHT routing geometry onresilience and proximity [A]. Proceedings of the SIGCOMM'03 [C]. New York: ACM, 2003. 381 - 394.

[18] Yang Dong, Zhang Hongke. URNS: a new name service for uniform network resource location [A]. Proceedings of the IET Int Conf on Wireless, Mobile and Multimedia Networks [C]. Hangzhou: IEEE, 2006. 1 - 4.

[19] Framling K, Harrison M, Brusey J. Globally unique product identifiers - requirements and solutions to product lifecycle management [A]. Proceedings of INCOM'06 [C]. IFAC, 2006. 855 - 860.

[20] Kong Ning, Li Xiaodong, Yan Baoping. A model supporting any product code standard for the resource addressing in the Internet of Things [A]. Proceedings of ICINIS'08 [C]. Wuhan: IEEE, 2008. 233 - 238.

[21] Liu Yang, Tian Ye, et al. Poster: A compatible and equitable resolution service for IoT resource management [A]. Proceedings of RFID'12 [C]. Florida USA: IEEE, 2012.

[22] Sergei Evdokimov, Benjamin Fabian, Oliver Gunther. Multipolarity for the object naming service [A]. Proceedings of IOT'08 [C]. Berlin, Heidelberg: Springer-Verlag, 2008. 1 - 18.

[23] Sandoche B, et al. Qualitative evaluation of a proposed federate-dobject naming service architecture [A]. Proceedings of iThings'11 [C]. Dalian: IEEE, 2011. 726 - 732.

[24] Fabian B, Gunther O. Security challenges of the EPCglobal network [J]. Communications of the ACM, 2009, 52(7): 121 - 125.

[25] Grummt E, Muller M. Fine-grained access control for EPC information services [A]. Proceedings of IOT'08 [C]. Berlin, Heidelberg: Springer-Verlag, 2008. 35 - 49.

[26] Shi Jie, Li Yingjiu, Deng Robert H. A secure and efficient discovery service system in EPCglobal network [J]. Computers & Security, 2012, 31(8): 870 - 885.

[27] Sun Jing, Zhao Huiqun, Xiao Huibing, et al. Lightweight public key infrastructure and service relation model for designing a trustworthy ONS [A]. Proceedings of ICIS'09 [C]. Shanghai: IEEE/ACIS, 2009. 295 - 300.

[28] 吴振强,周彦伟,马建. 物联网安全传输模 [J]. 计算机学报, 2011, 34(8): 1351 - 1364.
Wu Zhenqiang, Zhou Yanwei, Ma Jian. A security transmission model for the Internet of Things [J]. Chinese Journal of Computers, 2011, 34(8): 1351 - 1364. (in Chinese)

[29] Schapranow M, et al. Securing EPCglobal object name service-privacy enhancements for anti-counterfeiting [A]. Proceedings of ISMS'11 [C]. Kuala Lumpur: IEEE, 2011. 332 - 337.

[30] Sweeney L. k-anonymity: a model for protecting privacy [J]. International Journal on Uncertainty, Fuzziness and Knowledge - based Systems, 2002, 10(5): 557 - 570.

[31] Ashwin Machanavajjhala A, Gehrke J, Kifer D, et al. L-diversity: privacy beyond k-anonymity [J]. ACM Transactions on Knowledge Discovery from Data, 2007, 1(1): 1 - 53.

[32] Chen Rui, C M Fung B. Poster: A unified RFID data anonymization platform [A]. Proceedings of RFID'11 [C]. Florida USA: IEEE, 2011.

[33] Liu Yang, et al. Auser-oriented resource management model for the Internet of Things [J]. Advances in Wireless Sensor Networks: Springer Berlin Heidelberg. 2013: 313 - 324.

[34] Perera C, et al. Context-awaresensor search, selection and ranking model for Internet of Things middleware [A]. Proceedings of MDM'13 [C]. Milan, Italy: IEEE, 2013.

[35] Ning Huansheng, et al. nID-based Internet of Things and Its Application in Airport Aviation Risk Management [J]. Chinese Journal of Electronics, 2012, 21(2): 209 - 214.

[36] Tang Yuzhe, Xu Jianliang, Zhou Shuigeng, Lee Wangchien, et al. A lightweight multidimensional index for complex queries over DHTs [J]. IEEE Transactions onParallel and Distributed Systems, 2011, 22(12): 2046 - 2054.

作者简介

刘　阳　男. 1986 年 6 月出生于甘肃天水, 2009 年毕业于南开大学信息技术科学学院, 现为中国科学院大学博士研究生, CCF 学生会员, 主要研究方向为物联网名字服务和物联网资源管理.
E-mail: gstsly@ gmail. com

李馨迟　女. 1989 年 3 月出生于北京, 2011 年毕业于首都师范大学信息工程学院, 现为中国科学院大学硕士研究生, 主要研究方向为物联网对等解析服务.
E-mail: lixinchibj@ gmail. com

田　野(通信作者)　男. 1979 年 6 月出生于重庆, 2006 年毕业于中国科学院计算所, 现为中国科学院计算机网络信息中心副研究员, 主要研究方向为物联网、下一代互联网、网络安全、移动互联网.
E-mail: tianye@ cnnic. cn