

# 一种可控可信匿名的物联网查询机制

张丽娟, 吴振强

(陕西师范大学 计算机科学学院, 陕西 西安 710062)

**摘要:**近年来,物联网发展迅猛并得到广泛应用,在商品物流中的应用尤为突出。但其在传输的安全性及隐私的保护性方面存在不足,一定程度上限制了物联网的发展。文章基于 ECC 中的双线性函数和可信计算提出了一种可控可信匿名的物联网 ONS 查询机制(CTA-ONS),并且设计了 ONS 查询服务的安全协议。CTA-ONS 在传统物联网 ONS 查询中加入可信以及匿名认证的过程,实现了只对授权可信的 L-ONS 提供查询服务,避免了证书查询机制中 L-ONS 证书有效期内受到攻击或被恶意节点控制而遭受网络地址的重放、篡改和窃听,加入对 R-ONS 的可信验证保证了 R-ONS 的安全可信,从而为查询提供合法可信的网络地址。分析表明该模型具有匿名性、安全性、可控性和可信性等特点。

**关键词:**ONS;匿名认证;可信计算;双线性

**中图分类号:**TP309

**文献标识码:**A

**文章编号:**1673-629X(2013)06-0122-04

**doi:**10.3969/j.issn.1673-629X.2013.06.031

## A Controllable Trusted and Anonymous Query Mechanism of Internet of Things

ZHANG Li-juan, WU Zhen-qiang

(College of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

**Abstract:** In recent years, Internet of Things is developing rapidly and widely used, especially in the commodity logistics. But the development of Internet of Things was restricted due to the insufficiency of privacy protection and security transmission. So proposed an enquiry mechanism of IOT, Controllable Trusted Anonymous Object Naming Service (CTA-ONS) with trusted computing technology and bilinear function in ECC. It designed a security architecture and security protocols in the ONS query mechanism and added reliable and anonymous authentication process. CTA-ONS, only provided enquiry services to authorized L-ONS, avoided L-ONS controlled by malicious node which made network address subject to replay, tampering and eavesdropping within the validity period of certificate in the L-ONS query mechanism. In addition, it prevented R-ONS from taking attack and providing illegal network address by adding reliable authentication. The analysis shows that this model is safe, anonymous, trusted and controllable.

**Key words:** ONS; anonymous authentication; trusted computing; bilinear function

### 1 概述

物联网(Internet of Things, IoT)是把射频识别等传感器嵌入到公路、铁路、大坝以及家用电器等实物上,通过现有网络连接起来运行相关程序,实现物理世界与人类社会的融合以及物物之间的直接通信和信息交换;它具有非常广泛的应用前景,成为当前人们研究的热点。麻省理工大学在1999年创办了Auto-ID Center,开始研究和开发自动识别技术,并将因特网和RFID结合提出了产品电子代码(Electronic Product

Code, EPC)的概念<sup>[1]</sup>。国际物品编码协会与美国统一代码委员会将全球统一标识编码体系应用到EPC概念中,并将EPC纳入到全球统一标识系统。在物联网中使用EPC,就是为各物品分配唯一的编码,并存储在表面的标签上,把编码所对应的物品的详细信息存在物品信息服务器(Information Server of Things, TIS)中<sup>[2]</sup>。因此,在生产线到流向市场的整个过程中,均可以跟踪到物品。另外,可利用物联网的ONS查询机制查询TIS中记录的物品资源标识URI,从而通过因特网查询物品的详细信息,对物品进行深入了解、管理、

收稿日期:2012-09-06

修回日期:2012-12-10

网络出版时间:2013-03-05

基金项目:国家自然科学基金面上项目(61173190);国家“863”高技术发展计划项目(2007AA01Z438200)

作者简介:张丽娟(1988-),女,甘肃张掖人,硕士研究生,研究方向为匿名通信技术、可信计算;吴振强,博士,教授,博士生导师,研究方向为匿名通信技术、可信计算、普适计算等。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20130305.0815.015.html>

监控和跟踪等<sup>[3]</sup>。

然而,物联网中的实体均具有一定的感知、执行和计算能力,传感器等的广泛存在会对国家基础设施相关信息、个人私密信息等的安全构成威胁。一方面,国家电网、个人病例接入到物联网时,通过定位便可追踪用户的行踪,使得个人隐私在不知情的情况下被非法获取<sup>[4]</sup>;另一方面,社会上一些关键服务领域(如医疗等)和国家的重要行业都依靠感知业务以及物联网,国家基础设施领域的数据可能被窃取<sup>[5]</sup>。另外,RFID系统最大的特点是读取速度快,通过对物品信息的监控和定位可以跟踪企业销售状况,造成企业商业机密的泄露<sup>[6]</sup>。传统物联网 ONS 查询中,本地物品信息服务器与远程物品信息服务器在传输物品详细信息时可能会遭受嗅探、窃听以及流量分析等网络攻击,使详细信息传输的过程存在安全隐患<sup>[7]</sup>。与传统网络比较,物联网中的感知节点大都部署在无人监控的环境,资源相对受限,并且涉及面极广,冲破了传统的安全边界,使得一些传统的安全防御和保护措施不可用,无法为物联网提供安全可靠的保障,从而使物联网的安全问题变得特殊。分析得出物联网在隐私保护上不足的原因如下:物联网物品信息查询机制为 L-ONS 提供无限制查询功能并且假设 R-ONS 是安全可信的。而在实际的查询机制中 R-ONS 并非安全可信,一旦处于不安全状态它很可能提供非法的物品信息网络地址。由此,只有确保 L-ONS 的安全可信才能够满足一些如政府、银行等安全性高的机构的相关信息查询,同时保障 R-ONS 的安全可信才可以提供合法可信的物品信息网络地址。

针对物联网 ONS 查询机制中物品信息传输的安全性以及隐私保护的问题,文献[8]利用签名等技术提出了一种商品信息查询的防伪机制。文献[7]指出物联网中的物流要从容忍攻击方面研究,以解决服务器和客户端的隐私保护、数据认证、单点故障等问题,同时进行适当的风险管理。文献[9]就物联网信息查询机制中网络加密协议的低效以及安全威胁等问题,设计了一种椭圆曲线加密算法(ECC)解决 EPCglobal 网络安全的协议。但协议的运行效率低,影响庞大的物联网中 ONS 查询效率。文献[10]提出了一种新型物联网 ONS 查询机制,在 ONS 查询机制中通过证书对 L-ONS 进行认证,但在证书的有效期内,L-ONS 可能被攻击者控制,使查询到的物品信息网络地址遭到攻击者的窃取或修改。

文中提出的 CTA-ONS 在传统物联网 ONS 查询中加入匿名认证的过程,进行远程物品信息查询时,不仅实施对 L-ONS 的身份合法性以及平台可信性进行可信验证,而且在此前提下引入对 R-ONS 的可信验

证。CTA-ONS 只对授权可信的 L-ONS 提供安全高效的查询服务,同时只有安全可信的 R-ONS 才能加入查询系统提供网络地址。CTA-ONS 一方面避免了 R-ONS 返回非法资源地址,提高了查询的安全性;另一方面防止了非法 L-ONS 查询物品信息,避免了证书查询机制中 L-ONS 在证书有效期内受到攻击而遭受网络地址的重放、篡改和窃听等。

## 2 可控可信匿名的物联网查询机制

为了排除 R-ONS 本身以及 L-ONS 在证书有效期内存在的不安全因素,保证物联网中服务信息的安全,文中提出了一种基于可信计算技术和双线性对签名方法的 ONS 查询机制——CTA-ONS 查询机制。在该机制中,不再以证书作为安全性认证的唯一凭证,L-ONS 向 R-ONS 请求查询服务之前,TAS 对 L-ONS 进行安全性和完整性验证,验证成功后还要对 R-ONS 进行安全性和完整性验证,成功后 R-ONS 发送所要查询的物品资源地址。

### 2.1 机制的初始化

$G_1$  是阶为大素数  $p$  的加法群, $G_2$  是阶为大素数  $q$  的乘法群。设  $e$  为  $G_1 \times G_2$  到  $G_2$  的双线性对,通过 ECC 理论选取产生。另外选择  $H$  是单向安全的哈希函数  $\{0,1\}^* \rightarrow G_1$ 。参数由 TAS 选取并通过安全渠道公开。

### 2.2 CTA-ONS 查询过程

CTA-ONS 机制中加入 TAS 对 L-ONS、R-ONS 平台真实性以及完整性的检验。图 1 为查询机制的流程图。在本系统中 L-ONS 和 R-ONS 地位对等。

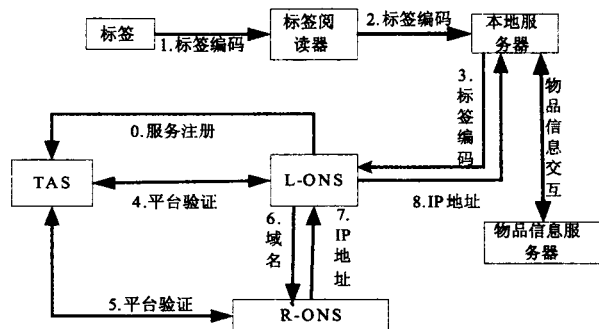


图 1 CTA-ONS 查询流程图

1) L-ONS 首次加入物联网 ONS 系统时先进行服务注册,注册过程中 TAS 对 L-ONS 的身份合法性及平台可信性进行验证。注册完成后获得由 TAS 产生的身份标识 ID,TAS 中多了一条有关 L-ONS 的记录;

2) RFID 阅读器从标签上识读一个比特字符串 EPC 编码(二进制格式表示);

3) 阅读器把读到的编码发给本地代理软件;

4) 经过排队、筛选以及对编码的格式变换,本地

服务器将最终的 URI 编码格式信息发给 L-ONS;

5) L-ONS 服务器把 URI 转换成 DNS 域名格式后基于 DNS 域名访问本地的 ONS 服务器(缓存 ONS 记录信息),如发现其相关 ONS 记录,直接返回 DNS 记录,即要查询信息的网络地址;否则触发安全性及完整性收集设备收集本地平台信息并将其与注册时的身份标识 ID 发送给 TAS, TAS 根据 L-ONS 注册时的状态以及特定的安全策略对 L-ONS 的平台安全性及完整性信息进行验证,验证成功后向 L-ONS 发送一个等待特定时间后进行 ONS 查询以及临时身份 TID 的消息。此时 TAS 向 R-ONS 发送授权查询信息, R-ONS 收集本机安全性和完整性信息并发送给 TAS, 平台验证成功后 TAS 向 R-ONS 发送 L-ONS 此次查询的临时身份标识 TID 以及验证标识。R-ONS 等待 L-ONS 的查询, 查询时验证完 L-ONS 的身份后向其发送所要查询的物品信息网络地址;

6) 本地 ONS 将从 R-ONS 查询到的网络地址返回给本地服务器;

7) 本地服务器再将此网络地址返回, 获取所需的 EPC 信息。

机制执行过程分为两步, 注册和查询。其中查询服务又包含 L-ONS、R-ONS 平台验证和查询服务两个阶段。

首先做以下假设: 认证协议执行过程中, CA 向 TAS 签署了证书且公钥经过安全渠道公布; 可信计算的核心 TPM 进行协议中所有的加解密等运算; L-ONS、R-ONS 及 TAS 间有时钟同步机制确保本机制消息时戳的新鲜性。

### 2.2.1 L-ONS 的注册

(1) L-ONS 发出注册请求;

(2) TAS 依据文献[11]中的策略验证 L-ONS 平台的可信性, 为身份合法且平台可信的 L-ONS 分配唯一的身份标识号  $ID_{L-ONS}$ , 并且将这次的完整性信息作为以后验证的依据进行存储。由式(1)计算产生秘密数  $S_{L-ONS}$ , 即:

$$S_{L-ONS} = H(ID_{L-ONS} || N_{TAS}) \quad (1)$$

TPM 根据需要随机产生了大数  $N_{TAS}$ 。  $TID_{L-ONS} = ID_{L-ONS} + S_{L-ONS} + ID_{TAS}$  用来建立临时身份。

TAS 为 L-ONS 建立账户  $\langle ID_{L-ONS}, S_{L-ONS}, TID_{L-ONS}, Num_{TAS} \rangle$ , 并且由 L-ONS 来存放  $S_{L-ONS}$  和  $ID_{L-ONS}$  [12]。

### 2.2.2 请求查询

L-ONS 注册完成便可以发出查询请求, 查询有关物品的资源地址。图 2 为查询流程:

(1) L-ONS 调用可信平台读出 PCR 值, 生成随机数  $X_0 \in [1, q-1]$ , 对  $s = E(KS_{L-ONS}, X_0 || PCR)$  签名, 导出日志 SML, 利用  $key = H(S_{L-ONS})$  求得临时会话密钥。

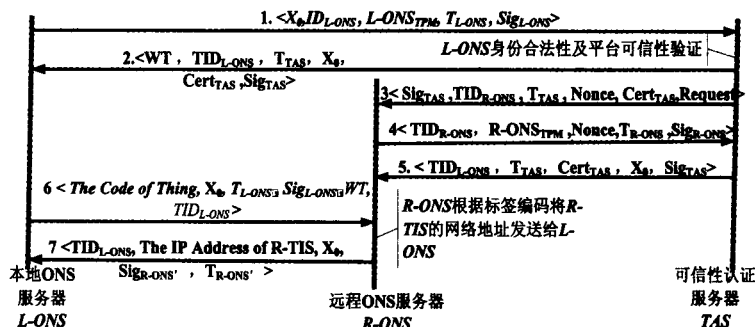


图 2 L-ONS 向 R-ONS 发起 ONS 查询服务

L-ONS 整理并计算出完整性信息  $L-ONS_{TPM} = E(key, SML || s)$ , 将  $ID_{L-ONS}, L-ONS_{TPM}, X_0$  及时戳  $T_{L-ONS}$  连同签名信息  $Sig_{L-ONS}$  一起发给 TAS, 其中  $Sig_{L-ONS} = H(KS_{L-ONS}, L-ONS_{TPM} || ID_{L-ONS} || T_{L-ONS})$ 。

(2) 为了避免出现重放攻击, TAS 验证 L-ONS 签名的真实性、身份的合法性及时戳的有效性。如果验证失败, 不能提供服务, 查询结束, 否则为其分配临时身份  $TID_{L-ONS}$  生成消息签名。  $Sig_{TAS} = H(WT || TID_{L-ONS} || T_{TAS} || X_0 || Cert_{TAS})$ 。

TAS 发送消息  $WT, TID_{L-ONS}, T_{TAS}, X_0, Cert_{TAS}$  及  $Sig_{TAS}$  给 L-ONS。 WT 为 L-ONS 需要等待的特定时间, 等待 WT 时间后 L-ONS 向 R-ONS 发起查询。

(3) TAS 向 R-ONS 发送授权验证消息, 请求对 R-ONS 平台完整性和安全性进行验证。授权消息为  $sig_{TAS} = H(TID_{R-ONS} || T_{TAS} || Nonce || Cert_{TAS} || Request)$ 。

(4) R-ONS 首先验证  $Cert_{TAS}$  是否真实以及时戳是否有效, 如果验证失败, 查询结束。验证成功则 R-ONS 调用可信平台读出 PCR 值, 生成随机数  $X_1 \in [1, q-1]$ , 对  $s' = E(KS_{R-ONS}, X_1 || PCR)$  签名, 导出日志 SML, 求得  $Key' = H(S_{R-ONS})$ 。

R-ONS 生成自身的完整性度量信息  $R-ONS_{TPM} = E(key, s' || SML)$  后, 将  $TID_{R-ONS}, R-ONS_{TPM}$ 、随机数 Nonce 及时戳  $T_{R-ONS}$  连同签名信息  $Sig_{R-ONS}$  一起发给 TAS, 其中  $Sig_{R-ONS} = H(KS_{R-ONS} || TID_{R-ONS} || R-ONS_{TPM} || T_{R-ONS} || Nonce)$ 。

(5) TAS 收到 R-ONS 的平台安全性信息和完整性信息后, 验证 R-ONS 签名的真实性、身份的合法性及时戳的有效性, 以防范重放攻击, 若验证无效, 则查询服务终止, 否则并生成消息签名  $Sig_{TAS} = H(TID_{L-ONS} || T_{TAS} || Cert_{TAS} || X_0)$ 。

TAS 发送消息  $TID_{L-ONS}, T_{TAS}, Cert_{TAS}$  与 L-ONS 通

信时的随机数  $X_0$  及  $\text{Sig}_{\text{TAS}}$  给 R-ONS。

(6) L-ONS 时机成熟之后将标签身份及编码、时戳、与 TAS 通信时的随机数、要求等待的时间和签名信息发给 R-ONS。  $\text{Sig}_{\text{L-ONS}} = H(\text{WT} || \text{TID}_{\text{L-ONS}} || T_{\text{L-ONS}} || X_0 || \text{The code of Thing})$ 。

(7) R-ONS 首先验证 L-ONS 的身份是否合法, 验证成功后搜索出(6)中 The code of Thing 所对应的 TIS 的 IP 地址, 产生时戳  $T_{\text{R-ONS}}$ , 生成消息签名, 发给 L-ONS。  $\text{Sig}_{\text{R-ONS}} = H(\text{TID}_{\text{L-ONS}} || T_{\text{R-ONS}} || X_0 || \text{IP Address})$ 。

L-ONS 将网络地址返回便可与远程物品信息服务器进行交互, 查询结束。

### 3 CTA-ONS 查询机制分析

#### 3.1 可控性和安全性分析

可控可信匿名的 ONS 机制中,  $G_1, G_2$  的选择都是基于难解的离散对数问题, 实现了安全的认证。另外, 求出临时密钥, 可以保证 key 是不能伪造的, 时戳的引入确保消息的新鲜性。同样的方法, 也保证了 R-ONS 的安全性。

L-ONS 申请查询时, TAS 检查时戳是否新鲜、平台是否可信及身份是否合法, 另外, 引入哈希函数确保了消息是完整的, 而时戳的引入也能保证消息不会被重放。同时, 机制避免了文献[8]中 L-ONS 证书有效期内遭受攻击或被恶意节点控制而破坏查询系统。验证了 L-ONS 平台的安全性和可信性之后, TAS 要用同样的方法验证 R-ONS 的平台可信性、完整性和安全性。在 R-ONS 安全可信的基础上, L-ONS 持相关证明信息向 R-ONS 发出查询, 避免了 R-ONS 被恶意节点攻击或控制而发送非法网络地址, 防止了整个查询机制因 R-ONS 被攻破而瘫痪, 保证了整个查询机制处在可控和安全的状态。

机制中, L-ONS 和 R-ONS 只要发起查询就会对其身份及平台进行验证, 而且每次产生的 key 都不相同。因此, 一次一密的实现更加提高了机制的安全性。

#### 3.2 可信性分析

查询过程中, L-ONS 的相关平台信息均由 TAS 保存, 实现了两方面的功能: 验证 L-ONS 的平台是否可信; 确保配置信息的安全性和隐私性, 避免泄露。其中任何两方的消息传递都需要经过 key 加密, key 的安全存储确保了 R-ONS 根据收到的消息推算出 L-ONS 的真实身份。

发起查询时, L-ONS 调用可信计算核心部件 TPM 进行自身平台的度量, 根据相关策略由下而上形成可信链, 并将自身平台的完整性信息发给 TAS, 经 TAS 验证成功后方可进行后续查询步骤。

同样, R-ONS 也如此, 通过向 TAS 提供签名后的平台 PCR 完整性信息和度量日志等, 保证了 R-ONS 平台的可信性。

#### 3.3 匿名性分析

通信消息中均未出现 L-ONS 的真实身份即有关可信平台的唯一背书密钥, 也没有出现注册时分配的主身份标识。在查询过程中, 只有拥有秘密数的 TAS 可以利用计算公式得到其真实身份, 而任何时候发起查询方总是以  $\text{TID}_{\text{L-ONS}}$  出现, 这个身份是临时的, 实现了查询的匿名性。

另外, L-ONS 的  $\text{TID}_{\text{L-ONS}}$  不会重复, 而且任何一个 L-ONS 只知道自己的  $\text{TID}_{\text{L-ONS}}$ , 对其他 L-ONS 的  $\text{TID}_{\text{L-ONS}}$  并不知情, 故具有不可跟踪性以及不可伪造性。

#### 3.4 效率分析

在 CTA-ONS 查询机制中, 加解密等复杂运算均通过可信计算的核心部件 TPM 操作, 只消耗极少一部分 CPU 资源。因此, 将 ONS 与可信计算技术结合, 提高了查询速度和效率。CTA-ONS 查询机制中, 在基本不增加线路吞吐量和 TAS 流量负载的情况下采用了一次注册次次验证的方法, 有效地增强了整个查询过程的实时安全性, 保证查询生命周期是可控可信的。在查询中, TAS 验证了 L-ONS 本地平台的安全性和可信性之后, 根据自身处理能力和实时负载动态决定 L-ONS 需要等待的时间, 有效地调节了 TAS 的通信量, 避免了系统瓶颈的发生, 在此机制中避免了使用证书认证时可能出现的证书有效期决定困难等问题, 不分发证书也节省了巨大的系统开支。综上, CTA-ONS 查询机制总体上提高了查询效率, 具有动态调控系统处理流量负载的能力。

### 4 结束语

文中综合分析了传统物联网在隐私保护与安全传输方面的缺陷, 在研究传统物联网 ONS 查询机制的基础上, 基于可信计算技术提出了一种改进的物联网查询机制, 机制中加入了 L-ONS 的可信和匿名认证, 防止非授权的 L-ONS 查询物品信息的流动, 同时对 R-ONS 的可信性和安全性进行验证, 防止了 R-ONS 自身的安全性问题而造成系统的不正常运行。分析表明 CTA-ONS 查询机制具有安全性、匿名性和可信性等特点。

#### 参考文献:

- [1] 刘宴兵, 胡文平. 物联网安全模型及关键技术[J]. 数字通信, 2010(8): 28-33.

(下转第 128 页)

得注意的是如何编写高效并且松耦合的程序来识别真签名数据和假签名数据。

### (3) 数据存储。

MapReduce 将真实的数据解析后保存到 CSC 指定的数据存储空间中以便以后分析使用<sup>[13]</sup>。

### (4) 数据分析。

CSC 的数据分析器与数据代理共享着相同的密钥, CSC 数据分析器通过密钥与数字签名仔细从结果中过滤掉假数据。

图 2 为具有虚假数据的 CSC 架构。

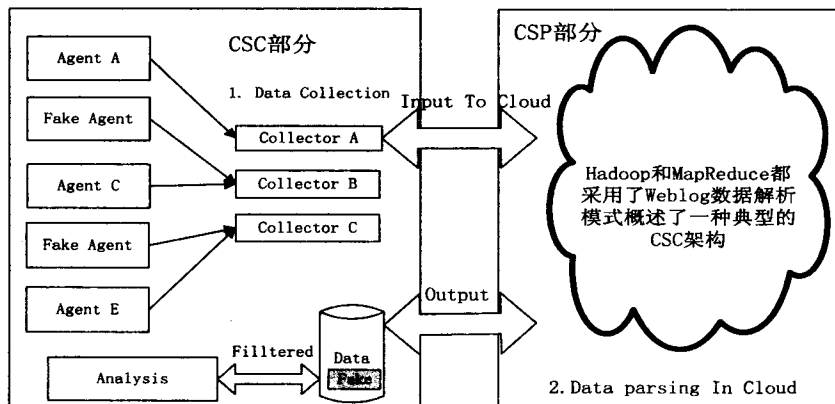


图 2 具有虚假数据的 CSC 架构

任何 CSP 的外部攻击者,或者不受信任的 CSP 本身由于缺乏密钥还不能将密集型任务解析成真实的数据。

## 3 结束语

值得注意的是,可以通过 CSC 所需的保密程度来逐步添加虚假数据的信息量,因此日志分析是一个密集型任务而不是分析假日志。

可以通过进一步分析这一技术来适用于其他云服务模型,如 SaaS 和 PaaS。

## 参考文献:


- [1] Rivest R. Chaffing and Winnowing Confidentiality without Encryption. [EB/OL]. 1998. <http://www.doc.ic.ac.uk/~mrh/430/04.PublicKeyDigitalSig.ppt.pdf>.
- [2] Bellare M, Boldyreva A. The Security of Chaffing and Winnowing[EB/OL]. [2000-11-22]. <http://charlotte.ucsd.edu/~mihir/papers/cw.pdf>.
- [3] Mather T, Kumaraswamy S, Latif S. 云计算安全与隐私[M]. 中文版. 刘戈舟, 杨泽明, 刘宝旭, 译. 北京: 机械工业出版社, 2012.
- [4] 邓倩妮, 陈全. 云计算及其关键技术[J]. 计算机应用, 2009, 29(9): 2562-2568.
- [5] 陈康, 郑伟民. 云计算: 系统实例与研究现状[J]. 软件学报, 2009, 20(5): 1337-1348.
- [6] 王德政, 申山宏, 周宁宁. 云计算环境下的数据存储[J]. 计算机技术与发展, 2011, 21(4): 81-84.
- [7] 李成华, 张新访, 金海, 等. MapReduce: 新型的分布式并行计算编程模型[J]. 计算机工程与科学, 2011, 33(3): 129-135.
- [8] 周锋, 李旭伟. 一种改进的 MapReduce 并行编程模型[J]. 科协论坛, 2009(2): 65-67.
- [9] Apache Flume[EB/OL]. 2012-07-26. <http://flume.apache.org/>.
- [10] Facebook's Scribe[EB/OL]. 2011-12-13. <http://www.cnblogs.com/brucewoo/archive/2011/12/13/2285482.html>.
- [11] Apache Hadoop[EB/OL]. 2012-03-16. [http://en.wikipedia.org/wiki/Apache\\_Hadoop](http://en.wikipedia.org/wiki/Apache_Hadoop).
- [12] 怀特. Hadoop 权威指南[M]. 中文版. 周傲英, 曾大聃, 译. 北京: 清华大学出版社, 2010.
- [13] 杨代庆, 张智雄. 基于 Hadoop 的海量共现矩阵生成方法[J]. 现代图书情报技术, 2009, 25(4): 23-26.

(上接第 125 页)

- [2] 曾炼成, 傅卓军, 沈岳. 超高频 RFID 标签可重用仓储管理系统的设计[J]. 计算机技术与发展, 2011, 21(9): 153-155.
- [3] Liu F L, Ning H S, Yang H P, et al. RFID-based EPC System and Information Services in Intelligent Transportation System [C]//The 6th International Conference on ITS Telecommunications Proceedings. Chengdu: IEEE Press, 2006: 26-28.
- [4] 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. Berlin, Germany: Springer-Verlag, 2010: 389-394.
- [5] 刘宴兵, 胡文平, 杜江. 基于物联网的网络信息安全体系[J]. 中兴通讯技术, 2012, 22(5): 233-236.
- [6] Atzori L, Iera A, Morabito G. The Internet of Things: A Survey

- [J]. Computer Networks, 2010, 54(1): 2787-2805.
- [7] Weber R H. Internet of things-New security and privacy challenges[J]. Computer Law & Security Review, 2010, 26(1): 23-30.
- [8] 芦佳, 卫强, 陈兵. 基于 RFID 技术的防伪平台的设计与实现[J]. 计算机技术与发展, 2012, 22(5): 233-236.
- [9] 欧若风, 文超, 陈睿, 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.
- [10] 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.
- [11] 吴振强, 周彦伟, 乔子芮. 一种可控可信的匿名通信方案[J]. 计算机学报, 2010, 33(9): 1686-1702.
- [12] 杨力, 马建峰, 朱建明. 可信的匿名无线认证协议[J]. 通信学报, 2009, 30(9): 29-35.

# 一种可控可信匿名的物联网查询机制

作者：[张丽娟](#)，[吴振强](#)，[ZHANG Li-juan](#)，[WU Zhen-qiang](#)  
作者单位：[陕西师范大学计算机科学学院, 陕西西安, 710062](#)  
刊名：[计算机技术与发展](#)  
英文刊名：[Computer Technology and Development](#)  
年，卷(期)：2013, 23(6)

本文链接：[http://d.g.wanfangdata.com.cn/Periodical\\_wjfz201306031.aspx](http://d.g.wanfangdata.com.cn/Periodical_wjfz201306031.aspx)