ONS安全机制研究

汪胡青[1,2] 孙知信[3,4]

(南京航空航天大学计算机科学与技术学院 南京 210016)[1]

(南京邮电大学通信与信息工程学院 南京 210003)[2] (南京邮电大学物联网学院 南京 210003)[3]

(南京邮电大学宽带无线通信与传感网技术教育部重点实验室 南京 210003)[4]

摘 要 物联网安全问题影响并制约着物联网的应用前景,成为物联网领域备受关注的研究热点之一。ONS负责将EPC编码定位到物理地址上某一点的物品信息,其安全机制得到越来越多学者的研究。介绍了ONS功能、解析流程;分析了其主要的安全隐患;分别从身份认证技术、数字签名技术和安全传输技术归纳和总结了目前已有的研究成果。最后探讨了目前研究中存在的问题,并展望了需要进一步研究的方向。

关键词 ONS,EPC,安全,身份认证,数字签名

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.1.001

Research on ONS Security

WANG Hu-qing[1,2] SUN Zhi-xin[3,4]

(College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)[1]

(College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[2]

(School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[3]

(Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education (Nanjing University of Posts and Telecommunications), Nanjing 210003, China)[4]

Abstract The IoT (Internet of Things) security problem is affecting and restricting application prospect of IoT, and has become one of the hotspots in the field of Internet of Things. ONS(Object Naming Service) is responsible for mapping function from EPC code information to URI (Uniform Resource Identifier). The security mechanism of ONS has been extensively studied by more and more scholars in recent years. The purpose of this paper is to do a survey on ONS security problem. Firstly, the function and resolution process of ONS were introduced. Secondly, the main security risk of ONS was analyzed. Thirdly, the latest research achievements were summarized based on identity authentication, digital signature and secure transmission. The current problems of ONS security and research trends in this area were also discussed finally.

Keywords ONS, EPC, Security, Identity authentication, Digital signature

1 引言

近几年,物联网的应用正逐渐改变人类的工作和生活[1-4]。物联网(Internet of Things, IoT)不仅是简单意义上的物物相联,在更深的层次上它是一个全球性的生态系统[5,6]。在这个生态系统中,人类仅仅是其中非常小的一部分,但人类的参与是其中最重要的特征,参与的形式不再停留在基本的生存生活阶段,而会过渡到更高级的感知自然、认知自然、理解自然、顺应自然、利用自然的新阶段。物联网涵盖了物与物、物与人之间的通信,体系庞大,涉及面广,应用场景复杂多样,物联网中任何一个环节错失安全防守,都有可能带来巨大的信息泄露,造成不可估量的损失[7-9]。同时,在通信网络、计算机技术稳步前进的时代,入侵攻击技术也愈演愈烈。因此,研究物联网安全机制,不断填补安全漏洞,构建物联网安全防御体系,确保物联网中通信、数据的安全性,才能保证物联网正常的发展和推广。国内外已有很多学者意识到物联网安全的重要性,并作过很多这方面的研究,提出了物联网安全架构模型。文献[10]针对物联网目前的主流体系架构,分别对每层的安全威胁进行研究,针对各类安全威胁给出相应的安全措施和建议;文献[11]提出一种基于等级划分的物联网安全模型,该模型首先预测攻击来源与类型并判定其所属的安全等级域,从而对该应用进行合适的安全技术配置;文献[12]提出了针对物联网的3层架构的4个级别的安全指标体系,并利用模糊层次分析法评价各项指标,得出提升物联

到稿日期:2014-11-26 返修日期:2015-05-11 本文受国家自然科学基金(61373135,61170276,60973140),江苏省产学研项目(BY2013011),江苏省高校自然科学研究重大项目(12KJA520003),江苏省科技型企业创新基金(BC2013027),南京邮电大学引进人才科研启动基金(NY214024),南京邮电大学校科研项目(NY210034)资助。

汪胡青(1979-),女,博士生,副教授,主要研究领域为物联网、网络安全、网络服务质量,E-mail:wanghuqing@njupt.edu.cn;**孙知信**(1964-),男,博士后,教授,博士生导师,主要研究领域为物联网、网络安全、多媒体,E-mail:sunzx@njupt.edu.cn。

网安全的关键指标主要为隐私保护、WSN 抗攻击能力、智能节点安全、信息应用安全，并说明物联网的安全属性主要体现在感知层；文献[13]从信息安全的机密性、完整性和可用性等3个基本属性出发，分析了物联网安全的特征和面临的安全问题，讨论了物联网安全的系统架构以及一些安全关键技术，包括密钥管理、认证与访问控制、安全路由、隐私保护、入侵检测与容错容侵等。上述所有文献都从不同角度为物联网提出了一种总体安全架构，为构建物联网整体安全架构提供了良好的借鉴；但是，物联网的安全机制在具体实施方案上还处于薄弱时期，还需要更细化、更具体、更明确的研究[14]。

目前关于物联网的各项技术标准还未形成统一的规范[15,16]，各个国家、组织都在积极制定自己的技术规则，其中EPCglobal 的电子产品代码(Electronic Product Code，EPC)网络标准更具有突出的影响力[17-19]。本文以 EPC 网络中对象名称解析服务(Object Naming Service，ONS)为重点研究对象，研究其工作流程，分析 ONS 与域名服务(Domain Name Service，DNS)的异同，探讨其潜在的被攻击行为及防范技术，并对其安全解决方案进行调研、分类比较。

本文第 2 节对 ONS 查询系统进行具体介绍，给出解析流程，比较 ONS 与 DNS 的异同；第 3 节基于 ONS 工作流程，分析 ONS 可能存在的威胁；第 4 节调研了目前已有的 ONS 安全解决方案，从身份认证技术、数字签名技术以及安全传输技术 3 个方面进行归类；第 5 节总结了目前方案存在的问题，展望了未来的研究趋势；最后总结全文。

2 ONS 查询系统

2.1 EPC 网络

EPC 网络是比较成熟的物联网代表[20]，以电子标签技术为基础，构建于互联网之上，不仅可以通过 RFID 非接触式技术采集物品信息数据，然后进行网络传输，还可以对物品的信息进行实时跟踪和监管，是一种能够实现自动即时识别和供应链信息共享的网络平台。EPC 网络通过收集物品的各种信息，为其他基于物联网的应用，如物品追溯、供应链分析、供应链预警、产品防伪等系统提供支持。EPC 系统主要由 EPC 编码系统、射频识别系统和信息网络系统组成，如图 1 所示。

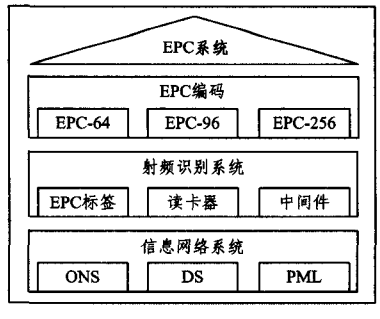

图 1 EPC 系统

EPC 编码是 EPCglobal 赋予全球物品唯一的电子编码，是 EPC 网络的基础[21]。其编码位长通常为 64、96 位，也可扩展为 256 位。EPC 编码的表示方法可以多样，包括二进制存储格式、域名字符串格式以及其他形式，不同的表示形式使用在不同的组件或者子系统中。射频识别系统中读卡器通过射频识别(Radio Frequency Identification，RFID)技术[22,23]，从物品 EPC 标签中读取出物品 EPC 编码传给中间件，中间件负责 EPC 编码的初步处理，包括过滤和收集。信息网络系统中 ONS 是一个类似 DNS 的网络服务，负责提供从 EPC 编码到与其相关的 EPCIS 地址的寻址定位；发现服务(Discovery Services，DS)[24,25]负责与 EPC 编码相关的 EPCIS 地址的汇聚和查询，从而实现物品跟踪以及历史信息的构建。实体标记语言(Physical Markup Language，PML)提供了一个描述自然物体、过程和环境的标准，由可扩展标签语言(Extensible Markup Language，XML)发展而来。

2.2 ONS 解析流程

物联网时代，人们关心自己所消费物品或其它产品的生产、运输等细节，即溯源问题。由于电子标签中只存储 EPC，而不储存产品对应的具体商业信息，因此需要 EPC 网络提供分布式存储中的各种详细信息。ONS 提供了追溯查询详细信息的入口，实现从 EPC 编码信息到统一资源标识(Universal Resource Identifier，URI)服务的映射功能。通过 ONS，用户可以获取特定 EPC 信息的存放地址，从而可以访问与 EPC 相关的详细信息。ONS 解析流程如图 2 所示。

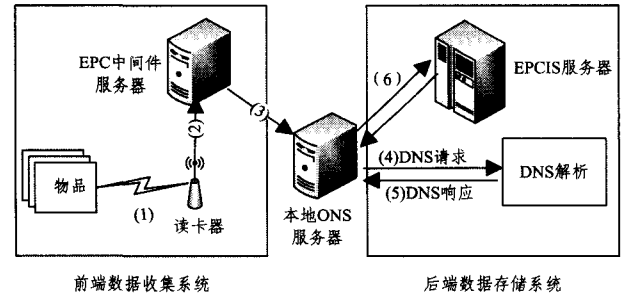

图 2 ONS 解析流程

完整的流程可以分成两部分：前端数据收集系统、后端数据存储系统。

前端数据收集系统负责物品 EPC 编码的读取、过滤和保存；后端数据存储系统负责 EPC 编码的查询与定位。具体步骤如下：

(1)阅读器读取 RFID 标签，以二进制格式获取 EPC 编码。

(2)传送 EPC 编码到 EPC 中间件服务器，中间件服务器负责 EPC 编码的过滤和存储。

(3)本地 ONS 服务器首先查询本地缓存，如果找到对应记录，解析终止，否则执行以下步骤。

(4)本地 ONS 服务器根据 EPCglobal 定义的标准，将 EPC 编码转换成合适的全域名(Fully Qualified Domain Name，FQDN)格式，提出 DNS 解析申请。

(5)DNS 解析设备返回解析结果，包括服务类型及其具体数值，解析到的结果可能是多条名称权威指针(the Naming Authority Pointer，NAPTR)记录。

(6)本地服务器从返回的 NAPTR 记录中提取出需求的 PML 服务器的 URI，访问 EPCIS 服务器，获取产品信息。

2.3 ONS 与 DNS

本小节将从以下方面对 ONS 与 DNS 进行比较。

(1)功能类似

ONS 与 DNS 都是通过解析系统的地址映射关系来获取详细的信息查询通道[26]。ONS 负责从 EPC 编码到 URI 的解析工作。ONS 服务器中并不存储与 EPC 编码相关的物品的详细信息，它只包含存储物品详细信息的 EPCIS 服务器的

IP 地址，解析到对应的 IP 地址后，查询节点可以到相应的 EPCIS 服务器上查询物品的详细信息。同样，DNS 负责从域名地址到 IP 地址的解析。

(2)解析方式类似

目前，ONS 基本上沿用 DNS 的解析方法，采用分布式的查询方式。在整个 ONS 解析系统中，ONS 服务器属于核心部件，如果查询成功，则返回该 EPC 对应的 URI，并将解析结果缓存到所经过的所有 ONS 服务器及客户端中，以备下次解析使用。类似于 DNS，ONS 层次结构的最顶层称为 ONS 根服务器，存储 EPC 名称空间中的顶级域名。一般情况下，ONS 查询请求不会到达根 ONS 服务器，但是 ONS 客户端从本地缓存或上一级 ONS 服务器中查不到所需的信息时，则将该查询请求转发给根 ONS，从根 ONS 开始逐级查询。目前，ONS 根服务器的域名为 epc. objid. net。

(3)解析结果属性不同

对于给定的 EPC 编码，由于其与产品信息相关，ONS 解析结果的内容通常是固定的，格式较短；而 DNS 解析的结果由于是网站信息，会经常发生变化。

(4)解析结果记录数不同

DNS 中，解析结果对应的 IP 网站地址一般只有一两条；而在 ONS 解析中，一般供应链越长，解析结果涉及到的 EPCIS 地址就越多，有时可能多达数十条。图 2 中，ONS 解析流程中步骤(6)NAPTR 记录的格式，如图 3 所示。

Order	Pref	Flags	Service	Regexp	Replacement

图 3　NAPTR 记录格式

其中，各字段的具体含义如下。

Order：顺序。用于保证返回的 NAPTR 记录，ONS 客户端按照 NAPTR 记录的前后顺序进行解释。

Pref：优先级。用于设置应答信息中 NAPTR 记录的优先级，该字段值越小，其优先级越高。

Flags：标记。一般设为字母“u”，说明后面的“正则表达式”字段代表一个 URI。

Service：服务。用于设置应答信息中 URI 的服务类型，用户软件可以根据服务类型选择自己所需要的服务 URI。

Regexp：正则表达式。该字段包含了指定服务类型的 URI。

Replacement：代替者。该字段暂时被保留。

当服务器返回多条 NAPTR 记录时，客户端根据“Order”和“Pref”两个字段决定选择何条 NAPTR 记录。具体策略是：当“Order”字段值相同时，根据“Pref”字段值决定选择哪一条记录，若选中的高优先级的服务连接失败，则启用次优先级的服务连接。

由以上分析可知，客户端获得了多条 NAPTR 记录，记录数越多，与产品相关的隐私信息也就暴露得越多；且客户端从多条 NAPTR 记录中的选择也可由“顺序”和“优先级”两个字段推断，即客户端的选择是公开的信息。

(5)ONS 较 DNS 安全性需求更高

DNS 设计之初是建立在互信模型的基础之上，是一个完全开放的协作体系，没有适当的信息保护和认证机制。但互信模型的前提在物联网大环境中并不成立，相对来说，ONS 在安全性方面的需求比 DNS 更高[27]。首先，需要保护 EPC 编码的隐私，一旦 ONS 服务器泄露了 EPC 编码，用户的隐私信息就会被泄露。其次，需要保证返回结果的真实性，并保护解析结果的隐私。若不能保证返回结果的真实性，根据服务器返回的解析结果，有可能会被链接到垃圾信息的网站。同时，由于不同的企业之间及企业与普通用户之间共享信息的级别不同，ONS 必须具备对 EPCIS 地址的访问权限控制功能，即对不同的用户展现不同的数据集而隐藏和屏蔽掉其他的数据。此外，ONS 的权限分配必须足够灵活和快速，以适应不稳定供应链的快速变化。

3　ONS 安全性分析

3.1　DNS 安全威胁及解决方案

ONS 查询服务的安全问题是 EPC 网络安全的基础。2013 年 1 月新出的 ONS 标准给出了 ONS 解析的一般流程，对如何将 EPC 转换为应用唯一字符串(Application Unique String，AUS)格式、DNS 查询格式、返回的记录 NAPTR 格式等都作了说明，但全文未涉及有关解析和管理的安全问题。按照 EPCglobal 的标准，ONS 的设计与架构建立在 DNS 基础之上[28]，这样，整个 EPC 网络都以 Internet 为依托，实现起来比较简单。但是这样的系统架构也继承了 DNS 系统自身的安全缺陷。DNS 的威胁主要有分布式拒绝服务(Distributed Denial of Service，DDoS)攻击[29-31]、恶意网址重定向攻击、中间人攻击、域名欺骗、缓存中毒、单点故障等[32]。前 4 类攻击均是由于 DNS 协议缺乏必要的认证机制导致[33,34]，未授权的攻击者将伪造的恶意域名信息返回给客户。在服务器端设置资源记录的缓存，在 TTL(生存期)内，可以直接查询解析过的资源，从而减少了解析通信量和客户端延时。但 DNS 协议缓存缺乏对附加数据的检查机制，攻击者利用该漏洞，将具有较大 TTL 值的恶意资源记录存入缓存，并进行扩散，实现缓存中毒攻击[35]。DNS 服务器的结构在物理上和逻辑上均是树型，容易导致单点故障问题。DNS 的解析是逐层递归或者迭代查询过程，如果在查询路径上有任何一个节点发生故障，将会导致整个解析不成功；并且越高层节点发生故障，故障的影响就越大，甚至可能导致整个网络瘫痪。

关于 DNS 的安全解决方案主要有 DNS 安全扩展协议(Domain Name System Security Extensions，DNSSEC)[36,37]和 DNSCurve[38]。DNSSEC 由 IETF 域名系统安全工作组于 1997 年提出，BIND9 系列版本开始提供对 DNSSEC 的支持。DNSSEC 考虑现有 DNS 协议本身的脆弱性，引入公钥加密和认证机制，通过签名来实现端到端的数据真实性和完整性认证。DNSSEC 存在系统效率低、密钥管理复杂、部署困难等问题。有很多文献对 DNSSEC 方案进行了分析讨论和实验验证[39,40]。文献[41]通过大规模实验的方法验证了使用 DNSSEC 的效果，得出：采用 DNSSEC 可能会使得部分用户拒绝服务，必须在成本和效益之间做出平衡。

DNSSEC 采用 RSA 算法对 DNS 数据实现电子签名，从而验证 DNS 数据的来源以及传输过程中的完整性，但不对数据包加密，DNS 数据仍然以明文形式传输；而 DNSCurve 使用更高速的椭圆曲线加密算法 Curve25519 以及随机数 nonce 实现 DNS 数据的机密性保护。DNSCurve 加密 DNS 数据包，验证 DNS 应答包，清除伪造的 DNS 数据包，能够加强 DNS 解析的机密性、完整性和可用性。表 1 对两种机制进行对比。

表1 DNSSEC与DNSCurve比较

	加密算法	机密性	完整性	DDos攻击	缓存中毒	部署情况
DNSSEC	RSA	不能提供	能提供	不能抵抗	能抵抗	提出较早，得到ICANN、BIND等国际组织和商业软件的大力支持，已经在多个顶级域上得到了部署
DNSCurve	椭圆曲线加密算法	能有限提供	能提供	部分抵抗	不能抵抗	提出较晚，除OpenDNS外，没有更多部署

根据以上分析比较，二者各有优缺点，虽然DNSCurve中的加密算法效率高于DNSSEC中的RSA，但由于DNSSEC提出较早，后续研究仍在大力开展，其有望成为最有影响并且最有可能得到广泛部署的DNS安全解决方案。未来应用应将两者结合，利用DNSCurve对DNSSEC进行补充，作为辅助机制。

3.2 ONS安全威胁

国内外已有很多学者意识到ONS安全对于EPC网络的重要性，对关于ONS的安全威胁作出了很多研究。郭卫锋等人分析了ONS解析过程中节点身份认证、数据完整性和机密性等方面的安全问题[42]。常见的攻击形式有截获、篡改和伪装。对于缺乏机密性的传输机制，攻击者可能截获ONS解析过程的通信信息，从而得到一些企业的内部机密信息；对于缺乏数据完整性检查，攻击者可能把截获到的信息进行篡改并发送，从而使ONS在解析中出现错误，给企业带来损失；对于缺乏身份认证，攻击者可能利用伪装技术，以虚假的身份进行ONS解析。例如攻击者利用非法手段得到了某产品的EPC编码，并以伪装身份通过合法的ONS系统来解析该EPC编码对应的物品详细信息或者得到进一步的相关服务的地址。ONS需要特别注意隐私保护[43,44]。若ONS解析过程中有关物品信息因缺乏安全机制而被泄露，如竞争对手或别有用心者截获到物品EPC编码的解析结果，获取到物品厂商的内部信息，如产量、利润等商业机密；也有可能被恶作剧者篡改信息，这些都将造成大量的经济损失和纠纷。

结合ONS解析的原理和流程，可以分析出ONS的安全威胁主要存在以下几个方面。

(1)缺乏对解析服务器的认证

缺少对解析服务器的认证，会带来两个方面的威胁：1)难以保证返回结果的真实性，解析结果可能会被链接到垃圾信息等一些非法网站；2)难以保证EPC隐私信息，一旦ONS服务器泄露了EPC编码，用户的隐私信息将会被泄露。

(2)缺乏对解析请求客户端的认证

缺少对解析请求用户的认证，会引起比较常见的服务器攻击方法——拒绝服务(Deny of Services，DOS)攻击：攻击者在很短的时间内使用一台或多台计算机向ONS服务器发出大量请求，如果服务器调用所有资源也无法处理这些请求，就会出现拒绝服务现象。

(3)明文传输

ONS的最后一步解析流程仍然依靠已有的DNS方法，而DNS查询请求的返回结果都是明文，没有采取任何安全机制。明文传输带来两个方面的威胁：1)恶意攻击者可以任意篡改返回结果的内容，实施解析欺骗；2)明文传输使得攻击者可以很容易地实时监听用户访问请求，导致用户隐私的泄露。

4 ONS安全解决方案

针对ONS的安全隐患，许多学者提供了不同的解决方法。文献[45-47]提出基于P2P结构的ONS解决方案，由于P2P结构的解决方案需要改变现存的网络拓扑结构，部署困难，本文不作详细研究。文献[48]从DNS的继承性考虑ONS，比较了常用于解决DNS安全方案的DNSSEC和DNSCurve两种机制，DNSSEC提供了完整性检查和认证机制，DNSCurve提供了保密性和高可用性。由于ONS与DNS类似，将上述两种方案应用于ONS，能在一定程度上改进ONS的安全性，但同时由于ONS的特殊性，不一定能获得理想效果。本节针对ONS的具体解析过程，选取一些较典型的方法进行分类介绍和评述。

4.1 身份认证技术

身份认证是用户在访问系统资源、使用系统服务时，系统确认用户的身份是否真实、合法和唯一的过程。文献[49]将椭圆曲线密码算法运用于ONS本地客户端的身份认证中。客户端将自己的ID嵌入在传输信息中，使用椭圆曲线密码算法进行加密。密钥采用一次一密的方式，且由随机整数产生，以防止中间人攻击。ONS服务器采用域名系统安全扩展(Domain Name System Security Extensions，DNSSEC)机制管理密钥信息，在验证客户端身份时，首先根据客户ID号从后台数据库中查找相应的椭圆曲线函数、加密算法以及公钥等信息；然后对接收到的信息进行解密，若解密成功，则认证通过，否则客户端ID不正确，无法获取相应的密钥，解密不成功，说明用户非法，身份认证不能通过。文献[50]设计了一种可信匿名物联网查询机制。该方案的原理是利用双线性函数及双线性难解问题，在ONS解析中加入匿名认证过程，对本地ONS的身份及平台可信性进行验证，一旦通过认证，便颁发临时证书，在证书的有效期内可多次申请查询服务。该模型必须有可信的第三方平台参与。以上方案均通过密码学技术实现身份认证。文献[51]考虑计算量的问题，在未使用密码算法和第三方平台的情况下，提出了一种轻量级的身份认证方案。该方案的目的在于验证ONS服务器身份的合法性，通过多轮校对的方式认证ONS服务器返回物品信息PML服务器IP地址的可信性。方案中验证集合包含两个元素：(epc,ip)，其中epc为客户端请求解析的物品epc编码；ip为服务器端返回的解析结果。假设MAP_{auth}为包含所有正确解析(epc,ip)映射对的认证列表，文中通过考虑(epc,ip)与集合MAP_{auth}的存在关系推导对应每个epc，服务器返回正确ip的概率，论证的思想基于历史事件诚实发生对后续事件的影响。

在ONS解析中加入身份认证机制，验证服务器端和客户端双方身份，能有效阻止恶意节点的进入，保证ONS解析的安全。针对物联网中用户的隐私保护需求以及节点资源有限的特征，物联网中身份认证技术应采用匿名身份认证机制[52]，并将身份认证带来的通信量和计算量限制到最低。运用可塑性干扰机制解决节点身份认证问题[53]，可以在ONS解析安全中进一步研究。

4.2 数字签名技术

数字签名有两种功效：1)能确定消息确由发送方签名并发送出来，防止交易中抵赖的发生，因为别人无法假冒发送方的签名；2)数字签名能确定消息的完整性，也即消息认证。

文献[42]使用对称密码和消息认证码等技术，提出了一种可证明安全的ONS查询方案。客户端向ONS服务器端发送数据项(ID_c, ID_s, ONS_Req, T_c, MAC_c)，其中ID_c和ID_s分别为客户端和ONS服务器的ID号，ONS_Req为ONS查询请求，用密钥k加密，T_c是客户端产生的一个时间戳，MAC_c是根据ID_c、ID_s、ONS_Req和T_c在密钥k作用下产生的消息认证码。ONS服务器收到信息后，首先检查时间戳T_c是否有效，若时间戳有效，则根据用户身份ID_c查找对应的共享密钥k，使用共享密钥计算消息认证码，比较计算得到的消息认证码值与查询请求中的值是否相等。该方案利用消息认证码验证请求信息的完整性，同时利用共享对称密码实现客户端和服务器端的双向认证。上述方案中消息认证码的产生带来了一定的计算开销。文献[54]提到一种更为简单的数字签名方案。在ONS解析中，类似于DNS，为了提高查询效率，ONS服务器会将成功解析的结果保存为EPC文档，用于记录EPC与EPCIS的对应关系，以备下次查询同样的EPC编码所用。文献[54]为了保护EPC文档的完整性，首先选择SHA-1算法计算出消息摘要，然后将摘要用私钥计算出签名信息后，将签名消息附在EPC文档最后。由于在该方案中由公信机构来签发EPC文档，增强了EPC文档的权威性和不可篡改性，签名方案不需要ONS服务器做任何额外的处理，不会增加其解析压力；而且，一旦ONS服务网络中的任何一个节点解析成功，获取了EPC文档，只要该文档本身没有过期，该节点便拥有了解析此EPC的能力。显然，该方案中EPC文档的可信性由第三方权威机构保证。

在ONS解析中加入数字签名机制，能有效阻止攻击者对ONS解析数据流的篡改，防止用户被链接到垃圾网站。文献[42]中的方案实现数字签名需要花费一定的计算代价；文献[54]中的方案计算代价小，但产生了存储开销，且需要建立在双方都信任第三方权威机构的基础上，存在一定的风险。未来的研究目标为寻找适合物联网的应用及开销小的数字签名机制。

4.3 安全传输技术

为了降低ONS解析过程明文传输带来的威胁，加密机制自然成为首先想到的安全解决方法。加密就是以某种特殊的算法改变原有的信息数据，使得未授权的用户即使获得了已加密的信息，但因不知道解密的方法，仍然无法了解信息的内容。众所周知，加密之所以安全，绝不是因为加解密算法，而是因为密钥的绝对隐藏，攻击者即便取得已加密的数据，并已经获悉加密算法，但若没有加密的密钥，也不能打开被加密保护的信息。文献[55]提出一个物联网安全传输模型，该模型实现了物品信息的秘密传输。在传输过程中，远程物品信息服务器按响应路径中各节点的顺序从后至前用公钥对物品信息嵌套加密，加密后的数据每经过一个路由节点被解密一层，直到到达本地信息服务器时物品信息才被还原成明文，传输过程中每个路由节点可以验证收到数据的完整性及转发路径的真实性。模型中每次查询使用的会话密钥采用一次一密的方式动态生成。同时，在响应路径中该方案的各节点使用填充机制使得通信数据包大小不变，以抵抗流量分析等攻击。

文献[56]提出了一种安全的ONS查询协议，该协议包括两个部分，一部分是利用二代洋葱路由协议抵御窃听和流量攻击，通过在公网中隐藏网络拓扑结构的方法来防止EPC信息的泄露；另一部分是扩展的DNS协议，利用该协议可以解决长途传输中的信任链路问题。文中采用无证书的公钥密码体制，用户由多个密钥生成中心(Key Generation Center, KGC)进行跨域协商会话密钥，控制匿名路由链路的长度，实现本地服务器匿名发送查询信息的目的。

在ONS解析中加入加密算法，将ONS解析数据流加密传输，能有效增强ONS解析的保密性，防止ONS解析数据流被攻击者截获以获取用户隐私信息。ONS解析加密机制的低代价密钥管理问题以及抗流量攻击问题将继续成为下一步重点研究的方向。

5 存在的问题与展望

5.1 当前研究存在的问题

随着物联网应用的兴起，关于ONS安全的研究已经引起越来越多学者的关注，也取得了一定成果，但在理论或者实现方面还存在以下问题：

(1)缺乏统一的安全规定标准。目前，随着物联网应用的兴起，物联网安全引起了国内外很多学者的关注，各项标准也在积极制定中。GS1一直致力于EPC网络的各项标准的制定，包括ONS信息服务中映射信息的管理与查询的标准，但关于ONS解析安全的标准涉及不多，特别地，基于P2P结构的ONS解决方案以及使用基于传统DNS技术的DNSSec和DNSCurve机制目前仍在持续讨论中。

(2)从上面介绍的典型方法可以看出，已有研究大多使用传统安全方案，从密码学角度出发解决ONS安全问题，未能考虑能量消耗问题。但在物联网应用中，由于多种终端的使用，特别是众多嵌入式设备和物品的联网，使得要解决安全问题，必须同时考虑能量和存储等资源消耗问题。

(3)诸多关于ONS安全的研究大多给出理论研究和分析，缺乏方案的实现部分，如数据存储与访问、传输协议等，这些可能会影响到方案的性能和扩展性，从而直接影响到方案在实际中的应用。

(4)上述方案中，认证的实现和密钥的产生大多依赖于第三方可信平台，存在第三方平台被劫持的威胁。

5.2 展望

结合5.1节提出的问题，关于ONS安全机制的研究，未来可以在以下几个方面进一步展开：

(1)加速ONS解析及各项安全规定标准的制定。

(2)探求一些超轻量级的解决方案，以适合资源有限的手持设备中ONS的解析安全。

(3)安全方案实现问题。研究各种安全方案中数据的存储与访问策略、传输协议，以及算法复杂度，以进一步验证方案的可用性。

(4)寻求摆脱第三方的安全方案，尽量减少第三方被劫持攻击的威胁。

结束语 ONS的安全研究目前得到了国内外很多学者的关注。通过在ONS中考虑安全问题，可以加速EPC网络的应用。本文通过比较ONS与DNS的异同，分析了ONS潜在的安全威胁，并将最新ONS安全解决方案按照身份认证技术、数字签名技术和安全传输技术进行归类，探讨了ONS安全中需要进一步研究的问题。然而，物联网相比于传统的网络结构所具有的开放性、自治性和无人值守的特点，决定了其网络安全威胁更大，面临的挑战更为严峻；同时由于物联网设备具有能量有限，计算和存储资源受限的缺点，导致其安全机

制设计受限，无疑加大了物联网安全的解决难度。ONS 的相关安全机制较为复杂，需要研究的问题还有很多。ONS 安全机制的研究对于物联网其他安全领域的研究具有借鉴意义。

参 考 文 献

[1] Presser M, Barnaghi P M, Eurich M, et al. The SENSEI project: Integrating the physical world with the digital world of the network of the future[J]. Global Communications Newsletter, 2009, 47(4): 1-4

[2] Sarma S, Brock D L, Ashton K. The networked physical world [M]// Proposals for engineering the next generation of computing, commerce & automatic-identification. MIT Auto-ID Center, White Paper: MIT-AUTOD-WH-001, 2010

[3] Koshizuka N, Sakamura K. Ubiquitous ID: Standards for ubiquitous computing and the Internet of Things[J]. IEEE Pervasive Computing, 2010, 9(4): 98-101

[4] Zorzi M, Gluhak A, Lange S, et al. From Today's INTRAnet of Things to a Future INTERnet of Things: A wireless and mobility related view[J]. IEEE Wireless Communications, 2010, 17(6): 44-51

[5] Ning Huan-sheng, Xu Qun-yu. Research on Global Internet of Things' Developments and it's Construction in China[J]. Acta Electronica Sinica, 2010, 38(11): 2591-2599(in Chinese)
宁焕生，徐群玉. 全球物联网发展及中国物联网建设若干思考[J]. 电子学报，2010，38(11)：2591-2599

[6] Atzori L, Iera A, Morabito G. The Internet of Things: A survey [J]. Computer Networks, 2010, 54(15): 2787-2805

[7] Shen Su-bin, Fan Qu-li, Zong Ping, et al. Study on the architecture and associated technologies for Internet of Things[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science), 2009, 29(6): 1-11(in Chinese)
沈苏彬，范曲立，宗平，等. 物联网的体系结构与相关技术研究[J]. 南京邮电大学学报(自然科学版)，2009，29(6)：1-11

[8] Sun M, Liu Y A, Liu K M. Security problem analysis and security Mechanism research of the Internet of Things[J]. Secrecy Science and Technology, 2011, 11: 61-66

[9] Medaglia C M, Serbanati A. An overview of privacy and security issues in the Internet of Things[C]// Proceedings of the 20th Tyrrhenian Workshop on Digital Communications. Sardinia, Italy, 2010: 389-394

[10] Yang Guang, Geng Gui-ning, et al. Security threats and measures for the Internet of Things[J]. Journal of Tsinghua University(Science and Technology), 2011, 51(10): 1335-1340(in Chinese)
杨光，耿贵宁，等. 物联网安全威胁与措施[J]. 清华大学学报(自然科学版)，2011，51(10)：1335-1340

[11] Sun Zhi-xin, Luo Bing-qing, et al. Security Model of Internet of Things Based on Hierarchy[J]. Computer Engineering, 2011, 37(10): 1-7(in Chinese)
孙知信，骆冰清，等. 一种基于等级划分的物联网安全模型[J]. 计算机工程，2011，37(10)：1-7

[12] Zhang Bao-quan, Zou Zong-feng, Liu Ming-zheng. Evaluation on Security System of Internet of Things Based on Fuzzy-AHP Method[C]// 2011 International Conference E-Business and E-Government (ICEE). 2011: 1-5

[13] Yang Geng, Xu Jian, et al. Security Characteristic and Technology in the Internet of Things[J]. Journal of Nanjing University of Posts and Telecommunication(Natural Science), 2010, 30(4): 20-29(in Chinese)
杨庚，许建，等. 物联网安全特征与关键技术[J]. 南京邮电大学学报(自然科学版)，2010，30(4)：20-29

[14] Kang Yong-shin, Lee Yong-han. Development of generic RFID traceability services[J]. Computers in Industry, 2013, 64: 609-623

[15] Ning H, Wang Z. Future Internet of Things architecture: Like mankind neural system or social organization framework? [J]. IEEE Communications Letters, 2011, 15(4): 461-463

[16] Wu M, Lu T, Ling F, et al. Research on the architecture of Internet of Things[C]// Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). Chengdu, China, 2010: 484-487

[17] Armen F, Barthel H, Burstein L, et al. The EPCglobal Architecture Framework[M]. EPCglobal, Standard Specification: Final Version 1. 3, 2009

[18] Guinard D, Mueller M, Pasquier-Rocha J. Giving RFID a REST: Building a Web-enabled EPCIS[C]// Proceedings of the 2nd Internet of Things Conference (IOT). Tokyo, Japan, 2010: 1-8

[19] Kang Y, Son K, Lee Y H, et al. A model-based performance study of the EPCglobal network[J]. IE Interfaces, 2011, 24(2): 139-150

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

[21] Kong Ning, Li Xiao-dong, et al. A Model Supporting Any Product Code Standard for the Resource Addressing in the Internet of Things[C]// First International Conference on Intelligent Networks and Intelligent Systems. 2008: 233-238

[22] Yang L, Han J, Qi Y, et al. Season: Shelving interference and joint identification in large-scale RFID systems[C]// Proceedings of the 30th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'11). Shanghai, China, 2011: 3092-3100

[23] Xie Lei, Yin Ya-feng, Chen Xi, et al. RFID Data Management: Algorithms, Protocols and Performance Evaluation[J]. Chinese Journal of Computers, 2013, 36(3): 457-470(in Chinese)
谢磊，殷亚凤，陈曦，等. RFID 数据管理：算法、协议与性能评测[J]. 计算机学报，2013，36(3)：457-470

[24] Evdokimov S, Fabian B, Kunz S, et al. Comparison of discovery service architectures for the Internet of Things[C]// Proceedings of the IEEE International Conference on Sensor Network, Ubiquitous, and Trustworthy Computing (SUTC). Newport Beach, CA, USA, 2010: 237-244

[25] Muller J, Oberst J, Wehrmeyer S, et al. An aggregating discovery service for the EPCglobal network[C]// Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS 2010). Koloa, Hawaii, US, 2010: 1-9

[26] Karakostas B. A DNS Architecture for the Internet of Things: A Case Study in Transport Logistics[C]// The 4th International Conference on Ambient Systems, Networks and Technologies (ANT 2013). Procedia Computer Science, 2013: 594-601

[27] Li Fu-juan. Analysis of ONS Architecture and Security in EPC Internet of Things[J]. Netinfo Security, 2010(12): 6-9(in Chinese)
李馥娟. EPC 物联网中的 ONS 架构及安全分析[J]. 物联网安全研究，2010(12)：6-9

[28] Zhang Li-juan, Wu Zhen-qiang. A Controllable Trusted and AnonymousQuery Mechanism of Internet of Things[J]. Coumputer Technology and Development, 2013, 23(6): 122-125(in Chinese)
张丽娟,吴振强. 一种可控可信匿名的物联网查询机制[J]. 计算机技术与发展,2013,23(6):122-125

[29] Claude F, Elias B-H, Mourad D. Fingerprinting internet DNS amplification DDoS Activities[C]// 2014 6th International Conference on New Technologies, Mobility and Security (NTMS 2014). Dubai, United arab emirates, 2014: 6814019

[30] Li Wei-min, Cao Xiao-guang, Liu Fang, et al. Improving DNS cache to alleviate the impact of DNS DDoS attack[J]. Journal of Networks, 2011, 6(2): 279-286

[31] Dhananjay P, Sherman A T, Nikhil J, et al. Spread identity: A new dynamic address remapping mechanism for anonymity and DDoS defense[J]. Journal of Computer Security, 2013, 21(2): 233-281

[32] Wang Yao, Hu Ming-zeng, Li Bin, et al. Servey on domain name system security[J]. Journal on Communication, 2007, 28(9): 91-103(in Chinese)
王垚,胡铭曾,李斌,等. 域名系统安全研究综述[J]. 通信学报,2007,28(9):91-103

[33] Mockapetris P V. Domain Names: Concepts and Facilities[OL]. http://www.ietf.ogr/rfc/rfc1035.txt. 2015

[34] Mockapetris P V. Domain Names: Implementation and Specification[OL]. http://www.ietf.ogr/rfc/rfc1035.txt. 2015

[35] Jung J, Sit E, Balakrishnan H, et al. DNS performance and effectiveness of caching[J]. IEEE/ACM Transactions on Networking, 2002, 10(5): 589-603

[36] Wijingaards W C, Overeinder B J. Securing DNS: Extending DNS servers with a DNSSEC validator[J]. Security & Privacy, 2009, 7(5): 36-43

[37] Ariyapperuma S, Mitchell P C J. Security vulnerabilities in DNS and DNSSEC[C]// Proceedings of the Second International Conference on Avaliability, Reliability and Security. 2007: 335-342

[38] Dempsky M. DNSCurve: Link-Level Security for the Domain Name System[Z]. Internet-Draft draft-dempsky-dnscurve-11, IETF Secretariat, 2010

[39] Wander M, Weis T. Measuring occurrence of DNSSec validation [C]// Proceedings of the 14th International Conference on Passive and Active Measurement. Hong Kong, China, 2013: 125-134

[40] Wang Yong, Yun Xiao-chun, Yao Yao, et al. Traffic Measurement Based DNSSEC Analysis[C]// Proceedings of the 2012 IEEE 12th International Conference on Computer and Information Technology. 2012: 62-69

[41] Lian W, Rescorla E, Shacham H, et al. Measuring the practical impact of DNSSEC deployment[C]// Proceedings of the 22nd USENIX conference on Security. Washington, D C, 2013: 573-588

[42] Guo Wei-feng, Li Jing-feng, Zhang Lai-shun. New Provably Secure ONS Enquiry Scheme in EPC Network[J]. Journal of Chinese Computer Systems, 2013, 34(7): 1620-1624(in Chinese)
郭卫锋,李景峰,张来顺. EPC 网络中一种可证明安全的 ONS 查询方案小型[J]. 微型计算机系统,2013,34(7):1620-1624

[43] Schapranow M, Zeier A, Leupold F, et al. Securing EPCglobal object name service-privacy enhancements for anti-counterfeiting [C]// 2011 Second International Conference on Intelligent System, Modeling and Simulation. 2011: 332-337

[44] Weber R H. Internet of things-new security and privacy challenges[J]. Computer Law & Security Review, 2010, 26(1): 23-30

[45] Fabian B. Implementing secure p2p-ons [C]// Proceedings of IEEE International Conference on Communications (ICC'09). 2009: 1-5

[46] Li Zhan-bo, Zhang Zhe. New ONS resolution mechanism based on DHT-P2P [J]. Computer Engineering and Applicaions, 2013, 49(3): 91-95(in Chinese)
李占波,张哲. 基于 DHT-P2P 新型的 ONS 解析机制[J]. 计算机工程与应用,2013,49(3):91-95

[47] Luo Wei-min, Xiong Jiang, et al. Object Naming Service Model Based on Two-layer P2P Strucutre in Internet of Things[J]. Computer Engineering, 2012, 38(12): 79-85(in Chinese)
罗卫敏,熊江,等. 物联网中基于两层 P2P 结构的 ONS 模型[J]. 计算机工程,2012,38(12):79-85

[48] Rosenkranz D, Dreyer M, Schmitz P, et al. Comparison of dnssec and dnscurve securing the object name service (ons) of the epc architecture framework [C] // Proceedings of the European Workshop on Smart Objects: Systems, Technologies and Applications(RFID Sys Tech'10). 2010: 1-6

[49] OU Ruo-feng, Wen Chao, et al. One design of solving the problem of the Internet of Things safety and efficiency based on the elliptic curve encryption algorithm[J]. Microcomputer Applications, 2011, 27(3): 14-17(in Chinese)
欧若风,文超,等. 一种基于椭圆曲线加密算法解决物联网网络安全和效率问题的设计[J]. 微型电脑应用,2011,27(3):14-17

[50] Zhou Yan-wei, Wu Zhen-qiang. TA-ONS—New enquiry system of Internet of Things[J]. Journal of Computer Application, 2010, 30(8): 2202-2206(in Chinese)
周彦伟,吴振强. TA-ONS—新型的物联网查询机制[J]. 计算机应用,2010,30(8):2202-2206

[51] Ren Wei, Ma Liang, Ren Yi. APP: An ultralightweight scheme to authenticate ONS and protect EPC privacy without cryptography in EPCgloabl networks[J]. International Journal of Distribute Sensor Networks, 2013(7)

[52] Han H, Sheng B, Tan C C, et al. Counting RFID tags efficiently and anonymously[C]// Proceedings of the 29th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'10). San Diego, USA, 2010: 1028-1036

[53] Wu Ding-ming, Chao Dong, Tang Shao-jie, et al. Fast and Fine-grained Counting and Identification via Constructive Interference in WSNs[C]// Proceedings of the 13th International Symposium on Information Processing in Sensor Networks. Berlin, 2014: 191-202

[54] Li Yang. Research of Object Name Service and its Security[D]. Hefei: Hefei University of Technology, 2012(in Chinese)
李杨. 物联网 ONS 解析技术及其安全研究[D]. 合肥:合肥工业大学,2012

[55] Wu Zhen-qiang, Zhou Yan-wei, Ma Jian-feng. A Security Transmission Model for Internet of Things[J]. Chinese Journal of Computers, 2011, 34(8): 1351-1364(in Chinese)
吴振强,周彦伟,马建峰. 物联网安全传输模型[J]. 计算机学报,2011,34(8):1351-1364

[56] Li Zhong-wen, Xie Yi, et al. A security query protocol of ONS in EPC system[C]// 2012 International Conference on Anti-Counterfeiting, Security and Identification(ASID 2012). 2012