物联网安全传输模型

吴振强[1)] 周彦伟[2)] 马建峰[3)]

[1)](陕西师范大学计算机科学学院 西安 710062)

[2)](陕西师范大学教师专业能力发展中心 西安 710062)

[3)](西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

摘 要 物联网的安全与隐私对参与方有着较大的影响,需要建立相应的安全框架实现数据保密、访问控制、客户端隐私保护等功能以抵抗复杂攻击.论文利用可信计算技术和双线性对的签密方法提出了一个物联网安全传输模型,满足了物联网的 ONS 查询及物品信息传输两个环节的安全需求.模型包括了 EPC 物联网中 ONS 查询服务的安全体系及相应的安全协议,ONS 根服务机构利用可信认证服务器对申请查询的本地 ONS 服务器(L-ONS)的合法身份及平台可信性进行验证,对通过验证的 L-ONS 签发临时证书,在证书有效时间内 L-ONS 可持证书多次申请查询服务.安全 ONS 查询服务实现了匿名认证功能,仅对授权且可信的 L-ONS 提供查询服务,阻止了非法 ONS 查询物品信息;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.分析表明,新的传输模型具有安全性、匿名性、可信性和抗攻击性等特点.

关键词 物联网;ONS 查询;可信计算;匿名认证;匿名传输

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2011.01351

A Security Transmission Model for Internet of Things

WU Zhen-Qiang[1)] ZHOU Yan-Wei[2)] MA Jian-Feng[3)]

[1)](*School of Computer Science, Shaanxi Normal University, Xi'an* 710062)

[2)](*Center for Teacher Professional Ability Development, Shaanxi Normal University, Xi'an* 710062)

[3)](*Key laboratory of Computer Network and Information Security of Ministry of Education, Xidian University, Xi'an* 710071)

Abstract The security and privacy of the Internet of Things has an impact on the involved stakeholders. Measures ensuring the architecture's resilience to attacks, data confidentiality, access control and client privacy need to be established. A novel transmission model of IoT is proposed with trusted computing technology. And signcryption schemes from bilinear pairings, which realizes the security requirement of IoT in ONS query and object information transmission. A security architecture and security protocols in the EPC ONS query system have been designed in this model. Root-ONS can authenticate the identities and platform creditability of local ONS servers (L-ONS) by trusted authentication server (TAS), and the TAS give a temporary certificate to validated L-ONS who can apply for enquiry services many times with the certificate in the validated time. A security ONS query service with anonymous authentication provides only to those authorized and trusted L-ONS, which prevents the illegal ONS to enquire information of things. In the transmission process, Remote Information Server of Things(R-TIS) wraps the information of

收稿日期:2011-03-29;最终修改稿收到日期:2011-06-29.本课题得到国家"八六三"高技术研究发展计划项目基金(2007AA01Z438200)、国家自然科学基金重点项目(60633020)资助.**吴振强**,男,1968 年生,博士,副教授,研究方向为匿名通信技术、可信计算、普适计算等.E-mail: zqiangwu@snnu.edu.cn. **周彦伟**,男,1986 年生,硕士,助理工程师,研究兴趣为匿名通信技术、可信计算. **马建峰**,男,1965 年生,博士,教授,博士生导师,研究领域为信息安全、密码学等.

things into multiple encryption layers with the routing node's public key according the order of responded nodes from the end to the start. The encryption data is decrypted the outer layer at each routing node, until the Local Information Server of Things (L-TIS) receives the plain text. Meanwhile, the responded nodes can check the integrity of received data and the creditability of routing path in the transmitting procedure. The analysis shows that the novel transmission model of IoT has many properties, such as security, anonymity, trustworthy and attack-resistant.

Keywords Internet of Things; ONS query; trusted computing; anonymous authentication; anonymous transmission

1 引 言

物联网(Internet of Things,IoT)将感应器嵌入或装备到电网、铁路、桥梁、隧道、公路、建筑、供水系统、大坝、油气管道等物体中,实现物体与现有互联网的融合,实现人类社会、信息空间、物理系统的有机整合.在这个整合的网络中,存在能力超强的中心计算机群,用于对网络内的人员、机器、设备和基础设施实施实时的管理与控制[1].传统EPC(Electronic Product Code)物联网中,每一个物品都被赋予一个独一无二的代码,将这个代码存储在电子标签中并贴在物品上,同时将这个代码所对应的详细信息和属性存储在物品信息服务系统的服务器中.流通环节中利用RFID阅读器读取标签代码,通过对象名解析服务(Object Naming Service,ONS)系统解析后,本地ONS(Local Object Naming Service,L-ONS)服务器可获得物品所属信息服务系统的统一资源标识,然后L-ONS将该标识转发到本地物品信息服务器(Local Information Server of Things,L-TIS),进而L-TIS通过网络与远程物品信息服务器(Remote Information Server of Things,R-TIS)间的消息交换获得非本地代码所对应的详细物品信息及属性,实现物品的识别、自动追踪和管理功能[2].

然而传统物联网在用户隐私保护和信息安全传输机制中存在诸多不足[3-5]:(1)标签被嵌入任何物品,用户在没有察觉的情况下其标签被阅读器扫描,通过对物品的定位可追踪用户的行踪,使个人隐私遭到破坏;(2)射频识别系统读取速度快,通过对物品的迅速扫描方式跟踪企业销售情况的变化特点,使企业的商业秘密遭到泄露;(3)物品的详细信息在L-TIS与R-TIS间的传输过程易受流量分析、窃听、嗅探等网络攻击,导致物品信息传输过程存在安全隐患.

针对物联网安全性问题,文献[5]指出应该从容忍攻击方面进行研究,以应对单点故障、数据认证、访问控制和客户端的隐私保护等问题;建议对企业进行必要的风险评估与风险管理.文献[6]提出在考虑物联网的各种安全因素时,隐私保护强度和特定业务需求之间是有折衷,即在满足业务需求(实用性、易用性)基础上尽可能地保护用户隐私、定制适度的隐私保护策略(实现匿名性和用户行为的不可追踪);并指出物联网的安全机制应该从认证、访问控制、数据加密和立法等方面加强保护.文献[7]提出物联网安全研究应主要集中在物联网安全体系、个体隐私保护模式、终端安全功能、物联网安全相关法律的制订等方面,并给出了一个物联网的安全层次架构,该架构根据物联网的感知层、网络层和应用/中间件层将安全架构分为感知层安全、网络层安全和应用层安全.

目前的物联网安全方案更多地是从宏观上进行框架性讨论,涉及到物联网相关的感知、信息传输与信息处理三个阶段.在感知阶段:文献[8]在分析RFID协议的安全需求基础上,基于通用可组合安全模型,设计了低成本的RFID匿名认证协议,在确定的安全目标下证明了该协议的安全性;文献[9]分析了基于密码技术RFID安全协议的不足,用可证明安全性理论对RFID安全协议模型进行安全性研究;文献[10]给出了RFID系统中改进的防冲突算法,当大量标签同时识别时,该算法根据上一轮的碰撞情况估计待识别的标签数,然后对其进行分类或改变帧的大小以降低标签发生碰撞的概率,从而提高识别效率.文献[11]在欧盟提案的基础上,制订了信息感知阶段的隐私及数据保护的评估框架.

在信息处理阶段:文献[12]基于RFID和物联网技术提出了全球物联网体系架构,并结合该架构给出了物联网信息服务系统的设计方案,为实现物

联网架构、信息服务系统和物联网管理协议提供了参考；文献[13-14]系统地介绍了物联网编码、编码转换、名称解析服务、信息发布系统、中间件及网络管理等物联网关键技术，通过大量实例分析了物联网的国内外发展现状，并在此基础上给出了部分设计方案，对物联网的研究起到了指导作用.

纵观国内外在物联网基础技术方面的相关研究，文献[3-7]只分析了物联网传输机制中所存在的不足，并未给出相应的解决方案. 因此有必要进行物联网安全传输机制研究，尤其是增强传输过程中安全协议与隐私保护方法的研究，以提高物联网的安全性. 物联网在信息传输过程中易出现隐私泄露，其主要原因有：(1) 阅读器与标签之间的任意读取，即阅读器无条件读取物品标签编码给用户隐私保护带来隐患；(2) ONS 查询系统为 L-ONS 提供无条件查询功能，即任何 L-ONS 均可申请查询物品的详细信息；(3) 物品信息由 R-TIS 以明文形式传送给 L-TIS.

本文在分析 EPC 物联网传输机制的安全性基础上，为解决物联网信息传输过程中隐私保护方面所存在的不足，综合可信计算技术与双线性对的签密方法提出了一个物联网安全传输模型. 本文创新性的工作是给出了物联网安全传输模型的框架，并对安全传输框架下涉及的 ONS 安全查询过程、物品信息安全传输过程进行了协议设计与实现.

本文第 2 节详细介绍物联网安全传输模型，对可信匿名认证的 ONS 查询机制和物品信息可信匿名传输机制分别进行研究；第 3 节对物联网安全传输模型的匿名性、可信性和安全性等方面进行分析；第 4 节给出了基于本模型的安全物联网系统架构；最后总结展望了本文工作.

2　物联网安全传输模型

本文提出的物联网安全传输模型是通过引入可信第三方——可信认证服务器(Trusted Authentication Server，TAS)对原有模型进行改进：在 ONS 查询机制中增加可信匿名认证过程对 L-ONS 的身份合法性及平台可信性进行认证；物品信息可信匿名传输机制确保物品信息的安全传输，保证了物联网中物品信息的安全性与可信性. 物联网安全传输模型如图 1 所示.

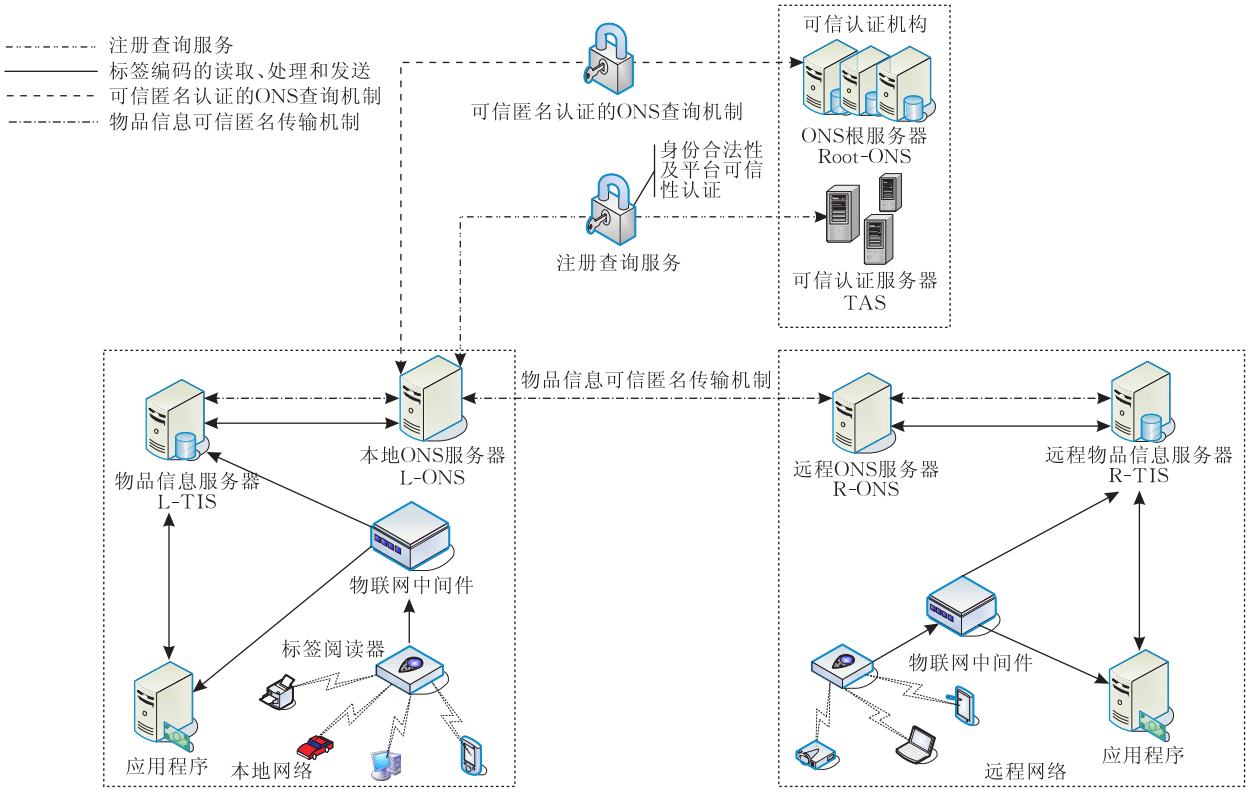

图 1　物联网安全传输模型

物联网安全传输模型由可信匿名认证的 ONS 查询机制和物品信息可信匿名传输机制组成，其中 TAS 在注册阶段为 L-ONS 生成查询系统的用户名，同时为其生成临时身份信息，完成对 L-ONS 的

身份合法性及平台可信性认证;在物品信息可信匿名传输机制中 R-TIS 按响应链路中各节点顺序从后至前用相邻节点的会话密钥对查询信息层层嵌套加密,传输过程中,响应数据每经过一个节点被解密一层,直到 L-TIS 时数据才被完全解密,且中间节点可根据前驱节点的签密信息验证转发数据的完整性,根据路由信息鉴别转发路径的真实性.

2.1 系统建立

设 G_1 和 G_2 是阶为素数 q 的群,G_1 为加法群,G_2 为乘法群,p 为 G_1 的生成元,设群 G_1 和 G_2 中离散对数问题是困难的,双线性对是满足下列性质的映射 $e:G_1\times G_1\rightarrow G_2$. TAS 选择满足双线性对要求的参数 G_1、G_2、e、q、p,其中 q、p 为 G_1 的生成元.

$E(k,m)$ 和 $D(k,c)$ 是一对单密钥加密/解密算法;P 是大素数;Q 是 $P-1$ 的大素数因子;g 是从 $[1,\cdots,P-1]$ 随机选取的模 P 的 Q 阶随机整数;$H(k,m)$ 是带密钥的杂凑函数;$H(m)$ 为标准散列算法 SHA-1,$\in_C$ 表示随机均匀选取集合中的元素,$\oplus$ 为异或运算,$\|$ 为连接符.

TAS 公开参数 $\langle G_1,G_2,e,q,p,H,P,Q,g\rangle$ 及加密/解密函数 E 和 D.

假设 1. 根 ONS 服务器(Root Object Naming Service,Root-ONS)与 TAS 都具有物联网管理中心 CA-IoT 签署的公钥证书. 如实体 A 的证书格式如下:

$$Cert_A=\{ID_A,KP_A,Date_A,LF_A,E(K_{\text{PrivCA-IoT}},ID_A\|KP_A\|Date_A\|LF_A)\},$$

其中 KP_A 是 A 的公钥,$K_{\text{PrivCA-IoT}}$ 是 CA-IoT 的私钥,$Date_A$ 是证书的签署日期,LF_A 是证书的有效期,则 Root-ONS、L-ONS 和 TAS 的密钥对分别为 $\{KP_{\text{Root-ONS}},KS_{\text{Root-ONS}}\}$、$\{KP_{\text{L-ONS}},KS_{\text{L-ONS}}\}$ 和 $\{KP_{\text{TAS}},KS_{\text{TAS}}\}$.

假设 2. 可信匿名认证机制和可信匿名传输机制中随机数的产生、加密/解密、Hash 运算等操作均可由可信平台模块(Trusted Platform Module,TPM)完成.

假设 3. R-TIS 基于可信计算技术构建物品信息传输链路的安全性和可信性,且每个节点有密钥协商、数据转发和加密/解密等操作能力.

假设 4. 物品信息传输链路中节点 R_i 的签密私钥为 $SK_i\in_C[1,Q-1]$,其公钥 $PK_i=g^{SK_i}\bmod P$.

假设 5. L-ONS、Root-ONS、TAS 及 CA-IoT 间有时钟同步机制可确保本模型中消息时戳的新鲜性.

2.2 可信匿名认证的 ONS 查询机制

在查询机制中,Root-ONS 在 TAS 的协助下对 L-ONS 的身份合法性及平台可信性进行认证,详细查询工作流程如图 2 所示.

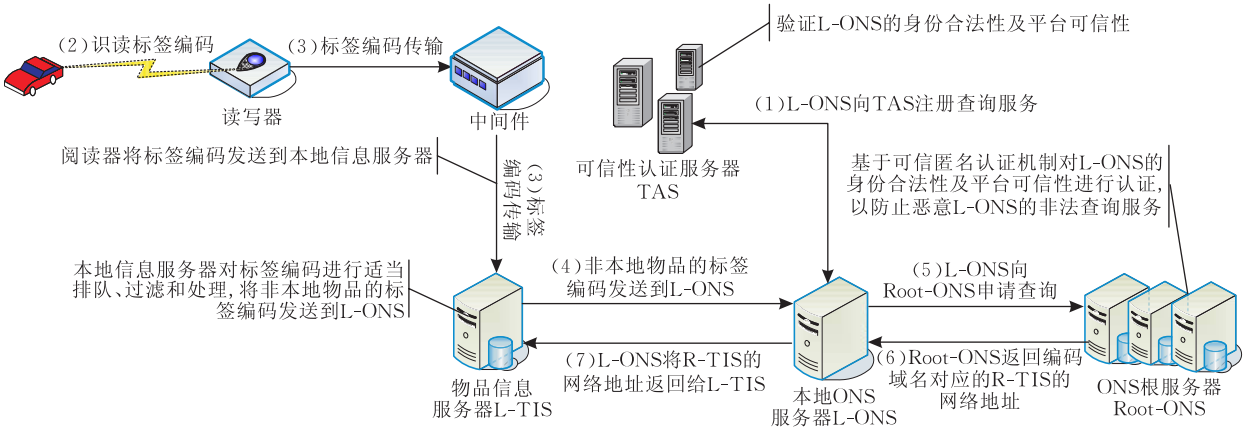

图 2 可信匿名认证的 ONS 查询机制

2.2.1 L-ONS 注册查询服务

L-ONS 向 TAS 申请注册查询服务,完成身份合法性及平台可信性认证.

(1) L-ONS 向 TAS 发送注册申请;

(2) TAS 基于平台可信性验证策略[15]认证 L-ONS平台的可信性,为身份合法且平台可信的 L-ONS分配唯一的临时标识号 $TID_{\text{L-ONS}}$,由式(1)计算产生秘密数 $S_{\text{L-ONS}}$,即

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

Num_{TAS} 为 TAS 随机选取的大数. 用式(2)计算 L-ONS 的临时身份 $TID_{\text{L-ONS}}$,即

$$TID_{\text{L-ONS}}=S_{\text{L-ONS}}\oplus ID_{\text{L-ONS}}\oplus ID_{\text{TAS}} \quad (2)$$

TAS 为 L-ONS 建立账户 $\langle ID_{\text{L-ONS}},S_{\text{L-ONS}},TID_{\text{L-ONS}},Num_{\text{TAS}}\rangle$,将 $S_{\text{L-ONS}}$ 和 $TID_{\text{L-ONS}}$ 交由 L-ONS

安全存储[16].

2.2.2　L-ONS 申请查询服务

L-ONS 注册成功后即向 Root-ONS 申请查询服务，以获知相关 R-TIS 的网络地址. 具体申请过程如图 3 所示：

(1) L-ONS 生成随机数 $X_0 \in [1, q-1]$，同时读取当前平台配置寄存器(Platform Configuration Register，PCR)的值，用私钥 $KS_{\text{L-ONS}}$ 对其加密，得 $s = E(KS_{\text{L-ONS}}, PCR \| X_0)$，读出度量日志 SML，并用式(3)计算临时密钥 key.

$$key = H(S_{\text{L-ONS}}) \tag{3}$$

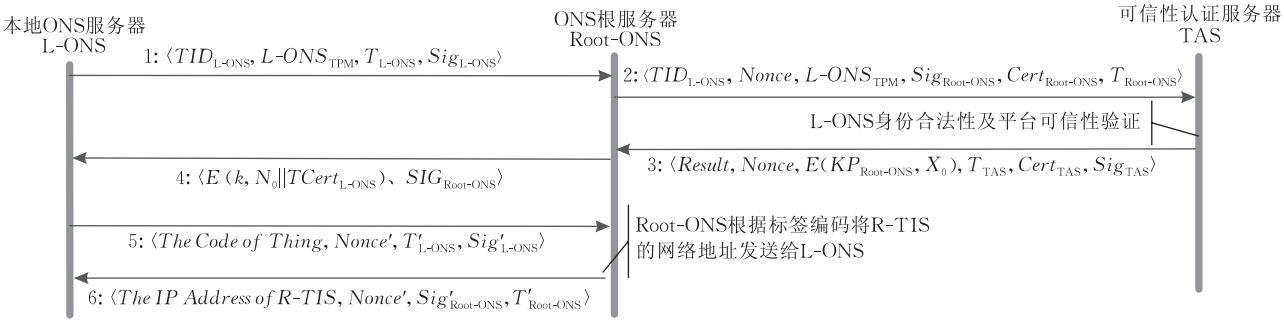

图 3　L-ONS 向 Root-ONS 申请查询服务

L-ONS 生成自身的完整性度量信息 $L\text{-}ONS_{\text{TPM}} = E(key, s \| SML)$ 后，将 $TID_{\text{L-ONS}}$，$L\text{-}ONS_{\text{TPM}}$ 及时戳 $T_{\text{L-ONS}}$ 连同签名信息 $Sig_{\text{L-ONS}}$ 一起发给 Root-ONS，其中 $Sig_{\text{L-ONS}} = H(KS_{\text{L-ONS}}, TID_{\text{L-ONS}} \| L\text{-}ONS_{\text{TPM}} \| T_{\text{L-ONS}})$.

(2) Root-ONS 验证 L-ONS 签名的真实性及时戳的有效性，以防范重放攻击，若验证无效，则拒绝为其提供查询服务，否则将选择随机数 $Nonce$，并生成消息签名 $Sig_{\text{Root-ONS}} = H(KS_{\text{Root-ONS}}, TID_{\text{L-ONS}} \| T_{\text{Root-ONS}} \| Nonce \| L\text{-}ONS_{\text{TPM}} \| Cert_{\text{Root-ONS}})$.

Root-ONS 发送消息 $TID_{\text{L-ONS}}$，$Nonce$，$L\text{-}ONS_{\text{TPM}}$，$Sig_{\text{Root-ONS}}$，$Cert_{\text{Root-ONS}}$，$T_{\text{Root-ONS}}$ 给 TAS.

(3) TAS 验证 Root-ONS 身份证书、消息签名及时戳的有效性，若无效则终止执行并退出认证机制，否则 TAS 按式(4)验证 L-ONS 的身份标识是否合法，即

$$ID_{\text{L-ONS}} = TID_{\text{L-ONS}} \oplus H(ID_{\text{L-ONS}} \| Num_{\text{TAS}}) \oplus ID_{\text{TAS}} \tag{4}$$

若 L-ONS 是非法用户，TAS 终止操作；否则计算密钥 key，解密 $L\text{-}ONS_{\text{TPM}}$ 获知度量 PCR 值及秘密随机数 X_0，结合 SML 及 PCR 值对 L-ONS 平台可信性进行验证，若验证不通过，TAS 终止操作；否则发送 $Result$，$Nonce$，$E(KP_{\text{Root-ONS}}, X_0)$，$T_{\text{TAS}}$，$Cert_{\text{TAS}}$，$Sig_{\text{TAS}}$ 给 Root-ONS，其中 $Sig_{\text{TAS}} = H(KS_{\text{TAS}}, Result \| Nonce \| E(KP_{\text{Root-ONS}}, X_0) \| T_{\text{TAS}} \| Cert_{\text{TAS}})$.

(4) Root-ONS 验证 TAS 身份证书的真实性、时戳的有效性，若无效，则中止执行，否则根据相关信息确认 L-ONS 的身份合法性与平台可信性，仅为身份合法且平台可信的 L-ONS 签发成员证书 $TCert_{\text{L-ONS}}$.

Root-ONS 解密 $E(KP_{\text{Root-ONS}}, X_0)$，计算 $k = X_0$，并产生随机数 N_0，将消息 $E(k, N_0 \| TCert_{\text{L-ONS}})$、$Sig_{\text{Root-ONS}}$ 发送给 L-ONS.

(5) L-ONS 获得 $TCert_{\text{L-ONS}}$ 和 N_0，并将标签编码、时戳、随机数和签名信息发给 Root-ONS.

(6) Root-ONS 根据收到的标签编码将对应 R-TIS 的网络地址与时戳、随机数和消息签名发给 L-ONS，即完成双方间身份合法性及平台可信性验证.

2.2.3　L-ONS 持成员证书申请查询服务

当 L-ONS 获得 $TCert_{\text{L-ONS}}$ 后，在有效期内可持其向 Root-ONS 多次申请查询服务，申请过程如图 4 所示.

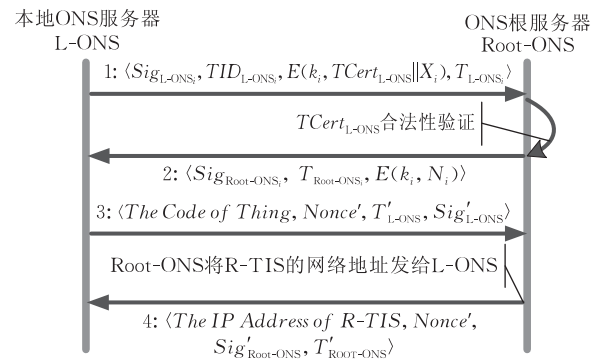

图 4　L-ONS 持 $TCert_{\text{L-ONS}}$ 申请查询过程

(1) L-ONS 再次申请查询时，生成随机数 $X_i \in_C [1, q-1]$，并计算本次查询申请的临时身份 $TID_{\text{L-ONS}_i}$，即

$$TID_{\text{L-ONS}_i} = TID_{\text{L-ONS}_{i-1}} \oplus N_{i-1} \tag{5}$$

其中 $TID_{\text{L-ONS}_0}=TID_{\text{L-ONS}}$，$i=1,2,3,\cdots,n$，用式(6)计算本轮会话密钥 k_i，

$$k_i=X_{i-1}\oplus N_{i-1} \tag{6}$$

其中 $k_0=k$，$i=1,2,3,\cdots,n$.

L-ONS 计算 $E(k_i,TCert_{\text{L-ONS}}\|X_i)$和 $Sig_{\text{L-ONS}_i}$，读取当前时戳 $T_{\text{L-ONS}_i}$，发送消息$Sig_{\text{L-ONS}_i}$，$TID_{\text{L-ONS}_i}$，$E(k_i,TCert_{\text{L-ONS}}\|X_i)$，$T_{\text{L-ONS}_i}$给 Root-ONS.

(2) Root-ONS 验证时戳和 $TID_{\text{L-ONS}_i}$ 是否有效，若无效则拒绝为 L-ONS 提供服务，否则计算 k_i，并解密 $E(k_i,TCert_{\text{L-ONS}}\|X_i)$，验证消息的完整性，同时验证 $TCert_{\text{L-ONS}}$的合法性，若合法则保存 X_i.

Root-ONS 产生随机数 N_i，计算消息签名 $Sig_{\text{Root-ONS}_i}$后发送消息$Sig_{\text{Root-ONS}_i}$，$T_{\text{Root-ONS}_i}$，$E(k_i,N_i)$给 L-ONS.

(3) L-ONS 将标签编码、时戳、消息签名连同随机数一起发送给 Root-ONS.

(4) Root-ONS 根据收到的标签编码，将对应 R-TIS 的网络地址连同时戳、随机数和消息签名一同发送给 L-ONS.

2.2.4 成员证书

(1) 证书结构

过频的申请查询服务，不仅增加 L-ONS 的完整性度量负载，同时降低了查询系统的工作效率. 本文使用证书机制减少 L-ONS 的可信性评估次数，提高查询系统的工作效率，证书的基本信息有：①有效期：证书的有效时间；②颁发时间：证书的颁发时间；③授权对象：证书拥有者临时身份信息 $TID_{\text{L-ONS}}$；④签名：Root-ONS 的签名信息.

(2) 证书合法性验证

在成员证书的有效期内，L-ONS 持该证书可多次申请查询服务，通过下述步骤验证成员证书的真实性，以判断 L-ONS 的身份合法性及平台可信性.

① 通过签名信息验证颁发者身份，同时检查证书内容是否被篡改；

② 根据证书的有效期、颁发时间等信息验证证书在当前时间是否有效；

③ 计算$TID'_{\text{L-ONS}}=TID_{\text{L-ONS}_i}\oplus N_{i-1}\oplus N_{i-2}\oplus\cdots\oplus N_0$，验证 $TID_{\text{L-ONS}}=TID'_{\text{L-ONS}}$是否成立，验证持有者是否是证书的申请者.

若上述验证均通过，表明 L-ONS 持有真实有效的合法成员证书.

2.3 物品信息可信匿名传输机制

L-TIS 通过 L-ONS 的查询机制获得相关 R-TIS 的网络地址，通过与 R-TIS 间的信息交互 L-TIS 可获知相关物品的详细信息. 本文设计的物品信息可信匿名传输机制实现 L-TIS 与 R-TIS 间物品信息的安全传输.

R-TIS 用合法且可信的中继节点建立如图 5 所示的物品信息传输链路，与各节点协商会话密钥，并获知各节点的身份 Hash 值.

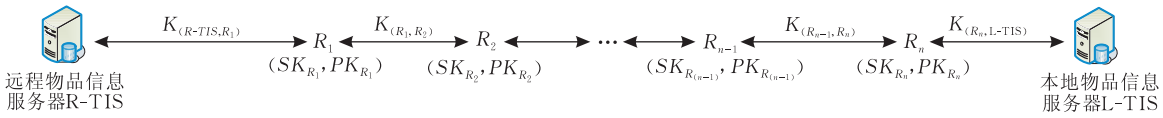

图 5 查询响应路径示意图

如图 6 所示，算法 1 中 R-TIS 根据链路中各节点顺序对物品信息依次进行嵌套加密封装，对封装的通信数据进行签密操作后产生查询响应信息 *Message*，节点 R_1 收到消息 *Message* 后通过算法 2 (如图 7 所示)进行消息转发，依此类推，链路中其它节点重复执行算法 2，直至 L-TIS.

节点 R_j 收到节点 R_{j-1} 发送的查询响应消息 *Message* 后，根据算法 2 对其进行转发，首先通过签密信息验证转发数据的完整性，根据路由信息鉴别转发路径的真实性. 然后将未被篡改的数据消息重新封装后转发到下一节点 R_{j+1}，在数据包封装过程中，节点 R_j 可在 *Message*′ 尾部填充任意字符，并对转发数据进行签密操作，确保通信数据及通信路径的真实性，即 R-TIS 生成的响应数据 *Message* 在节点间转发过程中大小不变，防止窃听者根据数据包的大小关系进行流量分析、窃听等攻击.

链路中的每个节点通过如图 7 所示的算法 2 根据消息验证数据的完整性及转发路径的真实性，将完整且真实的数据重新封装后转发给下一节点，直至目标 L-TIS.

3 物联网安全传输模型分析

本节从安全性、可信性、匿名性等方面对物联网安全传输模型进行分析.

3.1 可信匿名认证的 ONS 查询机制

在 L-ONS 申请查询服务时，Root-ONS 在 TAS 的协助下对L-ONS的身份合法性及平台可信性进

算法 1.　R-TIS 响应消息 *Message* 初始化算法.

输入：① R-TIS、L-TIS 及网络节点集合$\{R\text{-}TIS(R_0),R_1,R_2,R_3,\cdots,R_n,L\text{-}TIS(R_{n+1})\}$

② R-TIS、各节点的身份 Hash 值$\{H(ID_{\text{R-TIS}}),H(ID_{R_1}),H(ID_{R_2}),H(ID_{R_3}),\cdots,H(ID_{R_n}),H(ID_{\text{L-TIS}})\}$

③ R-TIS、各节点的签密公钥$\{PK_{\text{R-TIS}},PK_{R_1},PK_{R_2},PK_{R_3},PK_{R_4},\cdots,PK_{R_n},PK_{\text{L-TIS}}\}$

输出：$Message=E(KD_{(\text{R-TIS},R_1)},H(ID_{R_1})\|ST\|SP\|SQ\|T_{\text{R-TIS}}\|H(ID_{\text{R-TIS}})\|F_{R_0}\|w\|z\|INF)$

Begin

1. Add the R_j into the path of response, Only if the R_j is a trusted Node;

/ * 计算 R-TIS 与各节点的会话密钥 $k_{(\text{R-TIS},R_i)}$ * /

2. For $m=1$ to $m=n$
   $k_{(\text{R-TIS},R_m)}=e(qH(ID_{\text{R-TIS}}),H(ID_{R_m}))$;
   End For;
3. $k_{(\text{R-TIS},\text{L-TIS})}=e(qH(ID_{\text{R-TIS}}),H(ID_{\text{L-TIS}}))$;

/ * 封装查询响应数据，其中IP_m为节点R_m的 IP 地址，*Information* 为物品的详细信息 * /

4. $Data=E\{k_{(\text{R-TIS},\text{L-TIS})},Information\}$;
5. $Data=E\{k_{(\text{R-TIS},R_n)},IP_{\text{L-TIS}}\|Data\}$;
6. For $m=n-1$ to $m=1$
   $Data=E\{k_{(\text{R-TIS},R_m)},IP_{R_{m+1}}\|Data\}$;
   End For;

/ * 计算各节点的路由鉴别信息 * /

7. $J_{R_1}=H(ID_{\text{R-TIS}})\oplus H(ID_{R_1})\oplus H(ID_{R_2})$;
8. For $m=1$ to $m=n-1$
   $J_{R_{m+1}}=H(ID_{R_m})\oplus H(ID_{R_{m+1}})\oplus H(ID_{R_{m+2}})$;
   End For;
9. $J_{R_{n+1}}=H(ID_{R_n})\oplus H(ID_{\text{L-TIS}})\oplus H(ID_{\text{R-TIS}})$;
10. *Initial*(*ST*);
11. For $m=n+1$ to $m=1$
    $ST.Push(J_{R_m})$;
    End For;
13. $F_{R_0}=H(ID_{\text{R-TIS}})$;
14. $L_{R_0}=H(F_{R_0})$;
15. For $m=0$ to $m=n-1$
    $F_{R_{m+1}}=F_{R_m}\oplus H(ID_{R_{m+1}})$;
    $L_{R_{m+1}}=H(F_{R_{m+1}})$;
    End For;
16. $F_{R_{n+1}}=F_{R_n}\oplus H(ID_{\text{L-TIS}})$;
17. $L_{R_{n+1}}=H(F_{R_{n+1}})$;
18. *Initial*(*SP*);
19. For $m=n+1$ to $m=1$
    $SP.Push(L_{R_m})$;
    End For;
20. $KD_{(\text{R-TIS},R_1)}=H(ID_{\text{R-TIS}})\oplus H(ID_{R_1})$;
21. *Initial*(*SQ*);
22. $SQ.Push(PK_{\text{L-TIS}})$;
23. For $i=n$ to $m=2$
    $SQ.Push(PK_{R_i})$;
    End For;
24. $Num\in_C[1,Q-1]$;
25. $Key_1=g^{Num}\bmod P$;
26. $Key_2=H(PK_1^{Num}\bmod P)$;
27. $INF=E(Key_2,Data)$;
28. $w=H(Key_1,INF)$;
29. $z=Num(1+wSK_0)^{-1}\bmod Q$;
30. $R\text{-}TIS(R_0)$ generated time stamp is $T_{\text{R-TIS}}$;
31. $Message=E(KD_{(\text{R-TIS},R_1)},H(ID_{R_1})\|ST\|SP\|SQ\|T_{\text{R-TIS}}\|H(ID_{\text{R-TIS}})\|F_{R_0}\|w\|z\|INF)$;
32. R-TIS (R_0) Send *Message* to R_1;

End

图 6　响应消息初始化算法

算法 2.　节点 R_j 转发来自 R_{j-1} 的响应消息 *Message*.

输入：$Message=E(KD_{(R_{j-1},R_j)},H(ID_{R_j})\|ST\|SP\|SQ\|H(ID_{R_{j-1}})\|F_{R_{j-1}}\|T_{R_{j-1}}\|w\|z\|INF)$

输出：$Message'=E(KD_{(R_j,R_{j+1})},H(ID_{R_{j+1}})\|ST'\|SP'\|SQ'\|H(ID_{R_j})\|F_{R_j}\|T_{R_j}\|w'\|z'\|INF')$

Begin

/ * 验证转发数据的完整性 * /

1. $Key_1=(gPK_{j-1}^{w})^{z}\bmod P$;
2. $Key_2=H(Key_1^{SK_j}\bmod P)$;
3. $Data=D(Key_2,INF)$;
4. If $H(Key_1,INF)==w$ then go to 5;
   else stop and send error *message*;
   End if

/ * 鉴别转发路径的真实性 * /

5. $KD_{(R_{j-1},R_j)}=H(ID_{R_{j-1}})\oplus H(ID_{R_j})$;
6. Use $KD_{(R_{j-1},R_j)}$ decryption *Message*;
7. R_j get the $Y=H(ID_{R_j})$ from the *Message*;

/ * R_j 检查 $H(ID_{R_j})$ 与自身计算的是否相等 * /

8. R_j check $H(ID_{R_j})$ with the $Y=H(ID_{R_j})$ which decryption from *Message*;
9. If the check passes then go to 10;
   else stop and send error *message*;
   End If;
10. $L_{R_j}=SP.Get()$;
11. $SP'=SP.POP()$;
12. $F_{R_j}=F_{R_{j-1}}\oplus H(ID_j)$;
13. If $(L_{R_j}==H(F_{R_j}))$
    go to 14;
    else stop and send error *message*;
    End If;
14. $J_{R_j}=ST.Get()$;
15. $ST'=ST.Pop()$;
16. $H(ID_{R_{j+1}})=H(ID_{R_{j-1}})\oplus H(ID_{R_j})\oplus J_{R_j}$;
17. $K_{(\text{R-TIS},R_{j-1})}=e(qH(ID_{\text{R-TIS}}),H(ID_{R_{j-1}}))$;
18. R_j use $K_{(\text{R-TIS},R_{j-1})}$ decryption the Data;
19. $Data'=D(K_{(\text{R-TIS},R_{j-1})},Data)$;
20. $Num\in_C[1,Q-1]$;
21. $PK_{R_{j+1}}=SQ.Get()$;
22. $SQ'=SQ.Pop()$;
23. $Key_1=g^{Num}\bmod P$;
24. $Key_2=H(PK_{j+1}^{Num}\bmod P)$;
25. $INF'=E(Key_2,Data')$;
26. $w'=H(Key_1,INF')$;
27. $z'=Num(1+w'SK_j)^{-1}\bmod q$;
28. R_j get the IP of R_{j+1} from the Data;
29. $KD_{(R_j,R_{j+1})}=H(ID_{R_j})\oplus H(ID_{R_{j+1}})$;
30. R_j generated time stamp is T_{R_j};
31. $Message'=E(KD_{(R_j,R_{j+1})},H(ID_{R_{j+1}})\|ST'\|SP'\|SQ'\|H(ID_{R_j})\|F_{R_j}\|T_{R_j}\|w'\|z'\|INF')$;
32. R_j Send $Message'$ to R_{j+1};

End

图 7　响应消息节点转发算法

行验证,防止非授权 L-ONS 的查询申请,增强了物联网查询机制的可靠性、安全性及可信性.

3.1.1 安全性分析

认证机制的安全性是基于求解离散对数的困难性. L-ONS 利用秘密数 $S_{\text{L-ONS}}$ 和时戳通过散列函数计算临时密钥 k_i,由 $S_{\text{L-ONS}}$ 的机密性和散列函数的安全性保证 k_i 的不可伪造性,时戳保证了 k_i 的新鲜性.

TAS 检查时戳的新鲜性后,计算 L-ONS 的身份标识验证其合法性,同时结合完整性度量日志及 *PCR* 值验证 L-ONS 平台的可信性,即 Root-ONS 在 TAS 的协助下完成对 L-ONS 的身份合法性及平台可信性验证. 其中消息散列运算保证了消息的完整性,并且随机数可防止重放攻击.

L-ONS 再次申请服务时,其成员证书可证明身份的合法性及平台的可信性,并且每次均产生不同的会话密钥 k_i,实现了一次一密,增强了安全性. 由于 X_i 由 L-ONS 选择计算,而 N_i 由 Root-ONS 选择计算,因此 k_i 是一次性密钥,且任何一方无法单独计算产生,保证了会话密钥的公正性、新鲜性及前向保密性.

可信匿名 ONS 查询协议的安全性达到了通用可组合安全(UC 安全)等级,详细的证明过程请参见附录.

3.1.2 匿名性分析

(1)查询机制的匿名性和不可追踪性

通信消息中均未出现 L-ONS 的真实身份,注册时 L-ONS 的真实身份 $ID_{\text{L-ONS}}$ 被临时身份 $TID_{\text{L-ONS}}$ 替代. 因仅有 TAS 掌握秘密数 Num_{TAS},所以只有 TAS 才能通过式(2)正确验证用户的真实身份 $ID_{\text{L-ONS}}$,确保 L-ONS 身份的匿名性.

不同的 L-ONS 对应不同的 $TID_{\text{L-ONS}}$ 且由互不相同的随机数 Num_{TAS} 计算产生,并且任何合法 L-ONS 均无法通过自己的 $TID_{\text{L-ONS}}$ 计算其它 ONS 服务器的 ID 号,当同一 L-ONS 多次向 Root-ONS 申请查询时,每次均使用不同的临时身份 $TID_{\text{L-ONS}}$,具有不可跟踪性.

(2)证书的匿名性

成员证书仅报告持有者身份是否合法、平台是否可信,未包含其配置信息及其身份信息,即成员证书具有匿名性,匿名性的强弱取决于有效授权时间的长短,越短则匿名性越强,同时其匿名性是可控的,可控性依赖于证书持有者的临时身份信息,在有效期内仅允许同一用户用该证书建立查询服务.

3.1.3 可信性

TAS 对 L-ONS 配置信息的安全存储,保证了对 L-ONS 进行平台可信性验证的同时,有效保护了平台信息的私密性,即使 L-ONS 的配置信息遭泄露,但 L-ONS 可信性验证信息是经过密钥 k_i 加密处理的,由于 k_i 的保密性,避免 Root-ONS 依平台配置信息推知 L-ONS 的平台身份及配置状况.

L-ONS 通过向 TAS 提供签名后的平台 PCR 值及度量日志 SML 来证明平台的完整性. L-ONS 以硬件 TPM 为起点将可信性由底层通过信任链技术传递至应用层,即 TAS 根据完整性度量值及度量日志等信息鉴别 L-ONS 平台的可信性.

3.2 物品信息可信匿名传输机制

R-TIS 将物品信息按链路节点顺序从后至前嵌套加密,传输过程中加密后的数据每经过一个节点被解密一层,到 L-TIS 时数据才被完全解密,并且链路中各节点可根据前驱节点的签密信息验证数据的完整性,根据签名及路由信息鉴别链路的真实性,增强了物品信息传输过程的安全性.

3.2.1 匿名性分析

匿名通信链路中各节点仅知其前驱和后继节点的身份 Hash 值. 节点 R_{j+1} 用前驱节点 R_j 的 $H(ID_{R_j})$、自己的 $H(ID_{R_{j+1}})$ 和路由鉴别信息 $J_{R_{j+1}}$ 进行运算后仅得到后继节点 R_{j+2} 的 $H(ID_{R_{j+2}})$,无法获知其它节点的身份信息,即保证了 R-TIS 和 L-TIS 身份的匿名性;

每个节点通过计算仅能获知相邻节点的网络地址,无法获知其它节点的地址信息,即保证了 R-TIS 和 L-TIS 位置的匿名性.

匿名链路的路由鉴别信息、通信数据及地址信息只有合法的后继节点才能正确解密,保证了 R-TIS 和 L-TIS 通信的匿名性.

3.2.2 匿名度仿真

Reiter 和 Rubin[17] 提出针对共谋攻击的匿名度分析方法,攻击者由多个恶意节点组成,每个恶意节点占据了不同的位置. 从攻击者而言,发送者是位于第 1 个恶意节点之前的;接收者是位于最后 1 个恶意节点之后. 本文研究的物品信息传输机制由非恶意者发起,同时接收者也为非恶意者.

假设物品信息匿名传输链路的长度为 n,其中有 c 个恶意节点,则转发节点是有效节点的概率 p 为 $p=1-\frac{c}{n}$. 令发送者在第 0 号位置,接收者在第 $n+1$ 号位置,信息传输机制的匿名度为 d.

$H_x(1\leq x\leq n-c)$ 表示第 1 个恶意节点是链路的第 x 个节点;H_{x+} 表示第 1 个恶意节点在第 x 个

节点及之前的事件；$p(x)$表示链路中第 1 个恶意节点在第 x 个节点的概率，I 表示事件第 1 个恶意节点猜中发送者身份，则 $p(I|H_{1+})$表示恶意节点正确推断出消息发送者的概率，即为发送者匿名度.

第 1 个恶意节点在链路中第 x 个位置的概率 $p(H_x)$为 $p(H_x)=p^{(x-1)}(1-p)$；第 1 个恶意节点出现在链路中第 1 个位置及之后的概率 $p(H_{1+})$为

$$p(H_{1+})=(1-p)\sum_{i=1}^{n-c}p^{i-1}=1-p^{n-c}.$$

当第 1 个恶意节点是链路的第 1 个节点时，它的前驱节点即为发送者，恶意节点猜中发送者的概率为 1，即 $p(I|H_1)=1$；第 1 个恶意节点在第 2 个节点或在其之前，它的前驱不可能是发送者，即其猜中发送者的概率为 0，即 $p(I|H_{2+})=0$.

因为 $p(I)=p(H_1)\cdot p(I|H_1)+p(H_2)\cdot p(I|H_{2+})$，

又因为 $p(I)=p(H_{1+})\cdot p(I|H_{1+})$，

所以 $p(I|H_{1+})=\dfrac{1-p}{1-p^{n-c}}=\dfrac{1-p}{1-p^{np}}$.

$M_x(c\leq x\leq n)$表示最后 1 个恶意节点是链路的第 x 个节点；M_{x-}表示最后 1 个恶意节点在第 x 个节点及之后的事件；$Q(x)$表示链路中最后 1 个恶意节点是第 x 个节点的概率，R 表示事件最后 1 个恶意节点猜中接收者身份，则 $Q(R|M_{n-})$表示恶意节点正确推断出消息接收者的概率，即为接收者匿名度.

最后 1 个恶意节点是链路第 x 个节点的概率 $Q(H_x)$为 $Q(M_x)=(1-p)\ p^{(n-x)}$；最后 1 个恶意节点是链路中第 n 号位及以后的概率 $Q(M_{n-})$为

$$Q(M_{n-})=(1-p)\sum_{x=c}^{n}p^{n-x}.$$

当最后 1 个恶意节点是转发路径的第 n 个节点时，它的后继节点即为接收者，恶意节点猜中接收者的概率为 1，即 $Q(R|M_n)=1$；最后 1 个恶意节点是第 $n-1$ 个节点或在其之后时，它的后继节点不可能是发送者，恶意节点猜中接收者的概率为 0，即 $Q(R|M_{(n-1)-})=0$.

因为 $Q(R)=Q(M_n)\cdot Q(R|M_n)+Q(M_{(n-1)})\cdot Q(R|M_{(n-1)-})$，

又因为 $Q(R)=Q(M_{n-})\cdot Q(R|M_{n-})$，

所以 $Q(R|M_{n-})=\dfrac{1-p}{1-p^{n-c+1}}=\dfrac{1-p}{1-p^{np+1}}$.

综上所述，匿名度

$$d=P(I|H_{1+})\cdot Q(R|M_{n-})=\frac{(1-p)^2}{(1-p^{np})(1-p^{np+1})}.$$

仿真表明，匿名度随 n 和 p 的增大而减小，受 p 的影响较大(如图 8 所示). 当 $n\geq 10$，$p\geq 0.4$ 时匿名度大小趋近于 0，接近绝对匿名的等级，且此时匿名度大小不受节点数影响(如图 9 所示). 这种结果与现实情况基本一致，说明物品信息可信匿名传输机制具有较强的匿名性.

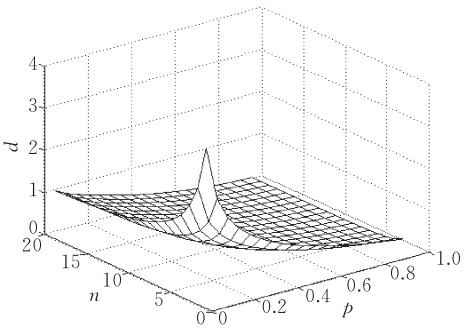

图 8　匿名度 d 变化趋势图

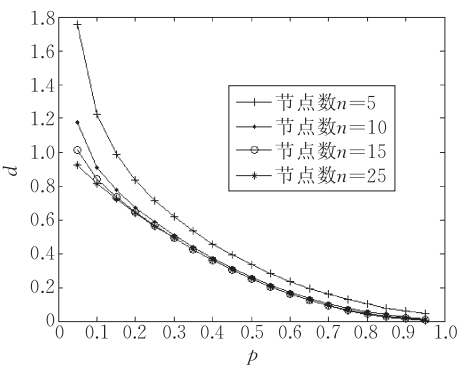

图 9　节点数 n 对匿名度的影响

3.2.3　安全性分析

安全性是建立在求解双线性难解问题的基础之上. 当窃听者获得节点的公钥 $H(ID_{R_i})$时，因大素数 q 的保密性而无法求解节点私钥 $qH(ID_{R_i})$. 即使当窃听者捕获了节点 R_i，获得节点的公钥和私钥对，因面临求解双线性难解问题而使窃听者无法求解出 q，因此即使捕获了一些节点，但其它节点的安全性不受其影响.

(1) 抗被动攻击. 若窃听者捕获到节点 R_{i-1}的 $H(ID_{R(i-1)})$，由于没有当前节点 R_i的 $H(ID_{R_i})$，而无法计算共享密钥，从而不能正确解密路由信息，因此仅有合法的路由节点才能得到正确的路由信息；同时响应路径中各节点的填充机制使通信数据包大小不变，方案可抵抗流量分析等攻击.

(2) 抗主动攻击. 若窃听者捕获 R_i与 R_{i-1}间的共享密钥，窃听者仅能获得 R_{i+1}的 $H(ID_{R_{i+1}})$，并不能获得其它路由节点的任何信息. 假设窃听者希望跳过节点 R_{i+1}并把下一节点设为 R_k，当节点 R_k收

到路由信息后根据算法 2 取出堆栈 SP 的栈顶元素 $L_{R_{i+1}}=SP.Get()$，计算 $F_{R_k}=F_{R_{k-1}}\oplus H(ID_{R_k})$ 后，显然 $L_{R_{i+1}}!=H(F_{R_k})$，则 R_k 拒绝转发数据，保证了数据转发链路的真实性.

(3) 信息的极小量泄露. 链路中各节点仅知晓其前驱节点和后继节点的假名信息及网络地址，无法获知其它节点及 L-TIS 与 R-TIS 的相关信息.

(4) 路由的可鉴别性. 链路中的各节点均能确认它是链路的一部分，并且每个节点都可确认数据信息来源的真实性.

(5) 响应数据的可验证性. 链路中各节点均能通过前驱节点的签密信息验证转发数据的真实性，且只有合法的后继节点才能解密前驱节点的签密信息.

3.2.4 可信性分析

链路建立阶段对各节点的可信性使用相关策略[15]进行验证，只有通过可信性验证的节点才能接入，增强了链路的可信性，物品信息传输过程中，建立了以 TPM 为核心的节点安全保护机制，以及节点接入时的可信性验证机制，确保物联网安全传输模型中查询响应链路的可信性，增强了物品信息传输过程的安全性.

3.3 安全传输模型效率分析

物联网安全传输模型中的部分运算(如加密/解密、生成随机数、散列运算等)是由 TPM 完成，不消耗平台 CPU 的计算能力，TPM 作为独立的计算单元，可以提高物联网安全传输模型中协议的执行效率.

身份合法且平台可信的 L-ONS 申请成员证书后可持其多次申请查询服务，证书机制的使用提高了物联网安全传输模型的工作效率，同时有效减少 L-ONS 的完整性度量负载，防止 Root-ONS 和 TAS 成为系统瓶颈.

查询机制中第一轮交互即对 L-ONS 的身份合法性和平台可信性进行验证，若验证未通过，TAS 和 Root-ONS 在第一轮后就终止交互，降低了传输模型的执行负载.

4 物联网安全体系架构

基于本传输模型的物联网安全体系架构如图 10 所示，其中物联网管理中心 CA-IoT 是一级管理中心，制定和发布总体标准，并对第二级的各地区的 Root-ONS 和 TAS 进行管理(Root-ONS 和 TAS 可由物理环境中同一台服务器实现，可合称为 TRoot-ONS)；第二级为相关地区的 TRoot-ONS，负责验证本地区 L-ONS 身份合法性和平台可信性，响应查询服务，同时可备份本地区 TIS 中相关物品的信息；第三级为本地物联网系统，负责物品标签编码的读取、处理、发送和申请查询服务等操作. TRoot-ONS 加入安全物联网系统时，CA-IoT 对其身份合法性及平台可信性进行验证，仅对通过验证的 TRoot-

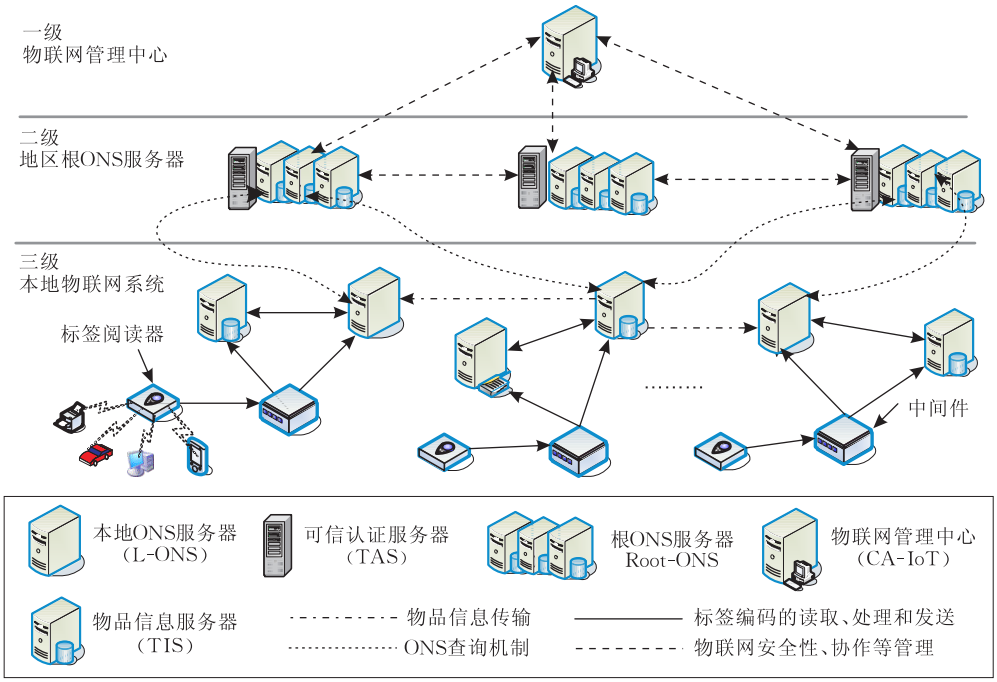

图 10 物联网安全体系架构

ONS 颁发身份证书，同时 CA-IoT 定期对系统成员进身份合法性和平台可信性验证，将属性发生变化的成员移出系统，确保物联网 ONS 查询系统的可信性，同时各地区 TRoot-ONS 形成分布式查询系统，来受理 L-ONS 查询申请.

本文物联网安全体系架构除安全性、高效性、可信性和匿名性等特点外，其还具有扩展性好、健壮性高和前向安全的特点.

(1) 扩展性好

当某地区需部署新的查询系统时，新成员只需向 CA-IoT 申请注册，CA-IoT 为身份合法且平台可信的新成员颁发身份证书，在 CA-IoT 的协助下系统成员更新相关成员信息，使各成员形成相互协作的整体.

(2) 健壮性高

本文的安全物联网中采用分布式的查询体系，即各地区 TRoot-ONS 相互协作完成 L-ONS 的查询服务，这种任务分级处理的查询体系可有效防止个别 TRoot-ONS 由于负载过重而成为系统瓶颈，同时物品信息的区域备份机制可保证在相关 TIS 无法正常工作时，物品信息机制可顺利进行.

(3) 前向安全性

假设 L-ONS 的第 i 次查询申请密钥 k_i 泄露，即攻击者获悉信息 X_{i-1} 和 N_{i-1}，但是攻击者无法从信息 X_{i-1} 和 N_{i-1} 推导出密钥 k_{i+1} 与 k_{i-1}，保证了物联网安全体系模型中查询系统的前向安全性.

5　结束语

本文提出物联网安全传输模型，该模型对传统物联网中 ONS 查询机制及物品信息传输过程进行改进. 在 ONS 查询机制中加入匿名认证过程，仅为经过授权且可信的 L-ONS 提供查询服务，防止非授权 L-ONS 查询物品信息；采用可信匿名通信过程完成物品详细信息的传输，增强物品信息传输过程的安全性，防止攻击者对其进行流量分析、窃听等网络攻击行为. 分析表明，物联网安全传输模型具有安全性、匿名性、可信性、高效性和抗攻击性等特点；本文的物联网安全体系架构具有扩展性好、健壮性高和前向安全的特点. 本模型的创新点是提出了一个传输模型框架，且给出了可行的协议实现方案.

本模型中 L-ONS 和 R-ONS 是对称的，在实际应用中可以将两个功能合并在同一个本地网络之中，以实现本地网络请求服务与远程网络的响应服务功能.

参　考　文　献

[1] Ning Huan-Sheng, Zhang Yu, Liu Fang-Li, Liu Wen-Ming et al. Research on China Internet of Things services and management. Acta Electronica Sinica, 2006, 34(12A): 2514-2517(in Chinese)
(宁焕生，张瑜，刘芳丽，刘文明等. 中国物联网信息服务系统研究. 电子学报，2006，34(12A)：2514-2517)

[2] Liu F L, Ning H S et al. RFID-based EPC system and information services in intelligent transportation system//Proceedings of the 6th International Conference on ITS Telecommunications Proceedings. Chengdu, China, 2006: 26-28

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

[4] Luigi Atzori, Antonio Iera, Giacomo Morabito. The Internet of Things: A survey. Computer Networks, 2010, 54(1): 2787-2805

[5] Weber Rolf H. Internet of Things-New security and privacy challenges. Computer Law & Security Review, 2010, 26(1): 23-30

[6] Ning Huan-Sheng, Xu Qun-Yu. Research on global Internet of Things' developments and it's lonstruction in China. 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. 电子学报，2010，38(11)：2591-2599)

[7] Liu Yan-Bing, Hu Wen-Ping, Du Jiang. Network information security architecture based on Internet of Things. ZTE Technology Journal, 2011, 17(1): 17-20(in Chinese)
(刘宴兵，胡文平，杜江. 基于物联网的网络信息安全体系. 中兴通信，2011，17(1)：17-20)

[8] Deng Miao-Lei, Ma Jian-Feng, Zhou Li-Hua. Design of anonymous authentication protocol for RFID. Journal on Communications, 2009, 30(7): 20-26(in Chinese)
(邓淼磊，马建峰，周利华. RFID 匿名认证协议的设计. 通信学报，2009，30(7)：20-26)

[9] Zhou Yong-Bin, Feng Deng-Guo. Design and analysis of cryptographic protocols for RFID. Chinese Journal of Computers, 2006, 29(4): 581-589(in Chinese)
(周永彬，冯登国. RFID 安全协议的设计与分析. 计算机学报，2006，29(4)：581-589)

[10] Ding Zhen-Hua, Li Jin-Tao, Feng Bo. Research on Hash-based RFID security authentication protocol. Journal of Computer Research and Development, 2009, 46(4): 583-592(in Chinese)
(丁振华，李锦涛，冯波. 基于 Hash 函数的 RFID 安全认证协议研究. 计算机研究与发展，2009，46(4)：583-592)

[11] GS1, European Commission. Privacy and Data Protection Impact Assessment Framework for RFID Applications. January 12, 2011. http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf

[12] Ken T, Felice A, Henri B, Paul D et al. The EPCglobal Architecture Framework (V1.4). December 15, 2010. http://www.gs1.org/gsmp/kc/epcglobal/architecture/architecture_1_4-framework-20101215.pdf

[13] Ning Huan-Sheng, Zhang Yan. RFID and IOT—RF, Middleware, Analysis and Services. Beijing: Publishing House of Electronic Industry, 2008: 108-235(in Chinese)
(宁焕生，张彦. RFID 与物联网—射频、中间件、解析与服务. 北京：电子工业出版社，2008：108-235)

[14] Ning Huan-Sheng, Wang Bing-Hui. Major Project of RFID and IOT of State. Beijing: China Machine Press, 2008: 95-178(in Chinese)
(宁焕生，王炳辉. RFID 重大工程与国家物联网. 北京：机械工业出版社，2008：95-178)

[15] Wu Zhen-Qiang, Zhou Yan-Wei, Qiao Zi-Rui. A controllable and trusted anonymous communication scheme. Chinese Journal of Computers, 2010, 33(9): 1686-1702(in Chinese)
(吴振强，周彦伟，乔子芮. 一种可控可信的匿名通信方案. 计算机学报，2010，33(9)：1686-1702)

[16] Yang Li, Ma Jian-Feng, Zhu Jian-Ming. Trusted and anonymous authentication scheme for wireless networks. Journal on Communications, 2009, 30(9): 29-35(in Chinese)
(杨力，马建峰，朱建明. 可信的匿名无线认证协议. 通信学报，2009，30(9)：29-35)

[17] Reiter M K, Rubin A D. Crowds: Anonymity for Web transactions. ACM Transactions on Information and System Security, 1998, 1(1): 62-92

附 录.

本文采用通用可组合(Universally Composable, UC)安全模型分析、证明可信匿名 ONS 查询机制的安全性.

在 L-ONS 申请查询服务时完成对 L-ONS 的身份合法性及平台可信性的验证，其中 $L\text{-}ONS_{\text{TPM}}$ 是 L-ONS 发送给 Root-ONS 的身份合法性及平台可信性验证消息. 对于 Root-ONS 而言，只要保证消息 $L\text{-}ONS_{\text{TPM}}$ 确实来自 L-ONS 且在传输过程中并未被篡改，就可以确保对 L-ONS 身份合法性及平台可信性验证的正确性，协议中证书和签名机制的使用可保证消息 $L\text{-}ONS_{\text{TPM}}$ 的上述性质.

首先给出查询机制的抽象描述协议 Π，因 Root-ONS 在 TAS 的协助完成对 L-ONS 身份合法性及平台可信性验证，Root-ONS 与 TAS 间存在安全的通信信道，并且 Root-ONS 与 TAS 可由物理环境中的同一台服务器实现，所以在模型抽象协议中将 Root-ONS 和 TAS 作为一个整体来考虑. 假设协议在两个实体 I 和 R 间进行. 如下所示：

$R\rightarrow I$: $T_{\text{L-ONS}}, TID_{\text{L-ONS}}, L\text{-}ONS_{\text{TPM}}, SIG_R$

$I\rightarrow R$: $TCert_{\text{L-ONS}}, Num_0, SIG_I$

$R\rightarrow I$: The Code of Things, $Nonce'$, $T'_{\text{L-ONS}}$, $TCert_{\text{L-ONS}}$, SIG'_R

$I\rightarrow R$: The Addresses of TIS, $Nonce'$, $T'_{\text{Root-ONS}}$, SIG'_I

定理 1. 协议 Π 安全实现理想函数 F_{KE}，对任何环境机 Z 均有等式 $REAL_{\Pi,I,Z}\approx IDEAL_{FKE,R,Z}$ 成立，即协议 Π 是 UC 安全的.

证明. 协议 Π 证明思路：首先构造安全实现签名的理想函数 F_{sig} 的协议 P_s；其次，给出安全的可信证明理想函数 F_{KE}，同时构造一个协议 Π_1，并证明协议 Π_1 在混合模型 F_{sig}-hybrid 下安全实现了 F_{KE}；将协议 P_s 与 Π_1 进行组合，通过 UC 安全组合定理，证明组合后的协议与 Π 等价，且在现实模型下安全实现了 F_{KE}. 证毕.

引理 1. $Sig=(gen, ID, ver)$ 是 UC 安全的一个签名方案，则在真实环境下，协议 P_s 可以安全实现 F_{sig}，当且仅当 S 是抗击选择消息存在性伪造.

实现理想签名函数 F_{sig} 的协议 P_s：

P_s 协议参与者为 P 和 Q，运行基本算法为 gen, sig, ver.

① P 收到输入 $(Signer, id)$ 后执行算法 gen，保留签名 $sign$，将验证密钥 PK 发给 Q.

② 当 P 需要对消息 m 进行签名时，P 利用签名算法计算 $\sigma\leftarrow sig(SK, m)$，并将消息 $(Signatare, id, m, \sigma)$ 发给 Q.

③ 当 P 接收到消息 $(Verified, id, m, \sigma)$，需要对消息签名 σ 进行验证时，则 P 输出 $(Verified, id, m, Ver(PK, m, \sigma))$.

引理 2. 如果 DDH 假设成立，且消息认证算法是安全的，则协议 Π 在 F_{sig}-hybrid 下安全实现 F_{KE}.

证明. 首先构造可信证明理想函数 F_{KE} 的协议 Π_1，构造过程如下所示：

协议参与者 P 与 Q 在混合模型 F_{sig}-hybrid 中运行协议 Π_1，进行交互.

① 当协议发起者 P 得到输入 (P, Q, Sid)，则发送初始化消息 $(signer, 0, Sid)$ 给 F_{sig}；同样，当协议响应者 Q 得到输入 (Q, P, Sid) 则发送 $(signer, 1, Sid)$ 给 F_{sig}.

② 协议发起者 P 选择随机数 $Nonce$，发送 $(sign, 0, sid, M_1)$ 给 F_{sig} 得到其返回的消息签名 σ_1，最后发送 $(Nonce, M_1, \sigma_1)$ 给 Q，其中 $M_1=T_{\text{L-ONS}}\parallel TID_{\text{L-ONS}}\parallel L\text{-}ONS_{\text{TPM}}$.

③ 协议响应者 Q 收到消息 $(Nonce, M_1, \sigma_1)$ 后，发送 $(Verify, 0, sid, P, M_1, \sigma_1)$ 给 F_{sig}，如果验证通过 Q 则随机选择 Num_0，发送 $(sign, 1, sid, M_2)$ 给 F_{sig} 得到其返回的消息签名 σ_2，最后发送 $(Nonce, M_2, \sigma_2)$ 给 P，其中 $M_2=TCert_{\text{L-ONS}}\parallel Num_0$.

④ 当 P 收到 $(Nonce, M_2, \sigma_2)$ 后，发送 $(Verify, 1, sid, Q, M_2, \sigma_2)$ 给 F_{sig}，如果验证通过则 P 选择随机数 $Nonce'$，发送 $(sign, 0, sid, M_3)$ 给 F_{sig} 得到其返回的消息签名 σ_3，最后发送 $(Nonce', M_3, \sigma_3)$ 给 Q，其中消息 $M_3=$ The Code of Things $\parallel$

$T_{\text{L-ONS}'} \parallel TCert_{\text{L-ONS}}$.

⑤当 Q 收到($Nonce'$,M_3,σ_3),发送($Verify$,0,sid,P,M_3,σ_3)给 F_{sig},验证消息签名 σ_3 的合法性,若验证通过,则发送($sign$,1,sid,M_4)给 F_{sig},得到其返回的消息签名 σ_4 后发送($Nonce'$,M_4,σ_4)给 P,其中 M_4 = The Addresses of TIS $\parallel$ $T_{\text{Root-ONS}'}$. 最后本地输出(Sid,Q,P).

⑥当 P 收到($Nonce'$,M_4,σ_4)后,发送($Verify$,1,Sid,Q,M_4,σ_4)给 F_{sig},验证 σ_4 的合法性,若通过合法性验证,则本地输出(Sid,P,Q).

Π_1 为基于可信证明理想函数 F_{KE} 的协议,令协议 Π_1 是在混合模型 F_{sig}-hybrid 下的可信证明协议,H 为攻击模型中的攻击者. 构造一个理想环境下的攻击者 S(仿真器),使得任何环境机 Z 都不能辨别 S 是与 H 及 Π_1 在 F_{sig}-hybrid 下进行交互,还是与 S 及 F_{KE} 在 Ideal-life 下进行交互,即对任何环境机 Z,等式 $REAL_{\Pi_1,H,Z} \approx IDEAL_{FKE,S,Z}$ 均成立.

仿真器 S

①任何从 Z 的输入均传递给 H,任何 H 的输出将作为 S 的输出使 Z 可以读取.

②当 S 从 F_{KE} 处收到消息(Sid,P,Q,$role$),表明 P 发起了可信证明信息的传输,那么让 S 仿真出 F_{sig} 及 F_{sig}-hybrid 下与 H 交互的协议 Π_1,并给定同样的输入. 并且 S 让 H 和 P 按照 Π_1 的执行规则与 Z 交互.

③为了仿真 Π_1 的执行,S 可以激活 F_{sig} 得到相应的消息签名 σ.

④当 Π_1 中的某个 P 产生了本地输出,如果对端 Q 没有被攻陷,则 S 将 F_{KE} 的输出发送给 P;如果 Q 已被攻陷,F_{KE} 则让 S 决定证明信息,而 S 则使用 P 前面的输出来确定仿真的 P 与 Q 的本地输出.

⑤当 H 执行攻陷 P 的操作,S 同样攻陷 P. 如果 F_{KE} 已经给 P 发送了可信证明信息,则 S 将得到该信息;如果 P 和 Q 均没有产生本地输出,则 S 将其内部状态传递给 H,包括它们的秘密选值;如果 P 或 Q 其中一方已产生本地输出,则它们的信息均被擦除,S 直接将本地输出的信息传递给 H.

假设在仿真器 S 的执行下,存在一个环境机 Z',成功辨别与 H 及 Π_1 在 F_{sig}-hybrid 下进行交互与 S 及 F_{KE} 在 Ideal-life 下进行交互的概率不可忽略,即 $prob(REAL_{\Pi_1,H,Z} \neq IDEAL_{FKE,S,Z})$ 为 $\frac{1}{2}$ 加上一个不可忽略的优势 ε. 使用区分器 D,利用环境机 Z' 来破解 DDH 问题,进而规约到矛盾.

区分器 D

①以 1/2 的概率选择选择 $I \leftarrow \{I_0, I_1\}$ 作为 D 的输入,记为(α^*,β^*,γ^*).

②随机选择 $\tau \leftarrow \{1,2,\cdots,L\}$,$L$ 为攻击者所能发起的会话数的上界,然后仿真 F_{sig}-hybrid 中 Π_1 和 H 与 Z 的交互.

③当 H 激活一个参与方建立一个新的会话 t($t \neq \tau$)或者接收一条消息时,D 代表该参与方按照协议 Π_1 在 F_{sig}-hybrid 中进行正常交互. 如果 $t = \tau$,则 D 代表 P 向 Q 发送消息(P,sid,α^*);当 Q 收到(P,sid,α^*),D 调用 F_{sig} 进行相应计算,并发送(sid,β^*,σ)给 P;最终 D 让 P 与 Q 本地输出(sid,P,Q,γ^*).

④如果 H 攻陷一个参与方,则 D 把该参与方的内部状态返回给 H;如果被攻陷的参与方是会话 t 的参与方之一,则 D 随机输出 $b' \leftarrow \{0,1\}$ 并终止.

⑤如果 F_{sig}-hybrid 中的协议 Π_1 运行完后,Z 输出 b,则 D 输出 $b' = b$ 并终止.

通过对区分器 D 执行过程分析,根据区分器 D 的构造原理,得出 D 成功区分输入 I_0 和 I_1 的概率等于环境机 Z' 成功辨别理想和混合两种环境的概率,即 D 能够以 $\frac{1}{2}$ 加上一个不可忽略的优势 ε 成功区分 I_0 和 I_1,而这与 DDH 假设矛盾.

证毕

引理 3. 令 Π_1 是 F_{sig}-hybrid 下的协议,P_s 为安全实现 F_{sig} 的协议,则对于任何攻击者 A 都存在一个攻击者 H,使得对任何环境机 Z 来说,等式 $REAL_{\Pi_1 P_s,A,Z} \approx IDEAL_{\Pi,H,Z}$ 均成立,即组合协议 $\Pi_1 P_s$ 安全仿真 F_{sig}-hybrid 下的协议 Π.

证明. 根据 DDH 假设即可证明引理 3 成立. 证毕

引理 4. 真实环境下,组合协议 $\Pi_1 P_s$ 与协议 Π 等价.

证明. 将混合模型 F_{sig}-hybrid 下协议 Π_1 对理想函数 F_{sig} 的访问均替换为对协议 P_s 的访问,即协议 $\Pi_1 P_s$ 与协议 Π 等价. 证毕

定理 2. 协议 Π 安全实现理想函数 F_{KE},对任何环境机 Z 则 $REAL_{\Pi,A,Z} \approx IDEAL_{FKE,S,Z}$ 均成立,即可信匿名的 ONS 查询机制是 UC 安全的.

证明. 根据引理 1～4 及定理 1 即可证得定理 2 成立. 证毕

综上所述,可信匿名认证的 ONS 查询机制是安全可信的物联网 ONS 查询机制

WU Zhen-Qiang, born in 1968, Ph.D., associate professor. His research interests include anonymous communication, trusted computing, and pervasive computing.

ZHOU Yan-Wei, born in 1986, M. S., assistant engineer. His research interests include anonymous communication and trusted computing.

MA Jian-Feng, born in 1964, Ph. D., professor. His research interests include information security and cryptography.

Background

The Internet of Things (IoT), an emerging global Internet-based technical architecture facilitating the exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders. Measures ensuring the architecture's resilience to attacks, data authentication, access control, confidentiality of address data, confidentiality of object data, confidentiality of provider identity (service anonymity), confidentiality of client identity (client anonymity), confidentiality of query content, query confidentiality, confidentiality of client location and client unobservability need to be established.

This paper focuses on the ONS queries and the transmitted data in IoT. The requirement of query confidentiality shall be satisfied if not both elements of a pair (identity, query content) become known to an adversary, for example as (IP, EPC) tuple. The pseudonymity of the concentration strategy, i.e., collecting ONS queries from different ONS to hide the real source IP address, would be the use of so called anonymous mixes, a strategy that might be viable for supply chains as well as for private households in IoT. Most popular implementation being Tor—is to cryptographically transform and mix Internet traffic from many different sources, in order to hamper matching a particular IP packet to a particular source. With onion routing, the transmitted data is wrapped into multiple encryption layers by using the public keys of the routers on the transmission path, but is not stored for later transmission, resulting in lower latency suitable for near real-time applications.

This research was supported by the National Natural Science Foundation of China (60633020) and the National High Technology Research and Development Program (863 Program) of China (2007AA01Z438200). The NSFC project, theory and application in trusted mobile Internet, has published two books by Higher Education Press, Beijing and Springer-Verlag Berlin Heidelberg, which titles are "Security Architecture for Wireless Local Area Network" and "Security Access in Wireless Local Area Network, from Architecture and Protocols to Realization". The latter 863 Program projects were applying trusted access technology in wireless network and IoT. The team has published several research articles as described in reference, submitted three industry specifications for trusted digital home, received two patents grant of China and registered two computer software copyrights.