工业互联网标识解析体系综述

任语铮[1,2]，谢人超[1,3]，曾诗钦[1,2]，赵浩然[1,2]，喻嘉义[1,2]，霍如[4]，黄韬[1,3]，刘韵洁[1,3]

（1. 北京邮电大学网络与交换国家重点实验室，北京 100876；2. 无锡北邮感知技术产业研究院，江苏 无锡 214135；
3. 网络通信与安全紫金山实验室，江苏 南京 211111；4. 北京工业大学北京未来网络科技高精尖创新中心，北京 100124）

摘 要：随着物联网、5G 和工业技术的发展，工业互联网已成为新兴研究领域。由于工业生产的特殊性，对标识解析服务的时延、安全性、稳定性都提出了更高要求。传统 DNS 标识主体单一、解析结果僵化、安全保护薄弱，无法满足工业互联网要求。在此背景下，如何对任意对象提供高效、灵活、安全的解析服务，已成为全球关注的热点领域。首先讨论了工业互联网标识解析体系设计原则和关键支撑技术，其次对现有标识解析体系进行了概述和对比分析，然后阐述了新型标识解析方案研究成果，最后讨论了该领域面临的核心问题，并对未来发展趋势进行了展望。

关键词：工业互联网；标识解析；句柄；对象标识符；泛在识别技术；物联网统一标识；分布式散列表；区块链

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019238

Survey of identity resolution system in industrial Internet of things

REN Yuzheng[1,2], XIE Renchao[1,3], ZENG Shiqin[1,2], ZHAO Haoran[1,2],
YU Jiayi[1,2], HUO Ru[4], HUANG Tao[1,3], LIU Yunjie[1,3]

1. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Institute of Sensing Technology and Business, Beijing University of Posts and Telecommunications, Wuxi 214135, China
3. Purple Mountain Laboratories, Nanjing 211111, China
4. Beijing Advanced Innovation Center for Future Internet Technology, Beijing University of Technology, Beijing 100124, China

Abstract: With the development of the internet of things (IoT), 5G and industrial technology, industrial IoT has become a new research field. Due to the specific requirements of delay, security and stability in industrial production, the traditional DNS has limitations to meet the needs of industrial IoT because of its single identity object, rigid resolution results, and weak security. In this context, how to provide efficient, flexible and secure resolution services for universal objects has become a hot area worldwide. Firstly, we discussed the design principles and key supporting technologies of the identity resolution system in industrial IoT. Then summarized and compared the existing identity resolution systems in detail. Next, the new identity resolution schemes in academic research were introduced. Finally, the core problems and the future research trend in this field were discussed.

Key words: industrial IoT, identity resolution, Handle, OID, UID, Ecode, DHT, blockchain

1 引言

随着物联网、5G 网络和工业技术的快速发展，智慧城市、虚拟现实、工业智能化生产等新型应用不断涌现，可穿戴设备、工业机器、传感器等数量呈爆炸式增长，未来网络正由消费型向生产型转

收稿日期：2019–08–16；**修回日期**：2019–09–16

通信作者：谢人超，renchao_xie@bupt.edu.cn

基金项目：2019 年工业互联网创新发展工程基金资助项目（创新型工业互联网标识解析系统）；2018 年工业互联网创新发展工程基金资助项目（基于 SDN 技术的工业网络互联和协同平台示范应用）；国家科技重大专项基金资助项目（No.2018ZX03001014-003）

Foundation Items: The MIIT of China 2019 (Innovative Identification and Resolution System for Industrial Internet of Things), The MIIT of China 2018 (SDN-based Industrial Network Interconnection and Collaborative Platform Demonstration Application), The National Science and Technology Major Project of China (No.2018ZX03001014-003)

变。根据 2018 年思科 VNI 报告，到 2022 年，机器设备连接数量将达到 146 亿，份额将达到 51%，超过全球连接设备的一半[1]。工业生产的特殊性要求工业网络能通过智能化手段对环境信息进行感知、支持大量异构设备接入、支持海量多源、多模态数据高速率传输、具备更强的安全性，从而为企业生产提供更好的服务，这给传统互联网在架构、安全、性能上带来了巨大的挑战。

为应对上述挑战，工业互联网研究应运而生。工业互联网通过连接智能机器、人、物、料，结合先进的网络、人工智能、云计算、大数据分析等技术，实现企业自动化决策，重构工业生产，已引起业界的广泛关注。工业互联网体系架构由网络连接、平台、安全体系以及标识解析体系 4 个方面组成。其中，网络用于实现人、机、物的泛在连接，是工业互联网的基础；平台旨在打通运营数据与互联网数据，整合资源、联合优化；安全体系负责提供安全防护和保障；标识解析体系是实现工业互联网的重要枢纽，负责对物品身份进行分发、注册、管理、解析和路由，支持工业互联网中设备、人、物料的全生命周期管理，是打破信息孤岛、实现数据互操作、挖掘海量数据的基础，也是实现企业智能管理的必备条件[2]。

与互联网不同，工业网络传输海量异构多源多模态数据，多协议、多种命名格式并存，传统的域名系统（DNS, domain name system）解析服务在标识主体、解析方式、安全性、服务质量等方面面临着严重挑战，无法满足工业网络需求，其主要原因可归结为以下几点。

1) 标识主体改变。与传统互联网不同，工业互联网通信实体发生了重要演变，从以固定主机为中心演化至以人、机、物、服务、内容为中心，解析结果由 IP 地址转换为数字对象。然而，现有 DNS 服务单一，对资源描述能力不强，无法对物品、传感器、服务等进行标识，且解析结果僵化，只能为 IP 地址，无法满足工业互联网多样化、差异化需求。

2) 海量数据与超低时延要求。未来工业标识数据量将大大超过现有互联网，到 2020 年，中国工业互联网标识注册量将超过 20 亿[3-4]。然而，现有 DNS 采用中心化、层级树状结构，面对海量数据时存在单点负载过重、服务拥塞的问题，无法满足工业互联网的海量数据超低时延解析要求。

3) 安全与隐私保护。工业互联网连接产业上下游，打破了以往相对明晰的责任边界，产生更大范围、更复杂的影响，给安全防护带来了巨大挑战[5]。此外，工业互联网服务与企业生产、人员安全密切相关，从而对安全有更高要求。然而，现有 DNS 协议在设计之初并未考虑太多安全因素，协议本身存在的脆弱性使 DNS 面临各种威胁[6]，如缓存投毒、中间人攻击等。并且如上文所述，工业互联网通信主体多样，许多传统 DNS 防护机制均采用基于 IP 地址的访问控制，无法满足工业对隐私保护与安全的需求。

4) 公平对等。工业互联网标识解析服务的提供应是公平对等的，即应为每一个用户都提供中立、同等的服务。然而，DNS 采用层次化树状结构，可能导致解析服务被非法控制而使企业遭受损失，无法满足构建公平对等良性解析生态的需求。

由于 DNS 的设计模式与工业互联网需求存在矛盾，仅依靠 DNS 不足以支持对海量、多样化通信主体进行对等、安全、低时延解析，因此，面向工业网络的标识解析体系研究已在全球范围内推进，并已取得部分成果。同时，由于工业互联网标识解析建设在产业界存在巨大商业前景，关系到各国核心利益，已引起国家高度重视，并启动一系列项目和研究计划。根据工业和信息化部《工业互联网发展行动计划（2018—2020 年）》，到 2020 年底，我国将初步建成工业互联网基础设施和产业体系，建设 5 个左右标识解析国家顶级节点，标识注册量超过 20 亿。根据规划，我国标识解析架构主要包括国际根节点、国家顶级节点、二级标识解析节点和公共递归解析节点四层，每层节点保存不同信息。其中，根节点归属管理层，负责保存最顶层信息；国家顶级节点部署在北京、上海、广州、武汉、重庆，负责对接国际根节点和对内统筹，兼容多种现存标识解析体系；二级节点负责面向行业提供标识注册和解析服务；递归节点负责通过缓存等手段提升解析网络服务性能。截至目前，5 个国家顶级节点均已上线，一批行业性二级节点正在各地快速建设和探索。

本文综述了现存主要的工业互联网标识解析体系。首先，讨论了工业互联网标识解析体系设计原则与关键技术；其次，对现有体系进行概述，讨论其关键技术实现、相关研究与应用，并对所述体系进行对比分析；然后，阐述了学术界对新型标识解析方案的探索；最后，讨论了工业互联网标识解

析体系研究面临的挑战与未来研究方向。

2 工业互联网标识解析概述

2.1 工业互联网标识解析体系设计原则

与消费互联网和传统物联网不同，工业互联网的通信主体多样、对性能要求更高，传统 DNS 解析服务无法满足其需求。为切合工业互联网特点与要求，其标识解析服务设计须遵循以下 5 项原则。

1) 支持多源异构通信主体

工业互联网的通信主体来自不同的国家和企业，数据所有者错综复杂且实时变化，同时涵盖范围更广，包括物料、设备、网元、服务、操作员等，具有更高的复杂性和多源异构性；其次，目前工厂内多标准、多协议、多命名格式共存，给对象的检索与理解带来巨大挑战。所以，工业互联网标识解析体系应能支持多类型主体命名，兼容工厂内外现存的异构命名方式与解析方式，满足多源异构数据互联互通，保证多种命名格式与检索协议均能无缝加入该体系。

2) 复杂环境下标识解析服务安全保证

工业互联网背后连接着数以万计的资产，其服务的正常提供是工业生产与人员安全的基本前提，所以其对工业环境下多维度数据接入、时延、网络安全、高效传输、确定性等都提出了更高的要求[7]。工业互联网标识解析体系应能保障服务提供者与用户的安全，包括身份认证、鉴权、隐私保护等，保证身份可信、操作可信、解析过程中商业信息不被暴露。

3) 多组织参与的公平对等保证

工业互联网标识解析服务应保证公平对等。传统的 DNS 架构采用层次树状结构，存在节点被非法控制、断网停服的风险。一旦解析服务无法正常提供，企业将面临停产等问题，造成巨额损失。所以，需设计对等、多利益主体共管的工业互联网标识解析体系，构建公平、良性的解析生态。

4) 多协议、高并发、差异化需求场景下有效性保证

工业互联网标识解析服务应具备有效性。一方面，工业网络对时延、效率等要求更高；另一方面，工业数据检索势必面临高并发、差异化需求、多命名格式映射、多协议转换等问题，可能会对检索服务性能产生影响。所以，需设计合理的标识方案与解析机制，保证标识与解析服务的高效提供。

5) 提供协议层面与系统层面的可扩展性

工业互联网标识解析服务应具备可扩展性，要求其架构在设计时具备一定的前瞻性，可根据实际需求进行扩充，保证该体系在未来海量数据及新增标识方案场景下依旧能满足需求。首先在协议层面，该体系应能无缝添加其他新型标识解析协议子域；其次在系统层面，需保证命名空间可容纳未来海量数据接入，并且保证系统扩展时，新增节点对现有服务没有影响或影响很小，即使进行大规模扩展，增加至成千上万个服务节点，该系统依然十分有效。

2.2 工业互联网标识解析体系中的关键技术

根据上述设计原则，需提供多项关键技术为工业互联网标识解析体系进行技术支持，包括标识方案、标识分配机制、注册机制、解析机制、数据管理机制与安全防护方案等。然而，工业互联网标识解析体系研究尚不成熟，部分关键技术有待进一步研究。根据该领域服务需求与研究现状，本文将着重对标识方案、解析机制与安全防护 3 个方面进行介绍，并对其支撑作用进行讨论。

1) 标识方案

工业互联网标识通过定义编码格式对工业生产中的人、物、料、工业设备进行唯一、无歧义命名，为感知物理世界、信息检索提供支持，助力开展各类相关应用。现有标识方案分为层次与扁平 2 种。层次化标识往往由多个包含语义信息的字符串级联而成，具备全局性、可记忆性，但缺乏安全性，如域名方案[8]。层次化标识自动支持内容分配、多播、移动性等，并且可充分利用长尾效应，实现请求聚合，从而减轻路由器负担。然而，层次化标识的语义性在一定程度上限制了标识的生命周期。例如，现存的多个方案将资源所有者信息纳入其层次化标识，导致资源所有者更改时该标识失效。

扁平标识通常通过散列运算得到，由一系列无规律的数字或字符串组成，具备全局性、安全性，但缺乏语义信息。扁平标识具有较好的稳定性与唯一性，支持自我认证，且相对于层次化变长标识，该方案利用散列运算结果，其标识往往具有固定长度，在条目匹配时查询速度更快。扁平标识的缺陷在于命名空间有界，且难以实现名称聚合，映射表规模较大，从而制约可扩展性。此外，扁平标识不具有可读性，不利于获取其背后的信息，且资源内容改变或散列算法升级均会导致原标识失效，进而

影响内容的检索与查询。

2) 解析机制

解析机制负责定义资源的检索过程。根据解析架构的不同，现有解析方案可分为层次解析与扁平解析。层次解析采用树状结构，每个解析节点负责一个域，该结构简单，可扩展性强，利于部署；但缺陷在于各节点权力不同，根节点权限最高，父节点权限高于子节点权限，父节点可屏蔽所有子节点服务。

扁平解析往往采用分布式散列表（DHT, distributed hash table）技术实现，各解析节点进行 P2P 组网，解析条目根据 DHT 算法存储检索。该架构中每个解析节点的管理权限相同，各解析节点无权篡改和丢弃其他节点的解析请求，避免解析服务被非法控制，便于构建分权、对等的解析生态。然而，扁平解析的效率显著低于层次解析，且其分布式解析架构不存在中心节点，不利于数据收集，难以对解析数据进行挖掘和分析。

3) 安全防护

安全防护负责解析过程中的隐私保护与安全保障，主要包括身份安全、数据安全与行为安全[9]。其中，身份安全用于保证用户侧与服务侧身份真实性；数据安全一方面用于保证大量数据在公共网络的传输过程中不被窃取与篡改，另一方面用于保证数据存储安全，即数据不被暴露；行为安全通过各种访问控制技术保证对数据进行合法操作。

3　国内外标识解析体系介绍

目前，国内外已存在多种标识解析体系，根据其演进方式可分为 2 类。一类是基于 DNS 的改良路径。该路径通过对现有 DNS 架构进行扩充，提供工业互联网标识解析服务，如美国麻省理工学院提出的产品电子代码（EPC, electronic product code）技术[9]、国际标准化组织 ISO/IEC 和国际电信联盟 ITU-T 联合制订的对象标识符（OID, object identifier）技术[10-11]，我国自主研发的物联网统一标识（Ecode, entity code for IoT）技术[12-13]与国家物联网标识管理公共服务平台（NIoT, national common identification management service platform for IoT）[14-17]等。另一类是与 DNS 无关的革新路径，即针对工业互联网场景提出一套全新的标识解析体系[18]，如 DONA 基金会维护的句柄（Handle）标识解析技术[19-21]、东京大学提出的泛在识别技术（UID, ubiquitous ID)[22-23]及一系列其他学术研究。现有标识解析体系如图 1 所示。

改良路径便于实现，仅需在现有的 DNS 架构上进行扩展便可提供解析服务，设计简单且部署较快，但不能完全匹配工业要求，且解析服务十分臃肿。革新路径则针对工业互联网特殊需求提出新型架构，弥补现有 DNS 缺陷，更契合工业互联网场景。然而，革新路径难以利用现有基础设施，需重新部署，成本较高，周期较长。本文将介绍 4 个典型体系，包括改良路径的 OID 与 Ecode 体系，以及革新路径的 Handle 与 UID 体系，每个体系分别从概述、关键技术、相关研究与应用 3 个方面进行详细探讨。

3.1　基于改良路径的标识解析体系

改良路径对现有 DNS 架构进行扩充，覆盖在 DNS 服务之上，解析服务依赖 DNS 资源记录，安全防护依托于 DNS 安全保障措施，较少提出新的安全保障机制。

3.1.1　OID 体系

1) 概述

OID 体系由 ISO/IEC 与 ITU-T 国际标准化组织

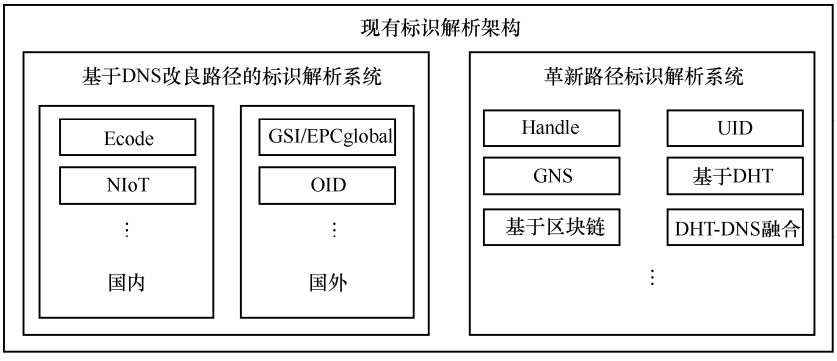


图 1　现有标识解析体系

于 19 世纪 80 年代联合提出，旨在识别物联网环境中的各种对象和服务。OID 采用分层树形结构，其编码由一系列数字、字符或符号组成，支持对任何类型的对象，包括用户、网络元件、网络服务及其他物理或逻辑对象等进行全球无歧义命名，且一旦命名该名称终生有效[11]。ISO/IEC 与 ITU-T 通过研制 ISO/IEC 29168、ISO/IEC 29177、ISO/IEC 9834、ISO/IEC 8824 等系列国际标准，针对 OID 的命名规则、分配方案、传输编码、解析管理体系等内容进行规范，设计正式、精确、无歧义的机制来标识、解析、管理对象[24]。截至 2019 年 4 月，OID 已覆盖全球 206 个国家和地区，目前国际 OID 数据库中已注册 1 408 431 个顶层 OID 标识符。

OID 体系通过将 OID 树映射为 DNS 树的一部分提供 OID 服务，具有人类可读、分层灵活、可扩展性强、跨异构系统、支持对各类对象唯一永久标识、便于部署等优势，且 OID 标识体系拥有无界命名空间，可支持全球任意对象标识[25]。此外，OID 体系支持域内自主管理，权限机构可自由地添加新节点。OID 独立于网络技术，不受底层设备影响，可兼容其他现有标识机制，具备很好的应用基础和发展前景，目前已在医疗领域、信息安全领域、物流领域等广泛使用。

2) 关键技术

① 标识方案

OID 采用分层树状结构，国际根节点下连 ITU-T、ISO 与 ISO-ITU 联合 3 个分支，支持对用户、网络元件、服务、有形资产、无形数据（如目录结构）等任意对象进行标识。OID 采用层次化标识方案，其编码规则规定了根节点到标识节点间的路径，OID 架构如图 2[26]所示。

OID 提供了 3 种常用标识方案，分别是传统标记法、点标记法与 OID-国际化资源标识符（OID-IRI, OID internationalized resource identifier），其中点标记与 OID-IRI 应用最广，其对比如表 1 所示。

传统标记法。该标识方法于 1986 年提出，以“{”开始，并以“}”结束，各子命名空间由文字和数字共同组成，并用空格分隔，具体有 3 种实现方式：a) 仅由数字组成，该标识方式贴近机器编码，检索较快，但不够人性化，目前很少被使用；b) 由文字和数字共同组成，文字后用数字插入说明，该标识方式兼顾了人类可读性与机器检索效率，但信息存在冗余，牺牲了标识的有效性；c) 由文字和数字共同组成，该标识方式对少数顶层命名空间不要

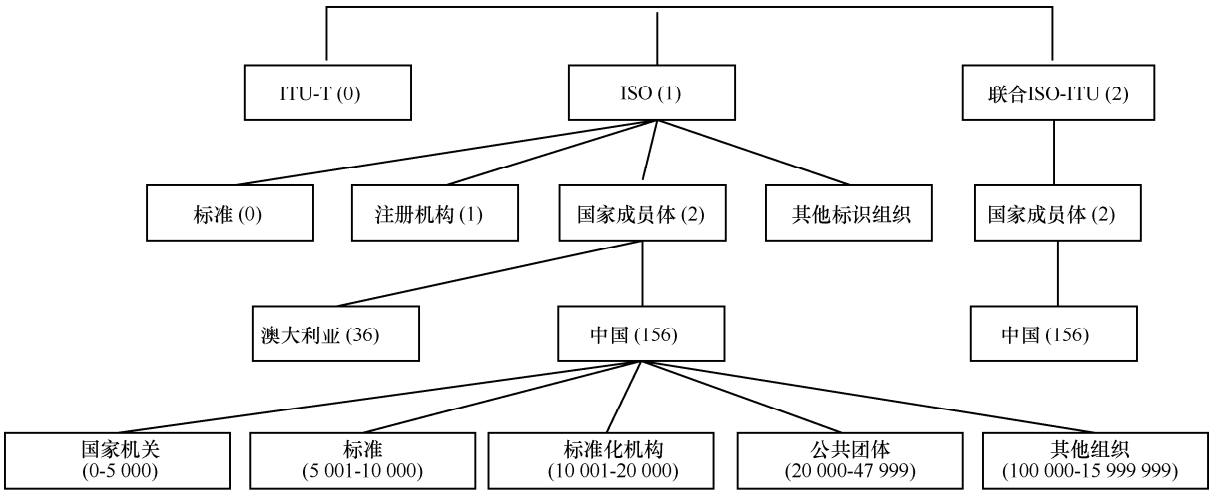


图 2 OID 架构

表 1 OID 标识方案对比

标识方案	分隔方式	标识组成	示例	特点
传统标记法	空格	数字 文字附加数字说明 文字、数字共同组成	{2 1} {joint-iso-itu-t(2) asn(1)} {joint-iso-itu-t asn(1)}	贴近机器码、检索快 可读、有效性差 性能介于上述 2 种方案之间
点标记法	点	数字	1.3.6.1.6.3	不可读、检索快、较为安全
OID-IRI	斜线	Unicode	/Joint-ISO-ITU-T/ASN1	可读、检索快、安全性弱

求数字说明、低层命名空间强制数字说明，该方式性能介于上述 2 种方式之间。

点标记法。该标识方法由互联网工程任务组（IETF, the Internet Engineering Task Froce）首次引入并沿用至今，其编码结构规范，只由数字组成，使用点标记符对不同命名空间进行分隔，标识符为由树根到叶子全部路径上的节点顺序组合而成的字符串。点标记法可读性差，但检索快速且较为安全。

OID-IRI。该标识方法是 ITU-T X.680|ISO/IEC 8824-1 中定义的一种 ASN.1 类型，于 20 世纪 90 年代提出并沿用至今。OID-IRI 由一系列 Unicode 标签组成，并使用斜线进行分隔。该标识方案具有通用、可读的优势，且允许域内自主定义标识，较为灵活，但安全性较弱。

② 解析机制

OID 解析采用递归查询方式、分层树状架构。OID 解析系统（ORS, OID resolution system）负责提供解析服务，目前可同时兼容点标记与 OID-IRI 这 2 种标识方式。ORS 依托 DNS 解析服务，通过 DNS 的完全合格域名（FQDN, fully qualified domain name）与名称权威指针（NAPTR, naming authority pointer）记录完成解析操作。NAPTR 是 DNS 记录的一种，用于记录统一资源名称（URN, uniform resource name）、统一资源定位符（URL, uniform resource locator）和普通域名的映射关系，并为客户与映射资源通信的可使用协议提供建议。OID 体系完整解析架构由应用程序、ORS 客户端、DNS 客户端、DNS 服务器 4 个子系统组成，其架构如图 3 所示。

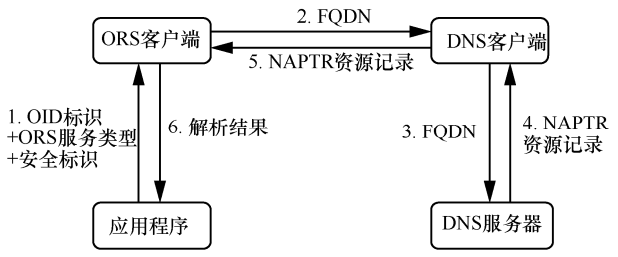


图 3　OID 解析系统架构

应用程序。该子系统负责向 ORS 客户端发送 OID 解析请求，该解析请求由 OID 标识、ORS 服务类型与安全标志组成，其中 ORS 服务类型是用于标识 ORS 服务的字符串，在 NAPTR 资源记录中使用。

ORS 客户端。该子系统通过功能接口与应用程序和 DNS 客户端通信，接收应用程序发送的 OID 解析请求。该子系统有 2 个主要功能：当接收到应用程序的请求后，该子系统将 OID 标识转换为 FQDN，并向 DNS 客户端发送 DNS 解析请求，以获取该 FQDN 的 NAPTR 记录；当接收到 DNS 客户端的回复后，ORS 客户机处理该 NAPTR 记录，并向应用程序返回零个或多个信息与 DNS 响应代码。

DNS 客户端。该子系统负责接收 ORS 客户端发送的 DNS 解析请求，并将该请求转发至 DNS 服务器，以获取相应 FQDN 的 NAPTR 资源记录。

DNS 服务器。该子系统负责响应 DNS 客户端的请求，返回相应的 NAPTR 资源记录或错误信息。

相较于其他解析架构，OID 解析具备分层灵活、可扩展性强、可利用现有网络基础设施、便于部署等优势。然而，OID 解析需依托 DNS，所以 DNS 系统本身的升级、替代或故障均会导致 OID 无法提供服务。其次，OID 解析继承了 DNS 单点故障、单点失效、负载过重和易被非法控制等问题。再次，OID 是 DNS 在一切对象和资源上的扩展，而 DNS 是支撑互联网正常运行的重要基础系统，任何针对 DNS 的扩展都应格外谨慎。此外，DNS 已经面临负担过重的问题，基于 OID 体系的工业互联网时代将有大量请求涌入 DNS 服务，导致 DNS 过载，对 DNS 的正常运行造成影响。

③ 安全防护

OID 体系安全防护主要依托于 DNS 的安全保障机制，ORS 客户端根据 ORS 请求中的安全标志决定 DNS 安全扩展（DNSSEC, domain name system security extensions）是否使用，除此之外并无其他安全机制。DNSSEC 是 IETF 提供的一系列 DNS 安全认证机制，通过散列运算和公钥技术形成信息摘要和数字签名，从而提供来源鉴定和信息完整性检验功能[27]。当安全标志为 1 时，OID 解析过程支持 DNSSEC，要求 DNS 服务器对返回的 NAPTR 资源记录签名，若无签名，DNS 客户端将返回 ORS 客户端一个错误代码，并且没有任何信息返回至应用程序。

OID 体系未提出额外的安全保障机制，仅允许用户选择性使用 DNSSEC 提供安全防护。该防护机制中的数字签名验证可保证解析参与者身份安全，信息摘要校验可保证数据不被篡改，但无法保证数据在传输过程中不被泄露，且该机制未提供行为安

全防护，无法保证用户对数据操作的合法性。

3) 相关研究与应用

① 相关研究

目前，关于 OID 的研究主要可以分为优化 OID 体系和部署 OID 这 2 个方面。

针对 OID 体系优化，文献[28]提出了一种面向物联网场景的基于 OID 的解析架构，该架构支持服务组概念。一个服务组由多个特定服务组成，保证事件触发时特定服务集合能并发调用，例如，该方案支持火灾发生时同时进行报警、消防报警以及开启逃生系统等。该架构采用两层注册和迭代解析，通过对服务进行标识、捆绑与动态更新，将组标识符解析为特定服务集合实现并发请求。该方案由 ORS、组服务解析服务器（GRS, group service resolution server）和服务注册（SR, service registry）3 个核心组件组成。其中，ORS 为 OID 原生解析功能；GRS 用于管理组服务，并与特定服务连接；SR 为本地解析系统，由服务提供者维护，用于管理特定服务信息。该方案利用 OID 标识服务组，支持服务请求同时发出，可以保证更低时延要求。

在 OID 部署的研究方案中，主要研究的问题是如何使其兼容异构标识方案。Jung 等[29]提出了一种面向物联网的基于 OID 架构的标识方案，该方案利用本地标识符和 OID 前缀构成虚拟标识层（VIL, virtual identifier layer）。通过 VIL 实现异构标识互操作，解析时，解析请求首先路由到 ORS，再重定向到相应的解析服务器响应解析请求，该方案可有效解决物联网异构标识符兼容和互操作问题。文献[30]提出了一种基于 OID 的异构标识集成解析架构，由 ID 注册表管理本地标识，ID 注册表在 ORS 中注册、申请 OID 标识。解析时，解析请求首先路由到 ORS，再根据 ORS 中的映射数据重定向到本地 ID 注册表。上述 2 种方案均对现有标识进行覆盖，同时支持新标识创建，不影响现存标识解析架构的操作流程、结构与拓扑等，在时延和开销上更为有效。

② 相关应用

目前，OID 技术已在 ISO、ITU 标准中被大量采用，应用于信息安全、电子医疗、网络管理、自动识别、传感网络等计算机、通信、信息处理等相关领域[24]。例如，在信息安全中，OID 用于指出 X.509 证书绑定的散列算法、公钥算法、分组算法和操作模式，具备高效可移植标识数据分组中所选算法的能力。随着工业互联网的不断发展，海量异构数据进一步涌入，对工业网络提出了新的要求。OID 以其面向多种对象、高效、灵活、兼容、可扩展等优势已广泛应用在 RFID、传感器、二维码等领域，具备良好的应用基础和发展前景。

3.1.2 Ecode 体系

1) 概述

Ecode 由中国物品编码中心于 2011 年提出，具有我国自主知识产权，拥有完整的编码方案和统一的数据结构，适用于任何物联网对象。Ecode 体系定义了编码规则、解析架构和解析服务要求，由 Ecode 编码、数据标识、中间件、解析系统、信息查询和发现服务、安全机制等部分组成。Ecode 体系采用一物一码唯一标识，在感知层，Ecode 中间件可兼容二维码、条形码等异构接入；在应用层，Ecode 能兼容其他编码方案如 Handle、OID 等。目前，Ecode 已广泛应用于我国工业生产的各个领域，为实现产品追溯查询、防伪验证、产品营销等提供有力支撑。

中国物品编码中心于 2015 年研制了我国首个物联网国家标准 GB/T 31866，该标准规定了物联网对象统一编码规则，目前已在中国物联网内广泛使用[12]。随着物联网技术的发展，Ecode 标识体系逐步建立。基于国家物联网产业化专项任务要求，近些年又有一系列核心标准发布，用于满足物联网标识应用需求、规范 Ecode 编码的注册和申请流程，保证 Ecode 编码唯一性、编码数据和注册信息的可靠性。目前，其他相关标准也正在抓紧制定中，这对于促进物联网和工业互联网产业发展有着重要意义。

2) 关键技术

① 标识方案

Ecode 为三段式层次编码，由版本（V, version）、编码体系标识（NSI, numbering system identifier）和主码（MD, master data code）构成。根据 MD 是否存在语义信息，Ecode 可分为标头编码结构和通用编码结构 2 种标识方案，如表 2 所示。

V 负责描述 Ecode 标识的版本，不同版本对应的编码长度不同。NSI 为标识体系代码，指明该标识的注册体系，如 Ecode、OID、Handle 等，用于实现异构标识体系兼容。NSI 长度由 V 决定，由我国物联网统一编码管理机构分配。MD 长度及其数

表 2　　Ecode 标识方案对比

标识方案	编码结构	命名空间	解析方式	标识对象
标头编码结构	V+NSI+MD，MD 包含语义信息	部分版本有界命名空间，部分版本无界命名空间	标识结构解析	针对未编码对象
通用编码结构	V+NSI+MD，MD 不包含语义信息	有界命名空间	通用结构解析	针对已在其他体系注册的对象

据结构由 NSI 决定，由某一编码体系的管理机构自行管理和维护，其中标头编码的 MD 包含厂商、项目、校验等语义信息，通用编码的 MD 无语义信息。针对未编码对象，可采用标头编码结构；针对已在其他体系注册的对象，可采用通用编码结构进行映射，完成对其他标识方式的兼容。此外，针对上述 2 种编码方案，Ecode 提供了标识结构解析与通用结构解析 2 种不同的解析方式。

Ecode 为层次编码结构，由多段数字组成，具备全局性、安全性与人类不可读性。由于 Ecode 编码中包含版本、编码体系、厂商等信息，意味着厂商、项目等信息的更新会导致原编码失效，缩短了标识的生命周期。此外，由于 Ecode 编码方案中部分版本为定长编码，因此检索速率更快，但可扩展性较差。

② 解析机制

Ecode 采用迭代解析方式，同样需依托 DNS，通过 NAPTR 资源记录提供解析服务。Ecode 解析架构由应用客户端、编码体系解析服务器、编码数据结构解析服务器和主码解析服务器 4 个部分组成[13]，其架构如图 4 所示。

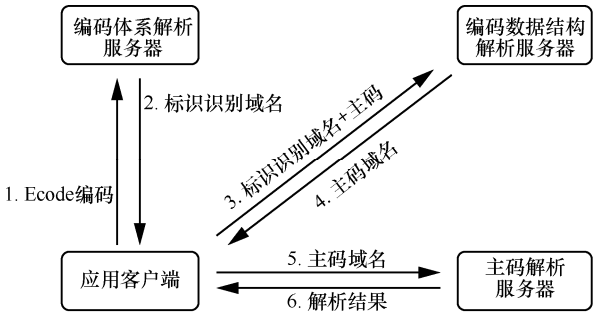


图 4　Ecode 解析系统架构

应用客户端。该组件负责分别向编码体系解析服务器、编码数据结构解析服务器与主码解析服务器发送解析请求，以获取编码所属体系、数据结构与标识解析结果。

编码体系解析服务器。该组件接收应用客户端发送的编码体系解析请求，该请求包括 Ecode 编码等信息。该组件负责将 V、NSI、MD 从接收到的 Ecode 编码中分离，根据一定的转化规则转化为标识识别域名，并将转换结果返回应用客户端。

编码数据结构解析服务器。该组件接收应用客户端发送的编码数据结构解析请求，该请求包括标识识别域名、MD 等信息。该组件以 NAPTR 记录格式存储了标识识别域名到主码域名的转换规则，并通过转换规则将标识识别域名转换为主码域名，再将转换结果返回应用客户端。

码解析服务器。该组件接收应用客户端发送的主码解析请求，该请求包括主码域名等信息。该组件通过查询 A / AAAA 记录或 NAPTR 记录得到该 Ecode 编码对应的解析结果，并将解析结果返回应用客户端，完成解析响应。

根据 Ecode 编码类型的不同，Ecode 存在标识结构解析与通用结构解析 2 种解析方式。标识结构解析中应用客户端顺次迭代查询编码体系解析服务器、编码数据结构解析服务器与主码解析服务器，逐步解析至最终结果。通用结构编码解析中应用客户端仅顺次查询编码体系解析服务器与主码解析服务器，编码体系解析服务器首先根据 V 与 NSI 判断出该编码的编码体系，如 Handle；主码解析服务器再根据其编码体系查找 Handle 体系的入口地址，将解析请求重定向到 Handle 入口。

③ 安全防护

Ecode 体系除使用传统安全技术与 DNS 防护方案外，其编码具备自认证功能，通过若干位校验码确保编码的准确性、完整性与真实性。近年来，Ecode 安全防护方案逐步完善。2019 年 4 月，物品编码中心新推出《物联网标识体系 Ecode 标识系统安全机制》标准征求意见稿，用来规定物联网标识体系中 Ecode 系统的一般要求、编码数据安全、鉴别与授权、访问控制、交互安全、安全评估和管理要求等内容。

3) 相关研究与应用

关于 Ecode 体系研究主要着眼于部署，相关研

究工作尚处于初级阶段，现有学术研究成果较少。黄永霞[31]设计了一种基于 Ecode 的冷链物流单品追溯系统，该系统由信息采集层、信息存储层、信息解析层与用户服务层组成，将产品、操作人员、温度、湿度等相关信息写入 RFID 标签，并通过阅读器回传至本地数据库，借助 Ecode 中间件完成用户解析请求。李凯迪[32]提出了一种基于 Ecode 的新型管理架构，该方案通过在 Ecode 云平台和企业间构建第三方平台解决企业间应用异构与互操作问题；同时，李凯迪基于该架构提出平台注册流程与企业注册流程，完成多企业 Ecode 管理，提供多企业数据共享与互操作能力。

目前，Ecode 已广泛应用于我国茶叶、红酒、农产品、成品粮、工业装备、原产地认证等领域，为实现产品追溯查询、防伪验证、生产营销、全生命周期管理等提供支撑。

3.2 基于革新路径的标识解析体系

基于革新路径的体系不使用 DNS 服务，提出了一套全新的标识解析体系。本节将对 Handle、UID 这 2 种典型的体系进行概述。

3.2.1 Handle 体系

1) 概述

Handle 是全球范围分布式通用标识服务系统，由互联网之父 Robert Kahn 于 1994 年提出，旨在提供高效、可扩展、安全的全局标识解析服务。Handle 系统于 2005 年加入下一代网络研究，并成为 GENI 项目中数字对象注册表的一个组成部分[33]，目前由 DONA 基金会负责运营、管理、维护和协调。Handle 体系是出现最早、应用最广的全球数字对象唯一标识符系统，提供名字对属性的绑定服务，其名字被称作 Handle，可用于标识数字对象、服务和其他的网络资源。Handle 体系包括一组开放协议、命名空间和协议的参考实现，定义了编码规则、后台解析系统和全球分布式管理架构[15]。

Handle 系统采用分层服务模型，无单根节点。顶层为数个平行的全局 Handle 注册表（GHR, global handle registry），GHR 间数据时时同步、平等互通；下层为本地 Handle 服务（LHS, local Handle service），如图 5 所示。

GHR 与 LHS 同构，均由一个或多个平行的服务站点组成，每个站点都是该服务中其他站点的复制品，每个服务站点又由多个 Handle 服务器组成。虽然每个站点都是平行的，但它们可以由不同数目的 Handle 服务器组成，所有 Handle 请求最终被均匀定向到 Handle 服务器上。GHR 与 LHS 的区别在于提供的服务不同。GHR 负责全局管理服务、分配前缀、授权命名空间。LHS 负责管理本地命名空间、定义本地命名空间的编码方式，其前缀和地址必须在 GHR 中注册。

Handle 体系从一开始就被设计为通用命名服

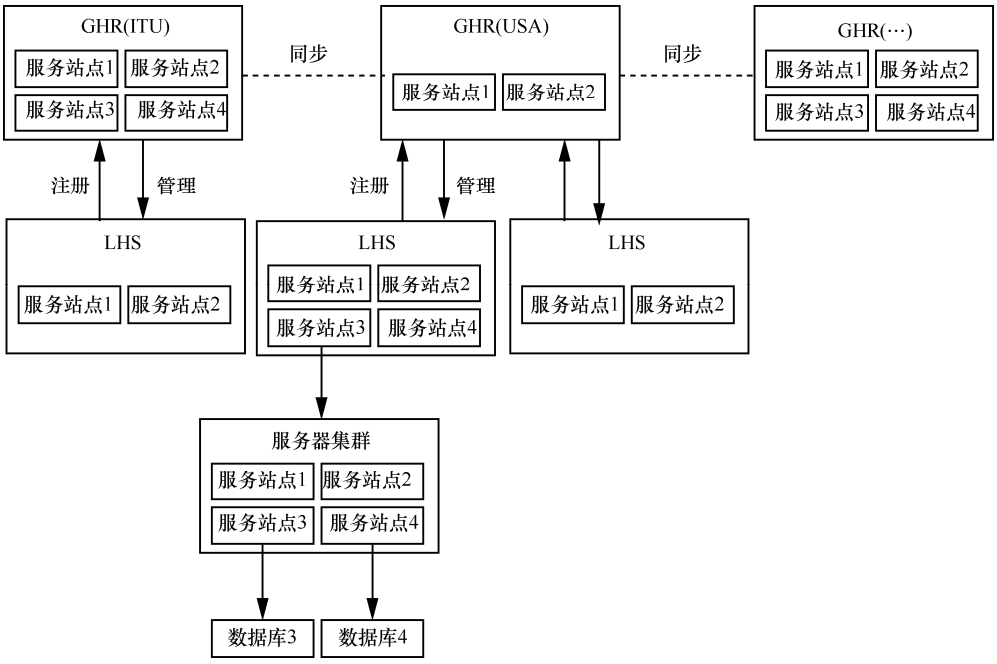


图 5 Handle 系统分层服务模型

务，可容纳大量实体，允许通过公共网络进行分布式管理，顶层节点平等互通，支持用户自定义编码，适用于工业互联网场景。此外，Handle 还具备唯一性、永久性、多个实例、多个属性、可扩展性强以及兼容其他标识等优点，目前已得到产学研各领域的日益重视和广泛应用。

2) 关键技术

① 标识方案

Handle 采用层次标识方案，每个 Handle 均由前缀和后缀两部分组成，前缀为其命名机构，后缀为命名机构下的唯一本地名称，两者由“/”分隔，如下所示。

<Handle> :: = <Handle Naming Authority>“/”<Handle Local Name>

命名机构为 Handle 标识的创建和管理者，由多个非空的子命名机构组成，子命名机构间由“.”分隔，共同形成树状分层结构；后缀由命名机构自行定义，只需保证在其本地命名空间内唯一，便可确保其在系统中是全局唯一的。例如，Handle“20.500.12357 /BUPT_FNL”的命名机构是“20.500.12357”，本地名称是“BUPT_FNL”。

Handle 全局命名空间可以认为是多个本地命名空间的超集，每个本地命名空间具有唯一的前缀，任何本地命名空间都可通过申请前缀加入全局命名空间，并且其本地标识及值的绑定关系在加入 Handle 系统后仍保持不变，只需将本地名称与前缀的组合作为全局标识，就可进行全局引用，有助于打破信息孤岛、便于企业加入各自的信息系统、兼容其他标识方案。

② 解析机制

Handle 体系提供标识到值的绑定服务，每个 Handle 可解析为一组值的集合，每个值可以是物品简介、信息摘要、URL 或其他自定义信息。Handle 体系采用迭代解析方式、层次解析架构，共分为 GHR 与 LHS 两层，其完整解析架构由 Handle 客户端、GHR 与 LHS 这 3 个部分组成，其架构如图 6 所示。

Handle 客户端。该组件负责向 GHR 发送标识前缀，以获取前缀所属 LHS 服务站点信息；向 LHS 服务站点发送完整标识，以获取解析结果。

GHR。该组件负责接收和响应 Handle 客户端发送的前缀解析请求，通过查询注册信息，检索到该前缀相应的 LHS 服务站点，并将服务站点信息返回给 Handle 客户端。

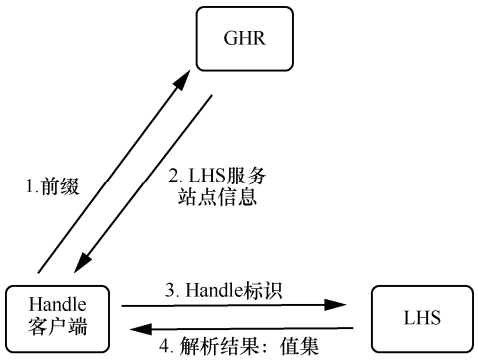


图 6　Handle 解析系统架构

LHS。该组件负责接收和响应 Handle 客户端发送的标识解析请求，通过查询本地数据库，检索到该标识对应的值集，并将解析结果返回给 Handle 客户端。

为提升解析性能，Handle 客户端可选择缓存 GHR 返回的 LHS 服务站点信息，并将其用于后续查询。根据缓存的服务信息，客户端可直接将请求发送至相应的 LHS 服务站点上，不需要询问 GHR。其次，Handle 对顶层进行了平行化改进，不再为单根架构，可部分缓解 DNS 集中式管理带来的问题。再次，Handle 允许已注册 LHS 自定义命名空间和解析机制，支持无缝添加其他协议子域，便于兼容其他标识解析体系。

③ 安全防护

Handle 体系不依托 DNS 服务，设计了一套全新的应用层解析系统与原生安全防护方案，其主要工作包含以下 3 个部分。

管理员与权限设计。Handle 体系为每个 Handle 标识设置一个或多个管理员，任何管理操作只能由拥有权限的 Handle 管理员执行，在响应任何 Handle 管理请求之前都需要对管理员进行身份验证与权限认证。Handle 管理员可拥有添加、删除或修改 Handle 值等权限。

客户端身份安全与操作合法。客户端可发起解析和管理 2 类请求，均需进行客户端身份验证。若客户端发起解析请求，Handle 服务器则根据权限对客户端进行差异化解析；若客户端发起管理请求，Handle 系统则根据质询响应协议对客户端进行身份验证。质询响应协议流程如图 7 所示。

客户端首先向 Handle 服务器发送一个管理请求；其次服务器向客户端发送质询请求来对客户端进行身份验证；然后客户端应答质询响应，并用其管理员私钥进行签名；最后服务器验证其

签名，保证客户端身份合法。若验证失败，则通知客户端；否则，服务器将进一步检查该管理员是否具有相应管理权限，若有相应权限，服务器执行该管理操作并向客户端报告成功，否则返回拒绝信息。

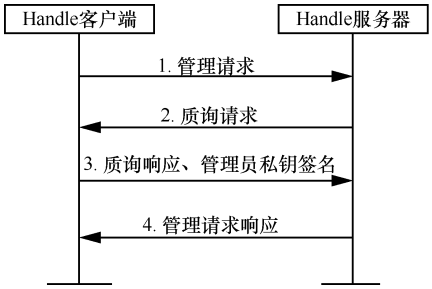


图 7 质询响应协议流程

服务器身份安全。客户机可以要求 Handle 服务器使用私钥对其响应进行签名，从而对服务器进行身份验证。

此外，Handle 系统提供分布式数据管理能力，兼容分布式、集中式、云存储等不同存储方式，保证用户数据主权，具备比 DNS 更强的内容保护机制和抗攻击能力。Handle 系统定义权限认证机制，支持数据、访问权限、用户身份等自主管理，保证身份安全、数据安全与行为安全，具备较高的安全性与可靠性。

3) 相关研究与应用

①相关研究

目前，关于该体系的研究主要着眼于 Handle 系统能否满足新型网络架构需求，保证在未来网络体系架构下其数字对象标识符依旧可用。Wannenwetsch 等[33]设计了一种面向 P2P 与命名数据网络（NDN, named data networking）的基于 Handle 的永久标识符，该方案通过结合 Handle、磁力链接（magnet URI scheme）、DHT、NDN 等技术，提供位置无关的数据解析服务。注册时，该系统将磁力链接嵌入 Handle，并将映射数据分布式存储在 DHT 网络或 NDN 内，而非传统的数据中心中；解析时，Handle 解析结果为磁力链接而不再是传统的信息存储服务器 URL，客户端可根据磁力链接将解析请求发送到相应的服务器上，由于磁力链接通过数字指纹而非文件位置或名称识别文件，因此可实现位置无关的解析服务。Schmitt 等[34]提出了一种面向 NDN 的 Handle 解析架构，该架构将 Handle 解析请求包成 NDN 兴趣包、将 Handle 解析响应包成 NDN 数据分组以便在 NDN 中传输，并且通过 Handle 网关实现 NDN 与 Handle 解析系统的连接，同时完成 NDN 数据分组与 Handle 请求的转换。Karakannas 等[35]提出了一种映射架构，该架构可实现 URN、Handle 等永久标识符在 NDN 中传输。该方案中，兴趣包内 NDN 名称由解析组件的 NDN 名称与待解析永久标识符共同组成。通过递归或迭代解析，该兴趣包内解析组件 NDN 名称将依次修改为根服务器名称、永久标识符类型服务器名称、权威服务器名称，保证其在 NDN 中顺利传输并提供永久标识符解析服务。虽然都通过构建兴趣包与数据分组实现 Handle 解析请求在 NDN 网络中传输，但与文献[33]不同的是，文献[35]中解析服务器部署在 NDN 网络内部，不需要设置 Handle 网关。

② 相关应用

Handle 体系既能与国际接轨，又可确保企业自主可控，目前已成功应用在数字图书馆、产品溯源、智能供应链等领域，为打破信息孤岛、降低成本、保证生产高协同等提供支持。

3.2.2 UID 体系

1) 概述

UID 是一种用于泛在计算的环境感知技术，支持对象及对象间关系描述，UID 中心于 2003 年在东京大学建立，得到了日本政府及企业的大力支持。截至目前，全球已有 500 多家公司和组织参与发布了 UID 标准与泛在计算系统的工业开放标准规范[36]。UID 通过泛在标识编码（ucode, ubiquitous code）标识客观实体、空间、地址、概念等物理或逻辑对象，并通过 ucode 关系模型为 ucode 间建立关联。

ucode 关系模型由 ucode 关系单元组成，图 8 展示了 ucode 关系单元结构，每个 ucode 关系单元由主体 ucode、关系 ucode 和客体 ucode 这 3 个部分组成，用于指明 2 个 ucode 或 ucode 与某未分配标识对象之间的关系。为描述多实体、复杂环境信息，UID 进一步将多个 ucode 关系单元拼接成 ucode 关系图，如图 9 所示。

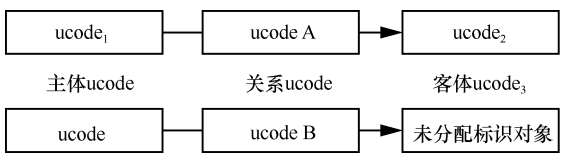


图 8 ucode 关系单元

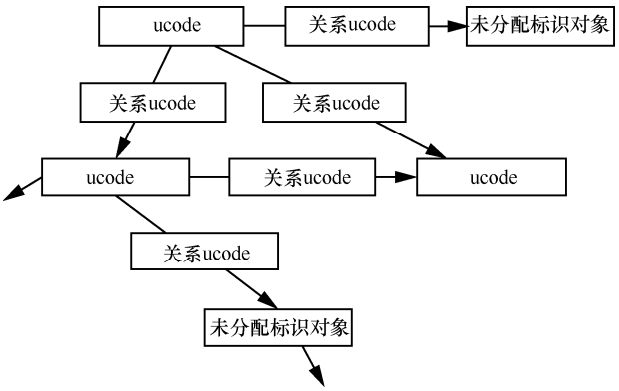


图 9　ucode 关系图

ucode 相关技术于 2012 年 10 月被写入 ITU-T 国际标准，可保证任意对象经由互联网进行识别和通信，是实现泛在计算、物联网和 M2M 计算范式的重要技术。目前，一系列基于 ucode 技术的建议书正在加速研制中，用于提供对象及其位置识别、环境理解、对象跨应用、跨组织信息交互等功能，保证最佳控制自动执行而不需要人工干预，助力泛在计算任务自动执行。该技术适用于工业互联网场景，有望用于建筑物管理、食品和医疗产品追溯、工厂设施处置、旅游信息服务及公共资产管理等应用领域。

2) 关键技术

① 标识方案

ucode 为层次、固定长度编码，由一系列无意义数字串拼接而成，其基本长度为 128 bit，并且支持长度扩展，ucode 编码长度可以扩展为 128 的整数倍，如 256 bit、384 bit、512 bit 等。ucode 命名空间采用分层结构进行管理，由顶级域和二级域两层组成[24]。每个 ucode 编码由版本、顶级域代码、类代码、二级域代码和标识码 5 个字段组成，图 10[23] 展示了 128 bit ucode 的编码结构。其中，版本占 4 bit，用于指明 ucode 版本；顶级域代码占 16 bit，用于指明该 ucode 的顶级域管理者；类代码占 4 bit，其最高位用于指明该 ucode 是否对编码长度进行了扩展，后 3 bit 用于指明二级域代码和标识码之间的边界；二级域代码长度存在多种类型，由类代码指定，用于指明该 ucode 的二级域管理者，二级域管理者由顶级域管理者分配；标识码长度存在多种类型，由类代码指定，负责对对象进行唯一标识。

相较于其他标识方案，ucode 标识主体多样，涉及实体、概念、地点、关系等对象，可满足工业场景多样化需求；其次，ucode 由一系列人类不可读的数字组成，更为安全。然而，ucode 编码并未提供兼容其他标识体系的方案，不具备兼容性；此外，ucode 采用固定长度编码方式，其命名空间受限，难以满足海量数据标识需求。

② 解析机制

ucode 关系图用于描述多个对象间关系，存储于 ucode 关系数据库内。ucode 解析系统负责接收 ucode 编码，并根据该编码在 ucode 关系数据库内检索 ucode 关系图，实现环境识别。ucode 采用递归解析方式，其解析系统由 ucode 关系数据库节点、ucode 关系数据库前端、ucode 关系词汇引擎和 ucode 信息服务 4 个核心组件组成[23]，ucode 解析系统架构如图 11 所示。

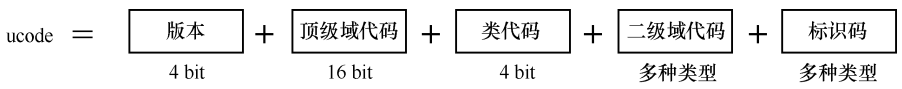


图 10　ucode（128 bit 基础长度）编码结构

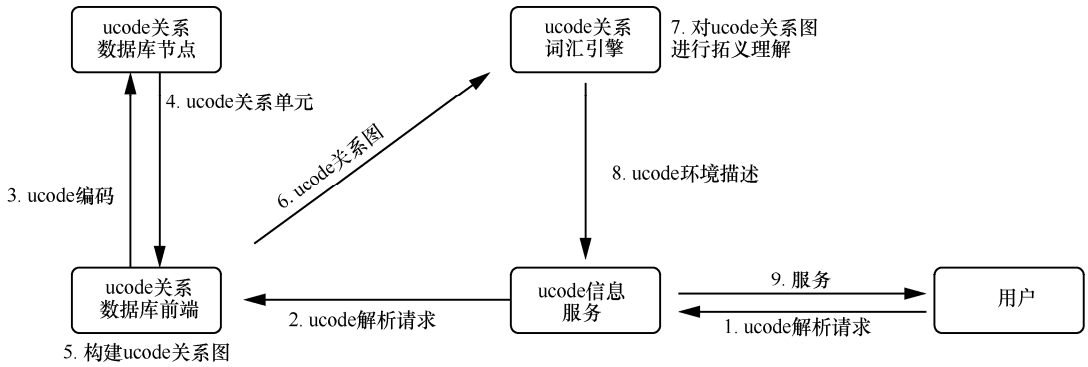


图 11　ucode 解析系统架构

ucode 关系数据库前端。该组件部署在 ucode 基础设施系统内，负责接收 ucode 编码解析请求，然后向分布式 ucode 关系数据库节点请求相关的 ucode 关系单元，并基于这些关系单元构建 ucode 关系图，之后基于 ucode 关系词汇引擎对该 ucode 环境信息进行描述。

ucode 关系数据库节点。该组件部署在 ucode 基础设施系统内，是 ucode 关系数据库中的一个独立节点，负责参与 ucode 关系单元的分布式存储。

ucode 关系词汇引擎。该组件部署在应用程序内，不同的应用程序拥有不同的 ucode 关系词汇引擎。该组件负责对 ucode 关系数据库前端生成的 ucode 关系图提供语义理解和搜索逻辑。例如，从 ucode 关系图中提取位置信息就是一种特定于应用程序的 ucode 关系词汇引擎。

ucode 信息服务。该组件部署在应用程序内，根据 ucode 关系图的搜索结果为用户提供服务。

与其他解析方案不同，ucode 解析结果为所有相关环境信息，然后应用程序根据其特定需求和搜索逻辑在环境信息中筛选出需要的内容，对象描述更为全面。不过，该体系在解析过程中需要向多个分布式节点收集 ucode 关系单元，解析效率较低。

③ 安全防护

除使用传统安全防护技术外，为满足不同应用对安全的差异化需求，UID 系统根据安全及隐私保护程度将安全功能从低到高划分为数据损坏探测功能、抗物理复制及伪造功能、接入控制功能、防篡改功能、支持与未知节点进行安全通信、支持基于时间的资源管理和支持内部程序和安全信息更新 7 个等级。

数据损坏探测功能。如果 ucode 标签由于物理损坏或干扰等导致部分数据采集时数据缺失或损坏，UID 系统可以立刻检测到，以保证数据的准确性与完整性。

抗物理复制及伪造功能。该功能保证 ucode 编码在物理上难以复制或伪造，实现数据安全。

接入控制功能。该功能通过权限定义、接入控制等技术，禁止未经授权的第三方应用识别 ucode，同时禁止其访问 ucode 相关的环境信息、状态和方法，保证行为安全。

防篡改功能。该功能负责将 ucode 的访问控制管理信息存储在标签内，且保证不能被非法读取或篡改，实现数据安全。

支持与未知节点进行安全通信。该功能负责保证即使与未预先共享私钥的未知节点通信，也可以建立安全的数据交换通道，保证数据传输安全。

支持基于时间的资源管理。该功能负责对数据、安全信息、操作等设置时间有效期，超出有效期后，所有相关的数据访问和操作都将停止，保证行为安全。

支持内部程序和安全信息更新。该功能负责保证防护系统处于最佳状态，对软件进行定时更新固件和安装安全补丁。

该体系通过实现数据损坏探测、抗复制和伪造、防篡改、与未知节点安全通信等功能，保证数据安全；通过设计接入控制、支持基于时间的资源管理等保证行为安全。通过设计上述 7 项安全防护功能，UID 体系为应用提供了细粒度、灵活的安全保护方案，满足用户对安全的差异化需求。

3) 相关研究与应用

① 相关研究

目前，关于 UID 的研究主要可以分为优化 UID 体系和部署 UID 这 2 个方面。

针对 UID 体系优化，Seike 等[37]基于区块链技术设计了去中心化 ucode 编码分配方案，以解决 UID 层次化结构带来的问题。该方案利用 ucode 编码中的顶级域代码字段定义 ucode 分配方式，保证用户可通过预约、拍卖等方式获得 ucode 编码。该方案便于实现、可应用于现有 ucode 系统，可有效解决目前 ucode 由于层次架构带来的问题。该方案通过采用区块链技术保证其标识分配过程公开透明且难以被非法控制。

在 UID 部署的研究方案中，主要着眼于如何在物联网中结合其他技术部署 OID，从而解决物联网中异构、互操作等问题。Yashiro 等[38]基于 UID 技术与受限制的应用协议（CoAP, constrained application protocol）提出 UID-CoAP 联合架构，该架构可实现在通用嵌入式节点上托管物联网服务。其中，CoAP 用于资源受限节点间通信，UID 技术负责描述实现物联网服务需要的知识和数据，该方案给出了一种将 UID 技术运用在物联网嵌入式系统中的新方法。Kiljander 等[39]基于 UID 技术提出了一种面向物联网的泛在计算互操作架构，该架构为各异构子空间建立信息服务器中介，再由信息服务器中介向 ucode 解析服务器注册。解析时，ucode 解析服务器首先将 ucode 编码解析为信息服务器中介

地址，再通过查询信息服务器将请求定向到特定的信息服务器上，从而完成解析服务，该方案可有效解决物联网泛在计算中的互操作问题。

② 相关应用

ucode 技术主要应用于日本实时操作系统内核（TRON, the real-time operating system nucleus）项目，负责为任意场所和物品植入 IC 电子标签，并分配唯一的 ucode 编码。目前，UID 系统已经从研究阶段转向商用阶段，用于支持东京都厅导游信息服务、观光巴士信息服务、上野动物园导游信息服务等。

3.3 分析与总结

表 3 从分类、标识主体及特点、解析方式、架构与结果、安全防护和应用领域等方面对上述标识解析体系进行了对比，并以 DNS 架构作为参照。从标识主体与解析结果来看，DNS 服务僵硬，无法满足工业互联网需求。OID、Ecode 这 2 种体系均依托于 DNS 服务，虽然对其标识主体和解析结果做了扩充，但仍无法满足工业互联网差异化需求。相较之下，革新路径体系服务更为灵活，支持用户自定义与环境描述，可以更好地运用在工业网络中。从标识特点看，除 UID 外，其他体系均提供不定长编码，这意味着 UID 系统能对标识进行更快速的查询和匹配，但其有界命名空间将会成为发展的瓶颈。从解析架构看，上述体系均采用层次结构，存在服务绑架风险，不过 Handle 在其顶层做了平行化处理，可部分克服层次结构的问题。从安全防护方案看，Handle 体系的安全与隐私保护设计最为全面，该体系通过公私钥技术、质询响应协议等，可较好地实现身份安全、数据安全与行为安全。

3.4 其他标识解析方案

本部分将针对新型标识解析方案学术研究进行梳理。根据技术方法，可将研究成果分为基于 DHT 技术、基于 DHT 与 DNS 技术和基于区块链技术 3 种；根据是否用于改进现有系统，可将研究成果分为改进方案与新型方案 2 种。改进方案往往未设计标识，仅对解析架构进行改进；新型方案往往同时提出标识方案与解析机制。

① 基于 DHT 的新型标识解析方案

DHT 是一种不需要中心服务器的分布式存储方法，通过某种协议将数据分散地存储在多个节点上，可有效解决集中式架构单一故障带来的服务瘫痪。同时，DHT 技术通过散列运算进行存储查询，可保证用户隐私与数据安全，目前已被广泛应用于优化和构建标识解析系统。Cox 等[40]提出了一种基于 DHT 技术的域名系统，该系统继承了 DHT 技术的容错性与负载均衡性，可解决 DNS 面临的许多管理问题。Fabian 等[41]针对 DNS 稳健性不足、配置复杂、安全性较弱等问题，提出了一种基于 DHT 的服务架构以替代对象命名服务，该方案可在一定程度上增强用户隐私保护

表 3　　现有标识解析体系对比

条目	分类	发起者	标识主体	标识特点	解析方式	解析架构	解析结果	安全防护	应用领域
DNS	无	Paul Mockapetris	主机	字符串编码；编码不定长；无界命名空间	递归、迭代	树状；单根	IP 地址	DNSSEC	消费互联网
OID	改良路径	ISO/IEC、ITU-T	任何类型的物理或逻辑对象	字符串编码；编码不定长；无界命名空间	递归	树状；单根	URL 或 IP 地址	通过安全标志决定是否使用 DNSSEC	电子认证证书、医疗卫生领域、金融领域、食品追溯领域等[25]
Ecode	改良路径	中国物品编码中心	任何物联网对象	纯数字编码；编码部分版本定长、部分版本不定长；部分版本有界命名空间、部分版本无界命名空间	迭代	树状；单根	URL 或 IP 地址	使用传统安全技术与 DNS 防护方案外；编码支持自认证	茶叶、红酒、农产品、成品粮、工业装备、原产地认证等
Handle	革新路径	Robert Kahn	数字对象	字符串编码；编码不定长；无界命名空间	迭代	两层；多根	自定义解析结果	权限设计保证行为安全；质询响应协议保证用户身份安全、操作合法；公私钥技术保证服务器身份安全	美国国防部数字图书馆项目、数字对象唯一标识符项目等[39]
UID	革新路径	东京大学	物理、逻辑对象及其关系	纯数字编码；编码定长；有界命名空间	递归	两层	环境描述	安全功能划分为 7 个等级，可满足对安全的差异化需求	泛在计算、TRON 项目

强度。Wachs 等[42]提出了一种兼容 DNS 体系、抗非法控制、对等、完全分布式、支持隐私保护的标识解析架构。该架构利用属性加密与简单分布式安全基础设施，用证书替换 DNS 可信根，映射数据通过 DHT 方式发布，实现安全、分布的标识解析服务。Rhaiem 等[43]提出一种基于多级 DHT 算法的标识解析系统，该系统将标识及其映射数据存储在多级 DHT 网络中，并由 DHT 节点提供解析服务。

② 基于 DHT 与 DNS 的新型标识解析方案

DNS 层次架构具有高效、可聚合等优势，DHT 技术拥有对等、安全等优势，已有部分学者着眼于联合二者构建混合标识解析系统。Doi 等[44]综合 DHT 与 DNS 的优势，提出了一种 DHT-DNS 混合域名系统，该系统将 DHT 命名空间挂载在 DNS 树下，DHT 节点充当权威域名服务器。当解析请求到来时，该系统将解析请求解析为某个 DHT 节点完成解析服务。Yan 等[45]提出了一种基于 DHT 与 DNS 的新型标识解析方案。该方案使用散列串标识对象，用于解决异构标识兼容问题，同时采用 0-1 二叉树构建解析架构，每个散列串都可映射为该二叉树的一个叶子节点。该方案综合了 DNS 与 DHT 的优势，能同时实现异构标识接入、对等、高效的标识解析服务。

③ 基于区块链的新型标识解析方案

区块链由 Satoshi Nakamoto 于 2008 年提出，是通过多点实现数据分享、同步和复制的去中心化数据存储技术，具备无中心、防篡改、安全等优势，可应用于标识解析系统的改进与构建。域名币是一种基于区块链的改进域名系统，该方案通过将域名存储在比特币内实现 DNS 服务，具有去中心、安全、支持隐私保护等优势。Ali 等[46-47]提出了一种基于区块链与 DHT 的新型解析系统，该系统通过散列串实现映射数据检索，自底向上分别由区块链、虚拟链和 DHT 网络 3 个部分组成。其中，区块链负责存储各域名及其对应散列串的变化；虚拟链读取底层区块链交易记录并进行抽象，按照域名存储其散列串变化；DHT 负责存储散列串及其对应的 IP 地址。注册时，映射数据存储在 DHT 网络内、域名与散列串存储在区块链内；解析时，客户端首先将域名发送至虚拟链，读取该域名对应的散列串，然后根据散列串在 DHT 网络中检索，完成解析服务。

4 未来挑战与研究展望

虽然目前国内外工业互联网标识解析技术已取得部分成果，但在架构、性能、安全等层面仍存在尚未解决的难题，有待进一步研究，具体如下。

1) 架构层面

① 多种标识解析方案兼容问题。工业互联网现存 Handle、OID、Ecode 等多种标识解析体系，给数据的互联互通和使用带来了巨大的挑战，所以如何构建异构兼容的标识解析体系，完成对多类业务、服务、数据的衔接与融合是亟需解决的问题。现存 2 种思路解决兼容问题。第一种是令原体系数据在新体系内重新注册，实现新体系兼容原体系。该类方案准确率较高但资源开销巨大。第二种不进行重新注册，只在新体系入口处训练分类器，对体系类别进行智能识别。如 NIoT 在其系统中构建异构标识识别功能[15]，通过识别算法确认输入标识对应的标识类型。此类方案开销较小，但对算法设计要求很高。

② 基于多标识解析体系的协同式服务。现存多种标识方案，包括条形码、二维码、RFID、URN、域名、IP 地址等，分别用于标识物料、传感器、工业设备、人员等，存在多个信息孤岛。为打破信息孤岛，实现生产信息的统一整合，如何基于多标识解析体系提供协同式服务是必须解决的问题，可根据以下 2 个思路进行解决：利用各体系提供的服务接口，设计合理的信息交换机制，为用户提供跨应用、跨体系的服务；对现有标识解析体系进行扩展，设计合理的架构和系统组成，实现各体系间数据和服务的互操作。

③ 解析节点权限不对等。现有标识解析体系多采用单根树状结构，该结构带来的服务节点权限不对等问题可能导致解析服务被非法控制，解析服务无法提供。即使 Handle 系统在其顶层构建多根，但仍未在根本上改变解析架构。DHT 技术与区块链技术以其去中心化的分布式存储方式，有望成为解决该问题的备选方案。目前，已有学者尝试基于 DHT 技术或区块链技术构建去中心化、对等解析架构[40-47]，保证各服务节点间权力相同，解决单根结构带来的安全问题与解析瓶颈问题等。

2) 性能层面

① 超低时延要求。工业网络对解析时延和准确性有更为敏感的要求，同时工业网络存在海量

数据高并发接入、多命名格式与协议并存等现象，所以如何设计更有效的解析机制，保证在复杂工业环境下，实现快速的命名映射与协议转换，完成超低时延跨体系、跨协议的解析服务也是亟需解决的问题。

② 可扩展性要求。工业互联网标识解析体系在标识主体、命名空间和协议上均有可扩展性要求[48]，为现有体系带来挑战。首先，如何设计合理的标识方案，保证标识主体可扩展，以满足未来多种主体标识需要是必须解决的问题；其次，如何保证命名空间足够大，以满足未来海量数据要求亟需解决；最后，如何设计合理的机制，保证设计的标识解析体系在协议层面可扩展，能无缝添加其他协议子域，实现未来其他协议和命名空间无障碍加入也值得进一步研究。

3) 安全层面

现有标识解析体系的安全与隐私保护方案不能满足工业需求。首先，基于改良路径的体系继承了 DNS 系统存在的一系列问题，包括架构脆弱、易被缓存投毒、单点故障风险等。同时，此类体系多依托于 DNS 安全保障措施，较少提出新的安全保障机制，而 DNS 安全防护方案并不完善，面临多种攻击风险，无法满足工业需求；其次，作为革新路径的代表，Handle 体系虽设计了一系列防护方案，但仅对用户设置了两级权限，数据权益保护粒度较粗，且同样无法解决缓存投毒、拒绝服务攻击等问题。此外，工业互联网标识解析服务存在大量跨信任域的访问控制，所以如何设计细粒度、动态化、轻量级、安全的跨域访问控制机制也是十分重要的研究内容。目前，已有学者开始尝试使用区块链技术解决标识解析体系存在的安全与隐私保护问题[49-50]。

4) 其他挑战

① 解析方式与结果僵化。现有体系解析方式与结果僵化，不能满足工业互联网需求，应从以下 4 个方面入手解决。第一，提供差异化解析服务。不同用户查询同一个标识，返回的结果应不同。第二，满足行业特殊需求。不同行业对解析服务要求存在差异，如交通行业对时延要求更高、林业对成本更为敏感，解析系统应能针对不同行业提供不同性能的服务。第三，自定义映射数据与解析结果。不同应用对解析结果要求存在差异，解析结果可能需要为 URL、IP 地址、商品简介等，工业互联网解析系统应允许用户自定义映射数据，支持差异化需求。第四，支持群组检索。现有解析技术只能根据标识进行粗粒度查询，无法根据对象属性或对象间相关性进行批量、群组检索。目前，已有学者提出面向工业互联网的信息聚合架构，以实现数据从多个分布式节点进行检索[51]。

② 标识失效问题。如何为对象设计永久标识是另一个需要解决的问题，永久标识是服务稳定提供的基础，现有 2 类标识思路均难以保证永久性标识。一种思路是根据对象所有者、管理者或其他属性设计包含语义的标识。然而这种标识方案具备语义信息，对象所有者、管理者或属性等信息更改时会导致标识失效。另一种思路是对资源内容做散列运算，并将散列运算结果作为标识描述对象。然而这种方案无法解决标识失效问题，资源更新后同样会导致标识失效。所以如何保证对象标识的永久性，从而提供稳定的网络服务有待未来进一步研究。

5 结束语

工业互联网已得到国内外产学研领域的充分重视，而作为工业互联网的重要支撑基础设施，标识解析技术是必须攻克的一环。本文首先讨论了工业互联网标识解析体系设计原则与关键支撑技术；其次对现有标识解析体系从概述、关键技术、相关研究与应用 3 个方面进行了综述，介绍了其核心原理与运行机制；然后针对新型标识解析方案学术研究进行了梳理；最后讨论了该领域面临的挑战与未来发展方向。

参考文献：

[1] Cisco. Cisco visual networking index: forecast and trends, 2017-2022[R]. (2019-01-27)[2019-08-16].

[2] 田野, 刘佳, 申杰. 物联网标识技术发展与趋势[J].物联网学报,2018,2(2):8-17.
TIAN Y, LIU J, SHEN J. Development and trend of IoT identifier technology[J]. Chinese Journal on Internet of Things, 2018,2(2):8-17.

[3] 工业互联网产业联盟. 工业互联网体系架构（版本 1.0）[R]. (2016-09-07)[2019-08-16].
Alliance of Industrial Internet. The architecture of industrial internet of things v1.0[R]. (2016-09-07) [2019-08-16].

[4] 工业和信息化部. 工业互联网发展行动计划（2018−2020 年）[R]. (2018-05-31) [2019-08-16].
MIIT. Development Action Plan of Industrial Internet of Things (2018—2020) [R]. (2018-05-31) [2019-08-16].

[5] 工业互联网产业联盟. 工业互联网安全框架[R]. (2018-12-11) [2019-08-16].

Alliance of Industrial Internet. Security framework of industrial Internet of things[R]. (2018-12-11) [2019-08-16].

[6] 闫伯儒. DNS 安全防护平台的研究与实现[D]. 哈尔滨: 哈尔滨工业大学, 2006.
YAN B R. Research and implement of DNS secure platform[D]. Harbin: Harbin Institute of Technology, 2006.

[7] SISINNI E, SAIFULLAH A, HAN S, et al. Industrial Internet of things: challenges, opportunities, and directions[J]. IEEE Transactions on Industrial Informatics, 2018, 14(11): 4724-4734.

[8] MARC S. An introduction to petname systems[J]. Journal of the Vacuum Society of Japan, 2014, 57(1):303-307.

[9] TRAUB K, ARMENIO F, BARTHEL H, et al. The GS1 EPC global architecture framework version 1.6[R]. GS1 EPCglobal Technology Report, 2014.

[10] ISO/IEC. Information technology——open systems interconnection -- part 1: object identifier resolution system: ISO/IEC29168-1 [S]. 2011.

[11] ISO/IEC. Information technology——open systems interconnection——part 2: procedures for the object identifier resolution system operational agency: ISO/IEC 29168-2[S]. 2011.

[12] 中华人民共和国国家质量监督检验检疫总局, 中国国家标准化管理委员会. 物联网标识体系物品编码 Ecode: GB/T 31866—2015[S]. (2015-09-11)[2019-08-16].
Identification system for Internet of things — Entity code: GB/T 31866-2015[S]. (2015-09-11)[2019-08-16].

[13] 国家市场监督管理总局, 中国国家标准化管理委员会. 物联网标识体系 Ecode 解析规范: GB/T 36605—2018[S]. (2018-09-17)[2019-08-16].
Identification system for Internet of things —Ecode resolution specification: GB/T 36605—2018[S]. (2018-09-17)[2019-08-16].

[14] YUAN B, LIU J, TIAN Y, et al. Technical specification for national common identification management service platform for Internet of things-part 1: vocabulary: Q/NIOT001-2016[S]. (2016-07-09)[2019-08-16].

[15] TAO Y, TIAN Y, YUAN B, et al. Technical specification for national common identification management service platform for Internet of Things-Part 2: Technical requirements of access: Q/NIOT002-2016[S]. (2016-07-09)[2019-08-16].

[16] TIAN Y, TAO Y, YUAN B, et al. Technical specification for national common identification management service platform for Internet of Things-Part 3: Technical requirements of sub-platform: Q_NIOT003-2016[S]. (2016-07-09)[2019-08-16].

[17] LIU J, TIAN Y, YUAN B, et al. Technical specification for national common identification management service platform for Internet of things-part 4 :requirements of identification coding structure: Q_NIOT004-2016[S]. (2016-07-09)[2019-08-16].

[18] YAN Z, LI H, ZEADALLY S, et al. Is DNS ready for ubiquitous Internet of things?[J]. IEEE Access, 2019(7): 28835-28846.

[19] SUN S, LANNOM L, BOESCH B. Handle system overview: RFC 3650[S]. IETF, (2003-11-11)[2019-08-16].

[20] SUN S, REILLY S, LANNOM L. Handle system namespace and service definition: RFC 3651 [S].IETF, (2003-11-11)[2019-08-16].

[21] LANNOM S S S R L, PETRONE J. Handle system protocol (ver 2.1) specification: RFC 3652[S]. IETF, (2003-11-11)[2019-08-16].

[22] UID Center. Ubiquitous ID architecture[R]. 2006.

[23] UID Center. Ubiquitous code: ucode[R]. 2009.

[24] 中国电子技术标准化研究院. 对象标识符(OID)白皮书[R]. (2015-07)[2019-08-16].
China Electronics Standardization Institute. Object identifier (OID) white paper[R]. (2015-07)[2019-08-16].

[25] 马文静, 吴东亚, 王静, 等. 物联网统一标识体系研究[J]. 信息技术与标准化, 2013(7): 52-56.
MA W J, WU D Y, WANG J, et al. The Research on Uniform Identification System of Internet of Things[J]. Information Technology & Standardization, 2013(7): 52-56.

[26] MEALLING M. A URN namespace of object identifiers: RFC 3001[S]. 2001.

[27] LARSON M, MASSEY D, ROSE S, et al. DNS security introduction and requirements: RFC4033 [S]. 2005.

[28] Object identifier-based resolution framework for IoT grouped services: ITU-T X.676 [S]. 2018.

[29] JUNG E, CHOI Y, LEE J S, et al. An OID-based identifier framework supporting the interoperability of heterogeneous identifiers[C]//2012 14th International Conference on Advanced Communication Technology (ICACT). IEEE, 2012: 304-308.

[30] OID-based resolution framework for heterogeneous identifiers and locators: ITU-T X.675 [S]. 2015.

[31] 黄永霞.基于 Ecode 的冷链物流单品追溯系统设计[J].中国自动识别技术,2017(2):57-64.
HUANG Y X. Design of traceability system for cold chain logistics products based on Ecode [J]. China Auto-ID,2017(2):57-64.

[32] 李凯迪.基于 Ecode 单品标识的工厂智能仓储管理新模式[J].中国自动识别技术,2019(1):51-54.
LI K D. A new model of factory intelligent warehouse management based on Ecode item identification [J]. China Auto-ID,2019(1):51-54.

[33] WANNENWETSCH O, MAJCHRZAK T A. On constructing persistent identifiers with persistent resolution targets[C]//2016 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, 2016: 1031-1040.

[34] SCHMITT O, MAJCHRZAK T A, BINGERT S. Experimental realization of a persistent identifier infrastructure stack for named data networking[C]//2015 IEEE International Conference on Networking, Architecture and Storage (NAS). IEEE, 2015: 33-38.

[35] KARAKANNAS A, ZHAO Z. Information centric networking for delivering big data with persistent identifiers[D]. Amsterdam: University of Amsterdam, 2014.

[36] KOSHIZUKA N, SAKAMURA K. Ubiquitous ID: standards for ubiquitous computing and the Internet of things[J]. IEEE Pervasive Computing, 2010 (4): 98-101.

[37] SEIKE H, HAMADA T, SUMITOMO T, et al. Blockchain-based ubiquitous code ownership management system without hierarchical structure[C]//2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation. IEEE, 2018: 271-276.

[38] YASHIRO T, KOBAYASHI S, KOSHIZUKA N, et al. An Internet of things (IoT) architecture for embedded appliances[C]//2013 IEEE Region 10 Humanitarian Technology Conference. IEEE, 2013: 314-319.

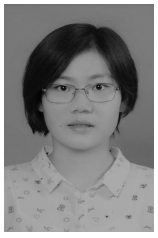
[39] KILJANDER J, D'ELIA A, MORANDI F, et al. Semantic interoperability architecture for pervasive computing and Internet of things[J]. IEEE Access, 2014, 2: 856-873.

[40] COX R, MUTHITACHAROEN A, MORRIS R T. Serving DNS using a peer-to-peer lookup service[C]//International Workshop on Peer-To-Peer Systems. Springer, 2002: 155-165.

[41] FABIAN B, GUNTHER O. Distributed ONS and its impact on priva-

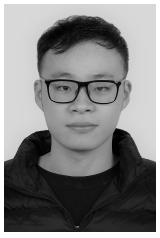
cy[C]//2007 IEEE International Conference on Communications. IEEE, 2007: 1223-1228.
[42] WACHS M, SCHANZENBACH M, GROTHOFF C. A censorship-resistant, privacy-enhancing and fully decentralized name system[C]//International Conference on Cryptology and Network Security. Springer, 2014: 127-142.
[43] RHAIEM W B, LOUATI W, ZEGHLACHE D. mhDHT: a scalable DHT-based name resolution system for the Future Internet[C]//2012 Third International Conference on The Network of the Future (NOF). IEEE, 2012: 1-5.
[44] DOI Y, WAKAYAMA S, ISHIYAMA M, et al. On scalability of DHT-DNS hybrid naming system[C]//Asian Internet Engineering Conference. Springer, 2006: 16-30.
[45] YAN Z, KONG N, TIAN Y, et al. A universal object name resolution scheme for IoT[C]//2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing. IEEE, 2013: 1120-1124.
[46] ALI M, NELSON J, SHEA R, et al. Blockstack: A global naming and storage system secured by blockchains[C]//2016 USENIX Annual Technical Conference. 2016: 181-194.
[47] ALI M, NELSON J, SHEA R, et al. Blockstack: design and implementation of a global naming system with blockchains[R]. (2016-02-25) [2019-08-16].
[48] VÖGLER M, SCHLEICHER J M, INZINGER C, et al. A scalable framework for provisioning large-scale IoT deployments[J]. ACM Transactions on Internet Technology (TOIT), 2016, 16(2): 11.
[49] SINGH S, SINGH N. Blockchain: Future of financial and cyber security[C]//2016 2nd International Conference on Contemporary Computing and Informatics (IC3I). IEEE, 2016: 463-467.
[50] ZHENG Z, XIE S, DAI H N, et al. Blockchain challenges and opportunities: A survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.
[51] ROUSSOS G, CHARTIER P. Scalable ID/locator resolution for the IoT[C]//2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing. IEEE, 2011: 58-66.

[作者简介]



任语铮（1995– ），女，北京人，北京邮电大学博士生，主要研究方向为工业互联网、标识解析技术、信息中心网络等。

谢人超（1984– ），男，福建南平人，博士，北京邮电大学副教授、硕士生导师，主要研究方向为信息中心网络、移动网络内容分发技术、工业互联网、标识解析技术和移动边缘计算等。

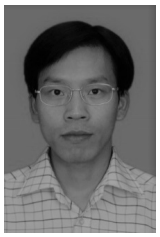


曾诗钦（1995– ），男，广西南宁人，北京邮电大学硕士生，主要研究方向为区块链、标识解析技术、工业互联网。

赵浩然（1996– ），男，重庆人，北京邮电大学硕士生，主要研究方向为工业互联网、标识解析技术、区块链。

喻嘉艺（1996– ），女，湖北黄冈人，北京邮电大学硕士生，主要研究方向为工业互联网、标识解析技术和区块链。

霍如（1988– ），女，黑龙江哈尔滨人，博士，北京工业大学讲师，主要研究方向为计算机网络、信息中心网络、网络缓存策略与算法、工业互联网、标识解析技术等。



黄韬（1980– ），男，重庆人，博士，北京邮电大学教授，主要研究方向为路由与交换、软件定义网络、内容分发网络、工业互联网等。

刘韵洁（1943– ），男，山东烟台人，中国工程院院士，北京邮电大学教授、博士生导师，主要研究方向为未来网络技术、网络体系架构、网络融合与演进、工业互联网等。