

权限可控传递的物联网共享设备委托授权访问机制

宋宇波, 戚姗姗, 胡爱群

(东南大学网络空间安全学院, 江苏 南京 211111)

摘要: 为了解决在共享模式下设备所有者在委托授权时权限敏感度保护以及中间代理滥用授权的问题, 综合基于信任度访问控制模型和代理签名的特征, 提出了一种基于信任度的可控部分权限委托授权机制。该机制采用基于角色和信任度值的授权策略, 通过代理签名实现可控的部分权限委托传递。经安全分析证明, 该机制可满足权限传递所需的可验证性、不可否认性、可区分性、可识别性和不可滥用性等安全属性, 确保了设备所有者权限的可控安全传递, 有效防止中间代理过度授权的问题。

关键词: 共享设备; 委托授权; 信任度; 代理签名

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019015

Delegation authorization mechanism with controllable permissions propagation for IoT devices sharing

SONG Yubo, QI Shanshan, HU Aiqun

School of Cyber Science and Engineering, Southeast University, Nanjing 211111, China

Abstract: In order to solve the problems of privilege sensitivity protection and the abuse of authorization by the agent when the device owner delegates authorization in IoT devices sharing environment, a trust-based delegation mechanism for controllable partial permissions was proposed with the trust access control model and the proxy signature. This mechanism generates trust values and authorization policies based on the relationship between the users, and implements controllable partial authority delegation through the proxy signature. According to the security analysis, the mechanism can meet the security attributes such as verifiability, non-repudiation, distinguishability, identifiability and non-abuse required by the permission transfer, and ensure the controllable security transfer of the

收稿日期: 2018-11-20; 修回日期: 2018-12-20

通信作者: 宋宇波, songyubo@sec.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61601113); 赛尔网络下一代互联网技术创新基金资助项目 (No.NGII20150409); 中央高校基本科研业务费专项基金资助项目 (No.2242017K40013)

Foundation Items: The National Natural Science Foundation of China (No.61601113), CERNET Innovation Project (No.NGII20150409), Fundamental Research Funds for the Central Universities (No.2242017K40013)

论文引用格式: 宋宇波, 戚姗姗, 胡爱群. 权限可控传递的物联网共享设备委托授权访问机制[J]. 网络与信息安全学报, 2019, 5(2): 40-49.

SONG Y B, QI S S, HU A Q. Delegation authorization mechanism with controllable permissions propagation for IoT devices sharing[J]. Chinese Journal of Network and Information Security, 2019, 5(2): 40-49.

device owner's permission. The problem of over authorization of an intermediary agent is effectively prevented.

Key words: devices sharing, delegation authorization, trust value, proxy signature

1 引言

随着物联网的迅速发展和智能手机的广泛使用,人们可以在任何时间、任何地点方便地访问智能设备。灵活的共享服务和设施建立了一个开放的、以个人为中心的无处不在的网络。在这个开放的物联网共享环境下,个人被鼓励以服务提供者的身份,与其他人分享他们的设施或资源,如停车场、公寓、仓库、电子储物柜、展览室等^[1]。

在一个典型的与多用户共享的公民设施中,所有者将权限分配给第一个用户,然后,第一用户可以通过社交网络将权限转移给其他用户。如果用户想要访问共享设备,将通过 Wi-Fi、蓝牙或 RFID 验证自己与智能手机的身份,然后,设备根据用户的社会属性做出访问决策^[2]。

在共享过程中,应该认真考虑以下安全问题:如何管理权限从一个用户到另一个用户的传播,如何在保护隐私的情况下验证用户的身份,如何对不同的用户进行细粒度的访问控制。传统的安全机制无法提供可控的权限传播、用户和所有者的隐私保护以及灵活的细粒度访问控制,因此需要设计新的安全机制来解决这些安全问题。

Sandhu^[3]最早提出了物联网权限管理方案,他提出了一种基于角色的访问控制模型,该模型中引入了角色的概念从而将设备所有者和其权限逻辑分离,并将权限授予角色,用户通过设备所有者为其分配的角色获得相应的权限,该模型有效地减小了授权管理的代价,并较好地实现了对授权的约束。Zhang 等^[4]基于角色的访问控制提出了一种可扩展的访问控制模型,该方案通过上下文信息对权限的访问控制的实现方法进行描述,将对象的操作转换成对服务的操作,通过收集系统和用户环境中的上下文信息对授予权

限的规则进行定义。Fu 等^[5]基于属性的访问控制提出了通过可扩展的访问控制标记语言对环境属性进行描述,设备所有者通过属性对权限和对用户的约束条件进行描述,从而在开放的物联网环境中实现基于用户身份和属性的访问控制方案。在物联网设备共享环境中,存在许多对设备所有者来说陌生的用户,当这些用户申请访问设备时,设备所有者很难直接依据其陌生的身份进行授权, Li 等^[6]基于角色的信任管理,提出了一种在开放的物联网环境中陌生用户间进行授权的方案,其核心的授权机制是通过委托实现的,但却没有很好地处理委托深度的问题。Kolev^[7]通过信任关系实现陌生用户到设备所有者权限角色的分配,同样该文也没有对委托深度的进行限制。翟征德等^[8]提出了一种基于角色细粒度的可控委托授权模型,该模型根据用户的信任度对设备所有者的敏感权限进行传播控制,但是该方案中用户间的信任度值都是由用户主观指定的,不具有通用性。

目前,对物联网共享设备的权限管理主要集中在设备所有者对用户进行直接授权管理上^[9-10],对于通过中间代理进行权限的可控传递缺乏研究,没有一个通用客观的信任度计算方法来表示用户间的信任程度。在由中间代理授权的物联网设备共享场景中设备的权限管理包括两方面^[11]:第一,设备所有者对中间代理的委托授权;第二,物联网设备对获取权限用户的访问控制。针对设备所有者委托授权时的权限敏感度保护问题,本文提出了一种基于信任度的可控的部分权限委托授权机制,设备所有者根据中间代理的信任度委托其相应范围的授权权限;针对中间代理过度授权的问题,提出了一种基于信任度的访问控制机制,该机制采用基

于角色和信任度的访问控制模型, 根据用户间的信任度和设备所有者设定的信任度阈值确定是否向访问用户授权, 该机制可以有效防止中间代理过度授权的问题。

2 基于角色和信任度的授权策略

在可委托授权的物联网设备共享场景中, 设备所有者将授权使用设备的能力委托给中间代理, 由中间代理向用户授权, 同时中间代理也可以将授权使用设备的能力委托给下一级中间代理, 依次类推, 形成了设备权限的多次委托传递。在此场景下, 存在中间代理过度授权的问题, 随着权限委托深度的增加, 距离设备所有者越远的用户, 其信任度越低, 且随着用户间关系的变化, 信任度也会动态变化, 然而设备的不同权限是存在敏感度差异的, 其中某些权限可能涉及设备所有者的隐私是具有高度敏感性的。因此为了实现设备所有者敏感权限保护, 针对不同信任度的用户释放相应的权限显得尤为重要。本文提出了一种基于动态信任度的访问控制机制, 该机制采用基于角色和信任度的访问控制模型, 根据用户的信任度和设备所有者设定的信任度阈值确定是否对访问用户授权, 从而可以防止中间代理过度授权的问题。

在物联网设备共享系统中, 将设备所有者与其权限分离, 为设备所有者设置角色, 并为不同的角色分配不同的权限, 因此角色实质上是一组权限的集合且每个角色对应的权限是存在敏感性差异的。

本文通过给每个角色对应的权限设置一个关联的信任度阈值来反映权限的隐私程度, 信任度阈值越大, 权限越敏感, 只有当某个用户获得该角色且其信任度大于角色对应的权限的信任度阈值时才可以激活该角色。在本文方案中, 用户不仅可以拥有其被分配的角色权限, 还可以继承

角色链中低于其角色的所有角色的权限。高级角色与低级角色的关系称为继承关系, 然而其中存在的问题是怎样确定高级角色从低级角色中继承来的权限的信任度阈值, 如果只是逐一地指定每个继承的权限的信任度阈值, 是不具有拓展性的, 且实现过程很烦琐。本文在角色继承关系中引进了信任度阈值衰减因子的概念, 在角色继承关系链中, 对于同一个权限, 低级角色中该权限关联的信任度阈值通过信任度阈值衰减因子后获得了高级角色中该权限对应的新的信任度阈值, 下面进行具体说明。

定义 1 用户集 $User = \{u_1, u_2, u_3, \dots\}$: 指设备所有者和想要访问设备的用户; 角色集 $Role = \{r_1, r_2, r_3, \dots\}$ 和权限集 $Permission = \{p_1, p_2, p_3, \dots\}$: 设备所有者将他的权限进行分散, 并将每个权限分配给角色。

定义 2 信任度集合 $TD = [0, 1.0]$: $t \in TD$, 信任度阈值集合 $TDT = [0, 1.0]$; 信任度阈值衰减因子集合 $TDTD = [0, 1.0]$; 用户-角色-权限-信任度集合 $URPT \subseteq User \times Role \times Permission \times TD$, 则 $(u, r, p, t) \in URPT$ 表示用户 u 以信任度大于 t 的信任度得到角色 r 并获得权限 p ; 角色链 $URL \subseteq Role \times Role$, 是由设备所有者的角色形成的树形结构。

定义 3 用户角色链: 用户的角色链是一种树形结构, 树中的每一个节点是角色, 每个角色按照对应权限敏感度大小由高到低排列, 角色链中上级角色可以继承下级角色的所有权限, 但是同一级的角色是并列的, 不可以相互继承。

以房屋共享为例对角色链的概念进行说明, 表 1 说明了房主设定的角色、对应的权限和权限的信任度阈值。

从表 1 中可以看出, 房主设定了 4 种角色, 在角色链中由低到高为 Guest、General、Close 和 VIP, 其中, General 和 Close 是并列角色。角色

Guest 可以获取房主车库的使用权 p_garage , 角色 General 获得客厅 $p_livingroom$ 和卫生间 $p_bathroom$ 的权限, 角色 Close 获得客房 $p_guestroom$ 的权限, 角色 VIP 获得书房 $p_studyroom$ 和主卧 $p_masterroom$ 的权限。具有角色 VIP 的用户可以继承角色 Guest、General 和 Close 的所有权限。从表 1 中可以看出, 主卧是一个高度涉及房主隐私的权限, 因此将它的信任度阈值设定得比较高。

表 1 房屋共享角色权限分配

角色	权限	信任度阈值
Guest	p_garage	0.3
General	$p_livingroom$	0.6
General	$p_bathroom$	0.7
Close	$p_guestroom$	0.8
VIP	$p_studyroom$	0.7
VIP	$p_masterroom$	0.92

在房主的角色链中, 角色 VIP 级别最高, General 和 Close 是同等级的角色, 没有继承关系, 角色 Guest 级别最低。角色 VIP 继承了角色 Close 的所有权限, 只获得角色 Close 的用户的信任度必须高于信任度阈值 0.8 才可以获得权限 $p_guestroom$, 那么角色 VIP 继承到的权限 $p_guestroom$ 需要设置多大的信任度阈值? 通常认为对于同一个权限, 具有角色级别高的用户比角色级别低的用户更加可信, 如对于房主而言, 父母比普通朋友更加可信, 因此可以认为获得角色 VIP 的用户可以以低于信任度阈值 0.8 的信任度获得权限 $p_guestroom$, 所以, 通过在角色链中引入信任度阈值衰减因子使高级角色继承来的低级角色的权限的信任度阈值变小是符合实际情况的。图 1 是房主设定的角色链中的信任度阈值衰减, 图中角色与角色之间边上的值是信任度阈值衰减因子。

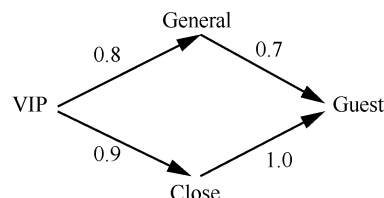


图 1 角色链上的信任度阈值衰减

在角色链中高级角色和低级角色之间权限的继承分为直接继承（如 $VIP \rightarrow Close$ ）和间接继承（如 $VIP \rightarrow Close \rightarrow Guest$ ）。用函数 $f(r_i, r_{i+1})$ 表示具有直接继承关系的角色之间的信任度阈值衰减因子, 而具有间接关系的 2 个角色间的信任度阈值衰减因子是路径中每一段直接关系的信任度阈值衰减因子的累积, 函数表示为

$$f_{accum}(r_n, r_0) = \prod_{i=n-1, \dots, 0} f(r_{i+1}, r_i), r_i \in Role$$

例如, 间接关系 $VIP \rightarrow Close \rightarrow Guest$ 的角色累积衰减因子为 $0.9 \times 1.0 = 0.9$ 。另外, 当从一个角色到另一条角色有多条路径时, 如 $VIP \rightarrow Guest$ 有 $VIP \rightarrow Close \rightarrow Guest$ 和 $VIP \rightarrow General \rightarrow Guest$ 这 2 条路径, 选择累积衰减因子最小的一条路径作为最终的信任度阈值衰减因子。本文方案中信任度阈值衰减因子是由设备所有者设置的, 如果设备所有者认为某一角色继承来的权限对该角色来说比较隐私, 就可以将衰减因子设置较大, 若希望该权限被高等级角色很容易获得, 就可以将衰减因子设置较小。

3 基于信任度的可控部分委托授权机制

物联网设备共享中常见的场景之一是通过中间代理授权的物联网设备共享平台, 在该场景下设备所有者将物联网设备委托给中间代理, 由中间代理负责向用户授予权限, 用户利用中间代理颁发的授权凭证获得设备的使用权, 整个交互过程中通过中间代理进行权限的传递, 设备所有者无须与用户进行线下的交互。中间代理可以有效解决设备所有者有自己的工作、无法实时对设备

的访问权限进行管理的问题,其可以代替设备所有者对用户的申请做出快速有效的回应,从而减轻设备所有者管理设备的负担,提高了物联网设备共享系统的效率;另外,由于设备所有者通常是向其认识或熟悉的用户分享自己的个人闲置设备,所以可获得使用权的用户范围有限,通过中间代理的集客效应可以扩大用户的范围,提高系统的实用性。

在该物联网设备共享场景下需要考虑的一个重要问题是如何实现设备所有者权限的可控传递,即如何实现设备所有者对中间代理的可控委托授权,在该场景下设备所有者对中间代理的委托授权需要满足以下性质。

1) 临时委托:设备所有者对中间代理的委托是有时间限制的,超过委托时间,中间代理的授权能力就会失效。

2) 单一性:当设备所有者委托中间代理对用户授权后,设备所有者仍可以对申请权限的用户进行授权。

3) 部分委托:由于设备所有者的权限是存在敏感性差异的,设备所有者将依据中间代理的信任度委托其相应范围的授权权限。

4) 自己管理:委托关系是由设备所有者直接管理的,其可以撤销行为表现不好的中间代理。

本文采用代理签名技术,由中间代理代替设备所有者对用户签发授权证书。中间代理的代理签名私钥由其和设备所有者共同生成,该方案可以有效实现委托授权的可验证性和不可否认性、授权者的可区分性和授权能力的不可滥用性,确保设备所有者权限的可控安全传递。

下面对本文用到的符号进行说明。

$\parallel$: 消息的串联。

ID_A : 用户 A 的身份标识。

T_A : 用户 A 生成的时间戳。

$Cert_A$: 用户 A 的证书。

$H(m)$: 散列函数。

x_A, y_A : 用户 A 的私钥和公钥。

$E_k(\cdot), D_k(\cdot)$: 消息加密和解密。

$Sign(x, m)$: 私钥 x 对消息 m 签名。

$Verify(y, m, Sign(x, m))$: 用公钥验证消息 m 的签名。

委托授权协议中的参与者包括设备所有者、中间代理、用户和物联网设备,图 2 是委托授权的流程。

接下来,对委托授权协议运行的具体步骤进行介绍。

1) 系统参数生成:生成一个大素数 p, q 是 $p-1$ 的素因子,选择 $\alpha \in Z_p^*$ 满足 $\alpha^q = 1 \bmod p$, 其中, α, p 和 q 是整个系统的公钥参数。设备所有者、中间代理、用户和物联网设备分别选择随机数 $x_o, x_p, x_u, x_d \in Z_q^*$, 其相应的公钥为 $y_o = \alpha^{x_o} \bmod p, y_d = \alpha^{x_d} \bmod p, y_u = \alpha^{x_u} \bmod p, y_d = \alpha^{x_d} \bmod p$ 。

2) 中间代理向设备所有者申请代理权。中间代理用其私钥 x_p 对其身份标识 ID_p 、社交信息 M_{SN} 和时间戳 T_p 进行签名生成数字签名 $Sign(x_p, ID_p \parallel T_p \parallel ID_p)$, 并用所有者的公钥 y_o 加密生成密文 $E_{y_o}(ID_p, M_{SN}, T_p, Sign(x_p, ID_p \parallel T_p \parallel ID_p))$ 发送给所有者进行设备代理权的申请。所有者收到申请后用其私钥 x_o 解密得到申请信息,验证该中间代理的身份是否合法以及时间戳的新鲜性。设备所有者搜索他的中间代理表查看当前是否有用户已经获取该设备的代理权,如果当前没有中间代理占用该设备,则所有者同意该用户的代理申请,然后根据该中间代理的社交信息计算对其的信任度,并根据信任度授予其相应的授权范围。设备所有者生成对中间代理的授权证书 $Cert_p = (ID_o \parallel validity \parallel T_o \parallel W, Sign(x_o, ID_o \parallel validity \parallel T_o \parallel W))$, 其中, ID_o 是所有者的身份标识, $validity$ 是所有者设置的代理权的有效时

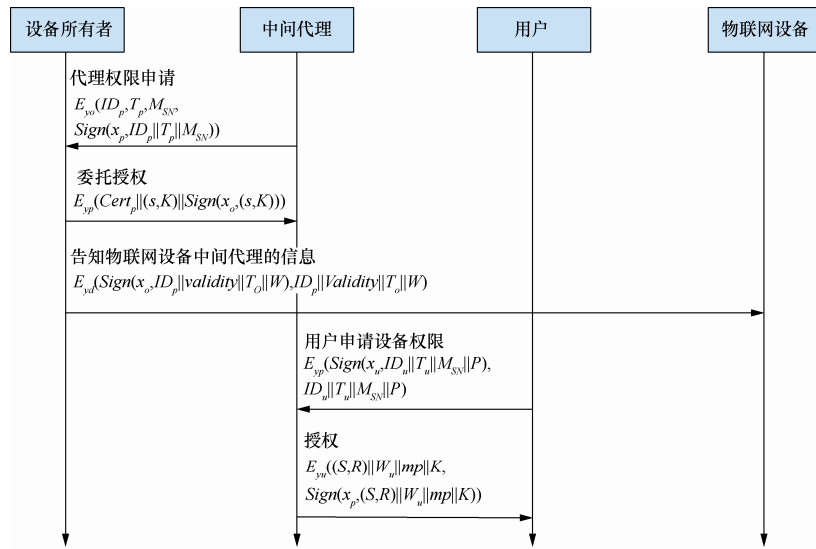


图2 委托授权流程

间, T_o 是所有者颁发证书的时间, W 是所有者的授权内容, 其中包括授予中间代理的角色及对应的权限和对他的信任度值。所有者在他的中间代理表上登记获得授权的中间代理的身份标识、代理有效时间、授权时间和授权内容等, 从而可以方便地对具有不良行为的中间代理进行追踪。最后, 所有者将获得代理权的中间代理的身份、代理有效期、授权时间等发送给物联网设备, 方便物联网设备对中间代理的身份进行验证。

3) 设备所有者选择随机值 $k \in Z_q^*$, 计算 $K = \alpha^k \bmod p$ 和 $s = x_o + kK \bmod q$, 生成代理签名密钥 (s, K) 。设备所有者对 (s, K) 进行签名, 并将授权证书 $Cert_p$ 、 (s, K) 和签名 $Sign(x_o, (s, K))$ 加密生成密文 $E_{y_p}(Cert_p, (s, K), Sign(x_o, (s, K)))$ 发送给中间代理, 通知中间代理其已经获得授权。

4) 中间代理收到所有者发送的授权消息, 得到代理签名密钥 (s, K) , 首先验证等式 $\alpha^s = y_o K^K \bmod p$ 是否成立, 其中, y_o 代表设备所有者的身份, 若成立, 则中间代理确认 (s, K) 是由设备所有者生成的代理签名密钥, 否则中间代理拒绝接受所有者的授权; 中间代理用所有者的公钥 y_o 验证授权证书的有效性, 并对授权证书进行解

析获取他的授权范围。

5) 中间代理关系网络中想要访问设备的用户将其身份标识 ID_u 、社交信息 M_{SN} 、申请的权限 P 和时间戳 T_u 发送给中间代理。中间代理对用户的身分进行验证, 判断用户申请的权限是否在自己的授权范围内, 若在, 则依据用户的社交信息 M_{SN} 计算对该用户的信任度。最后生成权限凭证 W_u , 其中包括授予用户的角色和信任度。

6) 中间代理同意用户的申请后, 计算代理签名私钥 $r = s + x_p y_p \bmod q$, 其在设备所有者生成的代理签名私钥 S 的基础上加入自己的私钥信息 x_p , 并用 r 代替 x_p 进行普通的数字签名。本文采用 ElGamal 数字签名方案对 W_u 进行签名, 中间代理计算 $m_p = H(ID_o || y_o || W_u)$, 选择随机值 $k \in Z_q^*$, 计算 $R = \alpha^t \bmod p$ 和 $S = t^{-1}(m_p - rR) \bmod q$, (R, S) 是代理签名, 其将密文 $E_{y_u}((R, S) || W_u || m_p || K, Sign(x_p, (R, S) || W_u || m_p || K))$ 发送给用户。中间代理在用户列表中记录该用户的身份和对应的权限 (ID_u, W_u) 。

7) 用户收到授权信息并验证其有效性。计算代理签名验证公钥 $h = y_o K^K y_p^{y_p} \bmod p$ 和 $m'_p = H(ID_o || y_o || W_u)$, 验证 $m'_p = m_p$ 是否成立,

若成立, 则用代理签名验证公钥 h 对收到的代理签名进行验证, 判断 $Verify(h, W_u, (S, R))=1$, 即 $\alpha^{m_p} = R^S h^R \bmod p$ 是否成立, 若该等式成立, 则用户认为该中间代理的身份是合法的, 并接受授权凭证。

4 基于信任度的访问控制

在一个角色链中等级高的角色可以继承等级低的角色的权限, 并且为了保护物主敏感度高的权限, 对每个权限设置信任度阈值, 只要获得该角色的用户的信任度大于对应权限的信任度阈值时就可以激活角色的访问权限。根据信任关系类型, 将用户划分为直接关系用户和间接关系用户。

直接关系用户与物主认识, 其可以与物主直接建立联系, 他向物主发出访问请求并将其社交文件和申请的权限 p 发送给物主, 物主计算对该用户的社交信任度值 t , 然后根据用户申请的权限和信任度值的大小向其分配角色 r 。物主生成授权凭证 $Cert_u = (E_{y_d}(r, t, p, Sign(x_o, r \| t \| p)))$ 发送给直接关系用户, 该授权证书中包含物主分配给该用户的角色 r 、申请的权限 p 以及对该用户的信任度 t , 物主用私钥 x_o 对 (r, p, t) 签名并用设备的公钥 y_d 加密, 直接关系用户收到授权凭证后

是无法打开授权凭证的, 目的是防止用户伪造角色和信任度值。用户将授权凭证转发给设备, 设备获得该用户的角色、权限和信任度后, 检索用户的角色并将其信任度与角色中用户申请的权限的信任度阈值相比较, 然后释放权限。

在开放的物联网环境中, 想要获取设备使用权的用户也可能是设备所有者陌生的用户, 他无法与物主直接建立联系, 但是他可以通过一个或多个“中介”间接地向物主申请权限, 因此形成了一个以物主为核心的关系网络。图3给出本文假设的关系, 图中的节点表示用户, 通过边相连的用户是相互认识的。

图3中用户 B 、 C 、 D 通过用户 A 与房主建立联系, 用户 E 、 F 、 G 通过用户 B 再通过用户 A 与物主建立联系, 用户 H 、 I 通过用户 E 再通过用户 B 、用户 A 与房主建立联系。从而分别形成了以用户 A 、 B 、 C 为中心的代理域, 相当于形成了物主权限的多级代理传递, 其中, 用户 A 、 B 、 C 称为各自域的管理员, 物主本身也形成一个管理域, 他们域中的成员是各自下一级的用户。每个域管理员只能对其域内的成员颁发授权凭证 $Cert_{p \rightarrow u} = (E_{y_d}(r, t, p, Sign(x, r \| t \| p)))$, 表明该成员获得的角色、权限和信任度, 其中, 域内成员不能对授权凭证进行解析。物主域外的用户, 即

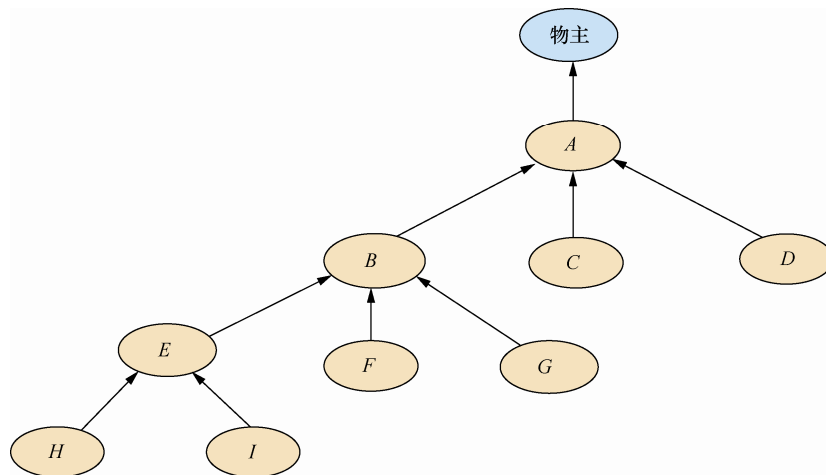


图3 用户关系

不与物主直接关联的用户是无法得到物主颁发的授权凭证的,间接用户得到的是一个授权凭证链,其中包含间接用户到物主的关系链中每个域管理员向其成员颁发的授权凭证。例如,用户H想要获得房屋的某个权限,其获得的授权凭证链是 $(Cert_{M \rightarrow A}, Cert_{A \rightarrow B}, Cert_{B \rightarrow E}, Cert_{E \rightarrow H})$,其中的信任度是由上级用户根据与下级用户的社交相似性计算而来。间接用户获得的授权凭证链是一个简单的线性结构,其综合信任度是由设备根据证书凭证链中每个凭证中包含的信任度值综合计算而来。设函数 $trust$ 计算2个直接关系用户间的基于动态关系的信任度,用函数 $path$ 计算关系链 $u_n \leftarrow u_0$ 中 u_0 对 u_n 的信任度,其中包含的直接关系为 $u_n \leftarrow u_{n-1}, u_{n-1} \leftarrow u_{n-2}, \dots, u_1 \leftarrow u_0$ 。

$$path(u_n \leftarrow u_0) = \begin{cases} trust(u_1 \leftarrow u_0), & n=1 \\ f(path(u_n \leftarrow u_{n-1}), trust(u_{n-1} \leftarrow u_0)), & n>1 \end{cases}$$

f 是房屋智能锁系统综合计算用户信任度的函数,其应满足2个条件:第一,对于函数 f ,输入任何合法的信任度后,输出的是新的合法的可信度,即对于 $\forall t_1, t_2 \in [0,1]$,满足 $f(t_1, t_2) \in [0,1]$;第二, f 输出的信任度不大于输入的任意的信任度,即随着权限传递的深度增加,获得权限用户的信任度是衰减的。因此,满足上述条件的 f 函数有乘法算法和取最小值算法。对于乘法算法,智能锁系统将用户授权凭证链中每个凭证中的信任度相乘;而对于取最小值算法,则选择授权凭证链中最小的信任度值作为间接用户的综合信任度。

综上所述,用户最终获取角色的信任度值取决于权限传递链中每一段直接关系间的信任度,且权限越往下传递,用户的信任度是衰减的,离物主关系越远的用户获得物主角色权限的可能性越低。本文方案实现了物联网设备共享环境中物主权限的可控传递,实现了对不同信任度用户的访问控制。同时,用户间的信任度不是固定不变

的,而是在一段时间内随用户间的关系变化而动态变化的,直接或间接用户最终获得的信任度也是动态变化的,因此,用户在不同时间访问设备时可能获得不同的访问权限。

5 安全性分析

委托授权过程的本质是代理签名技术的应用,而一个安全的代理签名方案需要满足可验证性、不可否认性、可区分性、可识别性和不可滥用性等安全属性,本文根据这些属性对所有委托授权协议的安全性进行分析。

1) 可验证性

可验证性是指用户根据系统的公开参数和代理签名对代理签名的正确性以及中间代理身份的有效性进行验证。本文方案中验证等式 $Verify(h, W_u, (S, R))=1$ 是否成立,如果成立,则说明代理签名是有效的且中间代理的身份是合法的。用户在验证代理签名时使用的验证公钥 h 中既包含所有者的公钥 y_o ,又包含中间代理的公钥 y_p ,并且他们是满足特定关系的,即验证代理签名的公钥只有在设备所有者和中间代理的共同授权下才可以生成,因此用户会相信该代理签名是合法的。 ID_o 和 y_o 是设备所有者的公开信息,用户已经事先知道,他收到中间代理的授权信息后首先验证 $m_p = H(ID_o \parallel y_o \parallel W_u)$ 是否成立,若成立,则对代理签名的有效性进行验证,证明如下。

$$\begin{aligned} h &= y_o K^K y_p^{y_p} \bmod p = \alpha^{x_o} \alpha^{kK} \alpha^{x_p y_p} \bmod p = \\ &\alpha^{x_o + kK + x_p y_p} \bmod p = \alpha^r \bmod p \\ V_1 &= \alpha^{m_p} \bmod q \\ V_2 &= R^S h^R \bmod p = (\alpha^t)^{t^{-1}(m_p - rR)} \cdot (\alpha^r)^R \bmod p = \\ &\alpha^{m_p - rR + rR} \bmod p = \alpha^{m_p} \bmod p = V_1 \end{aligned}$$

2) 不可否认性

中间代理的代理签名私钥是 $r = s + x_p y_p \bmod q = x_o + kK + x_p y_p \bmod q$,其中同时包含

设备所有者和中间代理的私钥信息，因此设备所有者不能否认是他授权中间代理对消息进行签名，而中间代理也不能否认该代理签名是由其生成的，二者都不能对委托授权的过程做出抵赖。

3) 不可伪造性

代理签名私钥中包含中间代理的私钥信息，而该私钥只能由中间代理掌握，因此任何人都不能伪造出有效的代理签名；另外由代理签名验证公钥 $h = y_o K^K y_p^{y_p} \bmod p = \alpha^r \bmod p$ 求出代理签名私钥 r ，需要计算离散对数问题，在本文方案中求解离散对数问题是困难的，所以，除了中间代理，包括设备所有者在内都无法以中间代理的名义生成有效的代理签名。

4) 可识别性

由于在代理签名私钥中包含中间代理的私钥，因此只有利用中间代理的公钥才能生成正确的代理签名验证公钥，从而对代理签名的有效性进行验证。任何得到代理签名的用户都可以通过中间代理的公钥确定中间代理的真实身份。

5) 不可滥用性

可能存在中间代理将代理签名私钥 $s = x_o + kK \bmod q$ 分享给其他用户进行授权的情况，代理签名私钥中只包含设备所有者的私钥信息，因此当出现纠纷时，中间代理可以否认该签名是由他生成的并且可以说是由设备所有者生成的，目的是掩盖滥用代理权限的事实。在本文方案中， $r = s + x_p y_p \bmod q = x_o + k \cdot \alpha^k + x_p y_p \bmod q$ ，中间代理如果要伪造有效的代理签名私钥，需要知道 x_o 和 k ，这需要通过求解离散对数问题才能得到，而在本文方案中求解离散对数问题是困难的。

6) 强密钥依赖性

中间代理签名时的代理签名私钥依赖于设备所有者的私钥和中间代理的私钥。

综上所述，本文方案具有更高的安全性和实现

效率，并且计算量小和通信复杂度低。该方案可以实现委托授权时设备所有者权限的可控传递，有效解决当设备的使用出现纠纷问题时，设备所有者和中间代理相互抵赖的问题；另外，该方案还根据由中间代理的用户关系计算的信任度授予其相应的授权范围，保护了设备所有者的敏感权限。

6 结束语

本文主要介绍了基于信任度的委托授权和访问控制方案，首先针对物联网设备共享场景中设备所有者委托授权时权限敏感度保护的问题，提出了一种基于信任度可控的部分权限委托授权机制，中间代理在设备所有者许可范围内将部分被委托的权限授权给用户，其使用的代理签名私钥由设备所有者和中间代理共同生成，防止设备所有者和中间代理相互抵赖的问题，提供了权限敏感度保护；针对用户访问物联网设备时中间代理过度授权的问题，提出了一种基于信任度的访问控制机制，该机制采用基于角色和信任度的访问控制模型，根据用户动态关系所生成的信任度和设备所有者设定的信任度阈值确定是否授权。

参考文献：

- [1] JIN J, GUBBI J, MARUSIC S, et al. An information framework for creating a smart city through Internet of things[J]. IEEE Internet of Things Journal, 2016, 1(2): 112-121.
- [2] MC-KINLAY P. Make way for smart cities: opportunities, challenges and capacities of New Zealand local governments[J]. Asia Pacific Journal of Public Administration, 2017, 39(4): 297-303.
- [3] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control models[J]. Computer, 1996, 29(2): 38-47.
- [4] ZHANG G, TIAN J. An extended role based access control model for the Internet of things[C]//2010 International Conference on Information Networking and Automation (ICINA). 2010: 319-323.
- [5] FU Y, YE C. Using XACML to define access control policy in information system[C]//IET Conference on Wireless, Mobile and Sensor Networks (CCWMSN 17). 2017: 676-679.
- [6] LI N, WINSBOROUGH W H, MITCHELL J C. Distributed cre-

dential chain discovery in trust management: extended abstract[C]//ACM Conference on Computer and Communications Security. 2016: 156-165.

- [7] KOLEV A, ČOBANOV S. Trustbac—integrating trust relationships into the rbac model for access control in open systems[C]//ACM Symposium on Access Control Models and Technologies. 2016: 49-58.
- [8] 翟征德, 冯登国, 徐震. 细粒度的基于信任度的可控委托授权模型[J]. 软件学报, 2017, 18(8).
ZHAI Z D, FENG D G, XU Z. Fine-grained controllable delegation authorization model based on trustworthiness[J]. Journal of Software, 2017, 18(8).
- [9] YU J, WANG G, MU Y, et al. An efficient generic framework for three-factor authentication with provably secure instantiation[J]. IEEE Transactions on Information Forensics and Security, 2016, 9(12): 2302-2313.
- [10] XUE K, MA C, HONG P, et al. A temporal credential based mutual authentication and key agreement scheme for wireless sensor networks[J]. Journal of Network and Computer Applications, 2017, 36(1): 316-323.
- [11] JIANG Q, MA J, LU X, et al. An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks[J]. Peer-to-Peer Networking and Applications, 2016, 8(6): 1070-1081.

[作者简介]



宋宇波(1977-), 男, 江苏无锡人, 博士, 东南大学网络空间安全学院副教授, 主要研究方向为移动通信安全, 物联网安全及安全协议设计。



戚姗姗(1992-), 女, 浙江余姚人, 东南大学博士生, 主要研究方向为物联网安全。



胡爱群(1952-), 男, 江苏南通人, 博士, 东南大学教授, 主要研究方向为通信网络安全。