物联网感知层基于资源分层的多用户访问控制方案

马 骏[1,2],郭渊博[2],马建峰[1,3],刘西蒙[1],李 琦[1]
(1.西安电子科技大学计算机学院,陕西西安 710071;2.解放军信息工程大学,河南郑州 450004;
3.西安电子科技大学陕西省网络与系统安全重点实验室,陕西西安 710071)

摘 要: 针对物联网感知层节点计算、存储能力受限情况下,多用户安全高效的资源访问需求,提出一种分层访问控制方案.将提供同级别资源的节点划分为一个层次节点,利用层次节点之间形成的偏序关系,设计了安全高效的密钥推导算法,使用户在掌握单个密钥材料的情况下,能够访问更多层次资源.同时引入 Merkle 树机制,使多个用户通过相互独立的哈希链,安全高效的获取层次节点的密钥材料.方案在存储开销、计算开销、可证明安全和可扩展方面,比现有类似方案更适合多用户在物联网感知层环境下资源的访问.

关键词: 物联网; 感知层; 访问控制; 资源分层; 可证明安全
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2014)01-0028-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.01.005

Multi-User Access Control Scheme Based on Resources Hierarchies for Perceptual Layer of IoT

MA Jun[1,2], GUO Yuan-bo[2], MA Jian-feng[1,2], LIU Xi-meng[1], LI Qi[1]
(1. *School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi* 710071, *China*; 2. *PLA Information Engineering University, Zhengzhou, Henan* 450004, *China*; 3. *Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: A novel hierarchical access control scheme for perceptual layer of the IoT is presented based on resources hierarchies, which could conform to the secure and efficient access requirement of multi-user. In the scheme, every hierarchical node is composed of perceptual nodes which provide resources with the same levels of security. More hierarchical nodes can be modeled as a set of partially ordered classes. With this mode, a deterministic key derivation algorithm is designed, which makes every user and perceptual node possesses a single key material to get some keys, and obtains the resources at the presented class and all descendant classes in the hierarchy. Furthermore, a mechanism of Merkle tree is introduced to guarantee secure and efficient multi-user key material derivation by independent of each hash link. Compared with previous proposals, the scheme is more suitable for multi-user to access resources of perceptual layer in IoT.

Key words: internet of things; perceptual layer; access control; resources hierarchies; provable security

1 引言

物联网(Internet of Thing, IoT)是指按照约定的协议,通过信息传感设备,将任何物品(Thing)与互联网(Internet)进行连接,完成信息交换和通信,以实现物品的智能化识别、跟踪、定位、监控和管理的一种网络[1].物联网作为继互联网之后的又一次信息技术革命,在实现人-人和人-机互联基础上,进一步增加了人-物、物-物互联,是互联网技术的延伸和扩展,且更加突出了随时随地的信息采集、感知功能.国内外学者普遍认为由 RFID、传感器等技术构成的物联网感知层,是物联网体系的重要组成部分,其主要作用是利用传感器节点完成海量信息的采集工作[2~6].考虑到数据访问安全、隐私、定制等应用需求,以及感知层节点存储和计算能力受限

收稿日期:2013-07-08;修回日期:2013-10-03;责任编辑:孙瑶
基金项目:长江学者和创新团队发展计划(No.IRT1078);国家自然基金委员会-广东联合基金重点基金(No.U1135002);国家科技重大专项(No.2011ZX03005-002);国家自然科学基金(No.61170251);国家 863 高技术研究发展计划(No.2012AA013102);中央高校基本科研业务费(No.JY10000903001)

的环境需求,对采集信息展开有效的访问控制是物联网发展面临的主要挑战之一[7].

1.1 问题的提出

大多数应用场景中,感知层节点采集到的信息往往受到节点密钥保护,想要访问该资源时,用户需要向CA(Central Authority)申请获得相应的密钥,然后进行解密操作,解密成功才能访问,否则被拒绝访问.用户每进行一次访问均需要与CA进行交互,随着访问节点数的增多,用户不仅需要保存大量的密钥,还需要频繁的与CA通信,这给用户存储和网络通信开销造成负担的同时,也会带来DDos攻击、中间人攻击等安全威胁.如何减少用户与CA通信,同时尽可能访问更多受保护的节点资源是本文考虑的问题之一.

多个用户访问同一感知层节点保护的资源时,都需要得到访问该节点的密钥,一旦某个用户遭受敌手攻击而使节点密钥失效,其他用户均无法正常访问.如何保证多用户安全有效的访问也是需要考虑的问题.

1.2 相关背景研究

针对上文提出的第一个问题,研究人员通常采用划分等级的分层访问控制方案.通过与CA的一次交互,用户能够利用得到的密钥访问对应层次的信息资源,并利用层次间的偏序关系,获得该层级别以下的所有层次密钥,从而尽可能更多的访问多个层次的信息资源.自Akl、Taylor[8]开创性的提出基于密码学方式的分层访问控制方案,研究人员结合不同的应用背景和安全需求,纷纷提出不同的分层访问控制方案:利用离散对数求解难题[9,10]和大素数分解难题[11,12]构造分层访问控制方案,具有较好的扩展性;文献[13~15]将中国剩余定理引入分层层次访问控制方案,具有较好的存储能力和较为简单的密钥推导过程;利用单向散列函数构造分层密钥推导算法[16~23],设计轻量级的分层访问控制方案,不仅能够减少对节点计算能力和存储能力的要求,又具备动态的可扩展性,是目前主流分层访问控制方案的设计思路.然而考虑到物联网感知层特殊的环境需求,现有的分层访问控制方案无法直接应用到物联网感知层环境:基于大素数分解和离散对数求解难题的方案存在存储开销和计算开销过大的问题,不适合资源受限的物联网感知层环境;基于中国剩余定理的方案由于动态扩展性差,不适合感知节点动态变化且数量庞大的访问控制需求;虽然单向散列函数的方案具有计算、存储和可扩展的优势,适用于物联网感知层环境,但也可能存在方案设计不合理,导致如文献[16,17]遭受共谋攻击的风险.

在划分层次的基础上,实现多用户的访问控制通常会采用基于RBAC的访问控制方案[24,25],然而考虑到物联网感知层环境,节点的主要目的是采集海量信息资源,对用户而言是通过有效的密钥访问相应节点资源,即层次节点仅允许用户进行"读"取资源,或拒绝用户"读"操作,策略相对简单,这就使传统的RBAC并不适合物联网感知层的访问控制.此外基于ABAC的访问控制方案[26~28],虽然具有细粒度的访问控制优势,但由于其通常采用计算相对复杂的模数运算,并不适合物联网感知层节点计算能力有限的需求.

1.3 文章主要工作

本文的主要工作体现在:(1)提出物联网感知层分层访问控制模型,以及针对该模型的安全威胁模型;(2)设计可证明安全且动态可扩展的分层访问控制方案;(3)给出高效的多用户访问解决方案.与其他类似方案相比[18~23],本文的先进性体现在:(1)多用户访问中,每个用户仅需要掌握单个用户密钥,通过简单计算,即能得到相应感知层节点的密钥材料;(2)每个感知层节点仅需要存储单个密钥材料,密钥值由密钥材料推导得到,增加了节点的安全性;(3)在标准模型下方案是可证明安全的;(4)方案支持感知层节点密钥的动态更新;(5)方案支持层次的动态扩展.

2 预备知识

安全参数.设 κ 为二进制字符串的长度,为安全起见,一般情况下 $\kappa=160$,表示随机二进制字符串的长度为160.

偏序与覆盖　设集合 $V=\{v_1,v_2,\cdots,v_n\}$,如果存在一种二元关系,使 $<v_i,v_j>$ 满足自反、反对称、传递特性,我们称集合 V 具有偏序关系,记做 $v_i\leq v_j$.如果 $<v_i,v_j>$ 之间,不存在任意的 v_k,使得 $<v_i,v_k>$ 和 $<v_k,v_j>$ 成立,则称 $<v_i,v_j>$ 是一个覆盖,记做 $v_i<\cdot v_j$.其中 $v_i,v_j,v_k\in V$.

伪随机函数簇$\{f_v\}$　指带密钥值 v 的哈希函数集合,可表示为 $f(v,m)$;当密钥值固定时,可表示为 $f(m)$.本文定义的$\{f_v\}$符合文献[29]的标准,用于完成本文设计方案中加密操作.

对称密钥加密方法　设 ε 是一个概率多项式时间算法(Gen,E,D)的三元组,密钥生成算法 Gen 用安全参数 1^k 作为输入,输出 sk;加密算法 E 将 sk 和明文消息 m 作为输入,并输出密文 c,记为 $c\leftarrow E_{sk}(m)$;解密算法 D 把 sk 和密文 c 作为输入,输出一个消息 m,记为 $m\leftarrow D_{sk}(c)$,如果解密失败记作$\perp$;

Merkle哈希树MH　是一个完全二叉树.树的每一个叶结点是用户密钥的哈希值、每个父结点下面的所有子结点的哈希值组合到一起再进行哈希运算就得到它们的父结点;这个过程一直进行下去直至得到树的根结点,即密钥材料.本文定义的 MH 符合文献[30]的

标准,用于完成本文设计方案中用户密钥与层次密钥材料多对一的构造.

可忽略函数 *negl*(*k*) 对于一个实函数 $negl(k)$,对 $\forall\ c>0$,如果 $\exists\ k_c>0$,使得 $negl(k)<k^{-c}$ 对于所有的 $k>k_c$ 都成立,则称 $ngel(k)$ 可忽略.

符号定义 v_i 表示第 i 层次节点;k_i、sk_i 和 dk_i 分别表示第 i 层对应的密钥材料、层次保护密钥和推导密钥;uk_i 表示能够通过计算获得第 i 层密钥材料的用户密钥;$\Gamma(Setup, Derivation)$ 表示本文设计的访问控制方案;A_{out} 和 A_{in} 分别表示能够针对本文方案展开攻击的两类敌手.

3 方案的提出

3.1 分层访问控制模型

将物联网感知层提供资源的感知节点按安全级别进行划分,将相同安全级别的节点划分为一个层次,我们称为层次节点.层次节点之间根据安全分级构成偏序或覆盖关系,可通过有向无环图表示.设 DAG $G=(V,E,S)$ 是一个有向无环图,其中 $V=\{v_1,v_2,\cdots,v_n\}$,表示 G 的节点集合,每个节点 v_i 代表一个层次节点;$E=\{e_1,e_2,\cdots,e_k\}$,表示 G 的有向边的集合,每条有向边 e_i 连接的两个层次节点之间具有覆盖关系;$S=\{s_1,s_2,\cdots,s_j\}$,表示当前级别的层次节点包含的感知节点集合,可以用函数 $\xi: V\to 2^S$ 表示,并且存在 $\forall\ v_i,v_j\in V$,如果 $v_i\neq v_j$,则 $\xi(v_i)\cap\xi(v_j)=\varnothing$.

该模型下,用户对物联网感知层的访问:当用户想要访问 v_i 层次节点的资源,首先从 CA 处获得合法的用户密钥,然后结合公开信息计算得到授权层次节点的密钥.接着利用公共边信息 E 得到与 v_i 构成偏序关系的层次节点集合,进而通过密钥推导算法得到层次节点 v_i 的密钥,最终访问该层受保护的资源.只要存在 $e_j\in E$ 满足从授权层次节点开始到其他层次节点的有向路径,均可通过公开的 e_j 利用重复的密钥推导算法获得下层密钥,从而使该用户能够访问更多层次资源.

3.2 安全威胁模型

为了保证物联网感知层节点采集到信息资源的机密性,通常情况下不允许未授权的用户进行访问,然而敌手可通过猜测用户密钥,利用掌握的公共信息试图获取层次节点资源的密钥,使该分层访问控制模型受到威胁;另外,对于授权用户,为了获得更多资源,可能通过多个用户的共谋,试图获得非授权的层次节点密钥,同样使分层访问控制模型存在安全风险.针对两类敌手威胁,我们定义内部攻击、外部攻击两类安全威胁模型:

(1)外部攻击:敌手允许查询物联网感知层公共信息,能够利用掌握的用户密钥,有目的选择任意多的层次节点 v_i,并获得相应的密钥.攻陷分层访问控制模型的方式是利用掌握的用户密钥成功恢复节点 v_m 的密钥 k_m,其中 v_m 与 v_i 不构成偏序关系.

(2)内部攻击:敌手允许查询物联网感知层公共信息,能够获得部分节点 $\{v_i\}$ 的密钥,猜测得到 k_m'.攻陷分层访问控制模型的方式是挑战者能够成功区分 k_m' 是否是真正的 v_m 密钥 k_m,还是与 k_m 等长的一串随机数.

3.3 提出的访问控制方案

3.3.1 方案的初始化构造

给出分层访问控制模型 $G=(V,E)$ 和安全参数 κ,取 G 中每个层次节点 $v_i\in V$,随机选取密钥材料 $k_i\in\{0,1\}^\kappa$ 分配给 v_i.需要注意的是本文设计的方案并未使 v_i 直接存储保护本层资源的密钥 sk_i,其目的是防止因单个密钥既用来保护本层资源,又用于推导下层密钥导致诸如文献[16,17]中受到内部攻击而使方案失效.此外,v_i 仅保存密钥材料 k_i 也便于多个用户持有不同的 uk_i 建立与 k_i 多对一的关系.

利用密钥材料 k_i 计算 $sk_i=f(k_i\parallel R_1)$,作为本层资源保护密钥;计算 $dk_i=f(k_i\parallel R_2)$,作为对称密钥,为 $e_{ij}=<v_i,v_j>$ 进行加解密操作.对于 G 中每条有向边 $e_{ij}\in E$,$e_{ij}=<v_i,v_j>$,利用得到的 dk_i,计算 $e_{ij}=E_{dk_i}(k_j\parallel R_3)$.其中"$\parallel$"表示连接符,$R_1,R_2,R_3\in\{0,1\}^\kappa$.

利用 CA 构造的 *MH* 可建立用户密钥 uk 与密钥材料 k_i 之间的对应关系,即 $k_i\leftarrow MH(uk_1,hl_1)$,$k_i\leftarrow MH(uk_2,hl_2),\cdots,k_i\leftarrow MH(uk_n,hl_n)$.其中,$uk_i$ 作为 *MH* 的叶子节点和唯一的一条哈希链 hl_i 对应.对于每一条哈希链 hl_i,使用 uk_i 进行加密操作,即计算 $l_i=E_{uk_i}(hl_i\parallel R_4)$,其中 $R_4\in\{0,1\}^\kappa$.

通过以上计算,uk_i,k_i 作为私密信息分别被用户和层次节点保存,l_i 和 e_{ij} 作为公共信息发布到感知层网络.

3.3.2 层次密钥获取

当一个用户访问感知层网络资源时,首先需要从 CA 获得有效的 uk_i.此阶段用户的目标是,通过保存的用户密钥 uk_i 和掌握的公共信息 l_i,得到层次节点 v_i 的密钥材料 k_i.根据给定 Merkle 哈希树 *MH* 和用户已掌握的感知层络公共信息,做如算法 1 的计算.

算法 1 用户获取层次密钥

```
for(int j=0, j<n, j++)
  {
  hl_i ∥ R_4 = D_{uk_i}(l_j);
  if  ture
  return  hl_i = hl_j;
  break;
  }
  compute  k_i ← MH(uk_i, hl_i);
```

该算法中,n 表示 Merkle 哈希树 MH 叶子节点的个数,考虑到 uk_i 和唯一的一条哈希链 hl_i 对应,因此至多通过 n 次 l_j 的解密运算可得到 hl_i,然后可通过构造的 MH 进行$\lceil \log_2^n \rceil + 1$ 次哈希运算得到层次密钥材料 k_i. 如果 n 次解密运算均失败,说明当前 uk_i 失效. 如图 1 是 $n=8$ 时层次密钥获取示例.

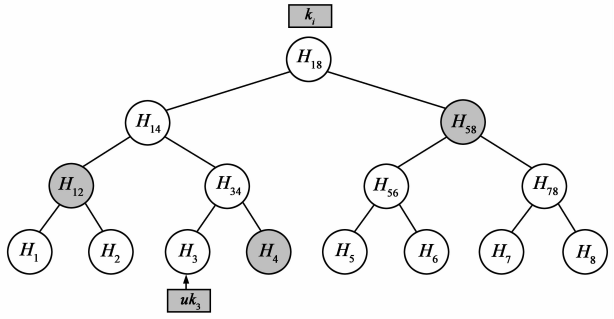


图1　基于Merkle哈希树的层次密钥获取

图 1 中,uk_3 是用户从 CA 处获得的用户密钥,$hl_3 = \{H_4, H_{12}, H_{58}\}$由 CA 通过 uk_3 加密得到 l_3 作为公共信息发布,$l_3 = E_{uk_3}(hl_3 \parallel R_4)$. 用户利用算法 1 计算 k_i 的过程如下:

(1)至多进行 8 次 l_3 的解密运算可得到 hl_3,即 $(hl_3 \parallel R_4) \leftarrow D_{uk_3}(l_3)$;

(2)计算 $H_3 = f(uk_3)$;

(3)利用 $hl_3 = \{H_4, H_{12}, H_{58}\}$,计算 $k_i = f(f(f(H_3 \parallel H_4) \parallel H_{12}) \parallel H_{58})$,返回 k_i.

3.3.3　密钥推导

用户通过上述计算可获得层次节点 v_i 的密钥材料 k_i,并能在给定的访问控制模型 G 下,获得 CA 发布的公共边信息 $e_{ij} = <v_i, v_j>$(其中 $v_i \leq v_j$). 该阶段用户的目标是通过掌握的密钥材料和公共信息利用设计的密钥推导算法获得下层节点 v_j 的密钥材料 k_j,从而计算访问 v_j 的保护密钥. 设计的密钥推导算法如算法 2.

算法 2　密钥推导算法

```
if <v_i, v_j> ∈ ∅, return ⊥;
else if v_i = = v_j, return k_i = k_i;
        compute sk_i = f(k_i ‖ R_1);
    else
        do{
            dk_i = f(k_i ‖ R_2);
            get v_m ≺ · v_i, (k_m ‖ R_3) ← D_{dk_i}(e_im);
            if true, return k_m;
            v_i = v_m, k_i = k_m;
        }while(v_i = = v_j)
        compute sk_j = f(k_j ‖ R_1);
```

该密钥推导算法中,用户仅需掌握层次节点 v_i 的密钥材料 k_i,从公共信息中找到与之形成覆盖关系的层次节点 v_m,利用计算得到推导密钥 dk_i 对 e_{im} 进行解密操作,从而得到层次节点 v_m 的密钥材料 k_m. 循环进行该步骤即能推导出目标层次节点 v_j 的密钥材料 k_j,进而计算保护密钥 sk_j. 该算法在推导过程中不产生中间层次节点的保护密钥,减少了推导算法的安全风险. 此外,该推导算法只要符合访问控制模型 G 的特性,并不限于树状分层结构. 如图 2 是一个应用算法 2 进行推导密钥的示例.

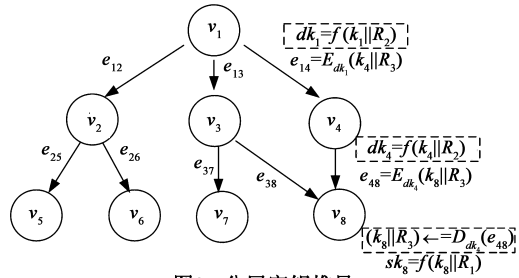


图2　分层密钥推导

上图中,假设用户通过算法 1 已获得层次节点 v_1 的密钥材料 k_1,用户想要继续访问层次节点 v_8 采集到的信息,利用算法 2 和发布的 $<v_1, v_8>$ 公共边信息,通过 2 次循环密钥推导即可得到 v_8 的保护密钥 sk_8,进而访问 v_8 资源.

3.4　方案的动态可扩展

分层访问控制方案的动态可扩展,包括层次结点的增加、删除,层次关系的动态变化,层次节点密钥材料更新;以及访问用户的动态扩展,包括用户的增加和用户密钥的更新.

(1)层次节点的密钥材料更新

本文设计的分层访问控制方案中,某个层次节点的密钥材料更新并不影响其他层次节点的密钥材料. 不会出现诸如文献[18,19]中,以当前层次节点为根的树状结构,所有层次节点密钥材料都须更新的情况. 本方案的密钥材料更新方法更加简单高效. 以图 2 为例,假设层次节点 v_2 需要更新密钥材料,则操作步骤如下:

步骤 1　从 CA 处随机选取相应的密钥材料 $k_2' \in \{0,1\}^{\kappa}$,并计算 $sk_2' = f(k_2' \parallel R_2')$,生成新的本层保护密钥;计算 $dk_2' = f(k_2' \parallel R_2')$,生成公共边的对称密钥.

步骤 2　因 k_2' 已更新,需要更新与 k_2' 相关的所有公共边信息. 即依次更新指向层次节点 v_2 的公共边和 v_2 指向其他层次节点的公共边信息. 图 2 中需要更新的公共边信息有 $e_{12} = E_{dk_1}(k_2' \parallel R_3')$、$e_{25} = E_{dk_2'}(k_5 \parallel R_3)$ 和 $e_{26} = E_{dk_2'}(k_6 \parallel R_3)$;

步骤 3　将更新后的公共信息进行发布,私有信息

由更新的层次节点保存.

(2)层次关系的动态增加、删除

层次关系的增加,即增加公共边,需要两个层次节点之间构成覆盖关系.本方案中,需要的参数包括下层节点的密钥材料,以及上层节点用于加密下层密钥材料的对称密钥.如果两个层次节点之间构成偏序关系,则依次将该路径中构成覆盖关系的层次节点之间添加公共边信息.仍以图 2 为例,如果增加的公共边信息为 e_{16},操作步骤如下:

步骤 1 计算 $dk_1 = f(k_1 \| R_2)$,然后计算 $e_{16} = E_{dk_1}(k_6 \| R_3)$;

步骤 2 将 e_{16}作为公共信息进行发布.

层次关系的删除,即删掉公共边,需要解除两个层次节点之间的覆盖关系,同时还要防止用户利用过时的公共边信息进行资源的错误访问.该删除操作的实质是将加密公共边的对称密钥进行更新操作,使掌握过时对称密钥的用户无法正常解密.值得注意的是,该更新过程中我们并未更新上层节点保存的密钥材料.仍以图 2 为例,假设删除 e_{14},则操作步骤如下:

步骤 1 更新 $dk_1' = f(k_1 \| R_2')$,但不需要进一步计算 e_{14};

步骤 2 发布 e_{14}过期信息.

(3)层次节点的增加、删除

如需增加一个层次节点,即与现有层次节点建立偏序关系,其操作过程可看作是先执行(1)中的步骤 1,然后执行(2)中的增加公共边操作即可;如需删除一层次节点,只需要将连接到该层次节点的所有公共边进行(2)中的删除公共边操作即可,完成后由 CA 发布该节点密钥材料失效通知.

(4)访问用户的动态扩展

本文采用 Merkle 哈希树构造了多用户的访问控制,新用户增加和用户密钥的更新均可通过 CA 随机选择未分配的叶子节点与用户建立新的对应关系,即为用户建立(更新)新的用户密钥.由于每个用户密钥和哈希链都相互独立,使得此操作并不影响其他用户的正常访问.

以上多用户的动态扩展,操作简单高效,但可能面临 Merkle 哈希树资源耗尽的风险.针对 Merkle 哈希树的动态扩展,文献[31]已给出成熟的解决方案,本文不过多敷述.

3.5 方案的可证明安全

为了验证设计方案的安全性,本文参考文献[32]的构造思想:利用单向散列函数的不可逆性和对称密码选择明文攻击的安全性两个方面,构造分层访问控制方案,并验证其是可证明安全的.

令 Γ(*Setup*, *Derivation*)表示分层访问控制方案,其中 *Setup* 表示方案的初始化,*Derivation* 表示密钥材料获取过程.通过建立敌手模型的不同,分别给出命题并验证其是可证明安全的.

3.5.1 敌手模型和系统目标

根据前文定义的安全威胁模型,将敌手 A 的攻击能力分为两类:

(1)A_{out}:通过询问挑战者得到 G 中公共信息 $Pub = \{l_i, e_{ij}\}$,掌握部分层次节点$\{v_i\}$对应的用户密钥$\{uk_i\}$.能够有针对性的选择任意一个层次节点 v_j(其中 v_j 与 v_i 不构成偏序关系),并询问挑战者取得相应的用户密钥,进而推导出密钥材料 k_j'.该敌手成功攻陷方案的方式是能够恢复节点 v_j 的密钥材料 k_j.该敌手成功的概率记为 $\Pr[k_j' = k_j]$.

(2)A_{in}:通过质询挑战者得到 G 中公共信息 Pub,掌握部分层次节点$\{v_i\}$的密钥材料.能够有针对性的选择任意一个层次节点 v_m(其中 v_m 与 v_i 不构成偏序关系),向挑战者询问 v_m 对应的密钥材料.敌手成功攻陷方案的方式是能够区分挑战者返回给敌手的 k_m' 是 v_j 的真实密钥材料 k_m 还是与密钥材料等长的随机数.该敌手成功的概率记为 $\Pr[k_m' = k_m]$.

本文设计的访问控制方案目标是,能够成功抵抗 A_{out}和 A_{in}两类敌手攻击,即如果 $\Pr[k_j' = k_j]$和 $\Pr[k_m' = k_m]$均是可忽略的,则认为本方案是安全的.

3.5.2 证明过程

我们分别按照 A_{out}和 A_{in}两类攻击给出命题,利用标准模型对方案的安全性展开证明.

命题 1 设$\{f_v\}$是伪随机函数集,$\{E\}$是对称加密方案集,对于 $\forall$ DAG G,如果存在类型为 A_{out}的敌手能以 ε 的概率攻陷 Γ,则存在敌手 A_{out}以 ε'的概率攻陷 f_v 和 E.

证明:为了证明该命题,定义一系列的 $Game_0$, $Game_1, \cdots, Game_h$,其中 $Game_0$ 是敌手发起的游戏.每个游戏 $Game_i (i>0)$对任意的拓扑序列中节点 v_i 展开密钥恢复操作.通过 *Game* 之间渐变的不可区分性,来证明敌手通过 $Game_0$ 攻陷方案的概率是可忽略的.

$Game_0$:

构造过程:挑战者 C 运行方案 Γ 的 *Setup* 过程,输入安全参数 1^κ,输出公共信息交给 A_{out};

询问过程:A_{out}向 C 发起挑战,询问任意层次节点 v_i 对应的用户密钥,挑战者 C 通过$\{0,1\}^\kappa$ 计算生成对应用户密钥 uk_i 并返回给 A_{out}.

分析过程:敌手 A_{out}指定层次节点 v_0, v_0 与询问阶段中的 v_i 不构成任何偏序关系.A_{out}通过 uk_i 猜测得到最接近 v_0 真实密钥材料的 k_0',A_{out}赢得 $Game_0$ 的优势可

作如下定义:

$Adv_{A'_{\text{out}},0} = \varepsilon_0 = \Pr[k'_0 = k_0]$

$Game_1$:

$Game_1$ 的过程与 $Game_0$ 类似,唯一区别在于推导得到 v_1 密钥材料所需的公共参数 l_1 由真正随机数替换,即 $l_1 \approx E_R'(hl_1 \parallel R_4)$,其中 $R \leftarrow \{0,1\}^{\kappa}$. 我们利用 $Game_1$ 和 $Game_0$ 之间的可区分性,可构造一个 PPT 算法以不可忽略的优势攻陷伪随机函数 f_v 和对称加密方案 E. 则存在:

$$|\varepsilon_1 - \varepsilon_0| < negl(f_v) + negl(E) \tag{1}$$

不失一般性,对 $Game_i(i = 2,\cdots,h)$如下描述:

$Game_i$:

$Game_i$ 的推导过程与 $Game_{i-1}$类似,区别在于推导得到 v_i 密钥材料所需的公共参数 l_i 是由一个真正的随机值替换,即 $l_i \approx E_R'(hl_i \parallel R_4)$,其中 $R' \leftarrow \{0,1\}^{\kappa}$. 利用 $Game_i$ 和 $Game_{i-1}$之间的可区分性,能构造一个 PPT 算法以不可忽略的优势攻陷伪随机函数 f_v 和对称加密方案 E. 则存在:

$$|\varepsilon_i - \varepsilon_{i-1}| < negl(f_v) + negl(E) \tag{2}$$

此外,由于 $Game_h$ 在整个计算推导中,对于敌手 A'_{out}始终无法获取 v_h 对应的任何一个真实的用户密钥,因此,敌手 A'_{out}在 $Game_h$ 中能够成功猜测 k_h 的优势定义为 $Adv_{A'_1,h}$:

$$\varepsilon_h = \Pr[k'_h = k_h] = 1/2^n \tag{3}$$

合并(1)、(2)、(3)可得,

$\varepsilon_0 < h \cdot (negl(f_v) + negl(E)) + 1/2^n$,命题 1 得证.

命题 2　设$\{f_v\}$是伪随机函数集,$\{E\}$是对称加密方案集,对于 $\forall$ DAG G,如果存在类型为 A_{in}的敌手以 ε 的概率攻陷 Γ,则存在敌手 A'_{in}以 ε'的概率攻陷 f_v 和 E.

证明:为了证明该命题,定义一系列的 $Game_0$, $Game_1$,…,其中 $Game_0$ 是敌手发起的游戏. 每个游戏 $Game_i(i > 0)$对任意拓扑序列层次节点 v_i 展开密钥材料推导操作,敌手的优势是能够区分挑战者返回的密钥材料是真实的密钥材料还是等长随机值. 通过 $Game_{i-1}$和 $Game_i$ 之间渐变的不可区分性,证明敌手 $Game_0$ 成功的概率是可忽略的.

$Game_0$:

构造过程:挑战者 C 运行方案 Γ 的 *Setup* 过程,输入安全参数 1^{κ},输出公共信息返回给 A'_{in};

询问过程:分两个阶段,第一阶段 A'_{in}向 C 提出询问,要求获得任意层次节点 v_i 对应的密钥材料. 挑战者 C 生成相应的密钥材料 $k_i \in \{0,1\}^{\kappa}$ 并返回给 A'_{in}. 第二阶段,A'_{in}中断第一阶段的询问,指定任一层次节点 v_0(v_0 与 v_i 不构成偏序关系),向挑战者 C 询问层次节点 v_0 对应的密钥材料. 挑战者 C 从 $\{0,1\}$中随机选择 r',如果 $r' = 1$,返回 v_0 的真实密钥材料 k_0,如果 $r' = 0$,则返回一串等长的随机值 k'_0.

分析过程:敌手 A'_{in}从 $\{0,1\}$中随机选择 r'作为对 k_0 成功的判定,则 A'_{in}赢得 $Game_0$ 优势可用下式表示:

$$Adv_{A'_{\text{in}},0} = \varepsilon_0 = \Pr[k'_0 = k_0] - 1/2$$

$Game_1$ 分析分 $Game_1^a$ 和 $Game_1^b$ 两种情况.

$Game_1^a$:

v_1 作为 G 中的一个根层次节点. $Game_1^a$ 的推导过程与 $Game_0$ 类似,区别在于推导生成密钥材料 k_1 的算法由随机函数替代,即 $dk_1 = R(k_1 \parallel R_2)$,其中 $R \leftarrow \{0,1\}^{\kappa}$. 利用 $Game_1^a$ 和 $Game_0$ 之间的可区分性,构造一个 PPT 算法以不可忽略的优势攻陷伪随机函数 f_v. 即存在

$$|\varepsilon_1 - \varepsilon_0| < negl(f_v) \tag{4}$$

$Game_1^b$:

v_1 作为 G 中根节点 p 的一个层次子节点,即 $v_1 \prec \cdot p$. $Game_1^b$ 的推导过程与 $Game_0$ 类似,区别在于用于生成 k_1 的密钥推导算法由随机函数代替,即 $dk_1 = R(k_1 \parallel R_2)$, $e_1 = E_{dk_1}(\$ \parallel R_3)$,其中 $\$$ 表示随机值. 利用 $Game_1^b$ 和 $Game_0$ 之间的可区分性,构造一个 PPT 算法以不可忽略的优势攻陷 f_v 和 E. 即存在

$$|\varepsilon_1 - \varepsilon_0| < negl(f_v) + negl(E) \tag{5}$$

不失一般性,对 $Game_i(i = 1,2,\cdots)$作如下描述:

$Game_i$:

$Game_i$ 的过程与 $Game_{i-1}$类似,区别在于用于生成 k_i 的密钥推导算法由随机函数代替,即 $dk_i = R(k_i \parallel R_2)$, $e_1 = E_{dk_i}(\$ \parallel R_3)$. 利用 $Game_i$ 和 $Game_{i-1}$之间的可区分性,构造一个 PPT 算法以不可忽略的优势攻陷 f_v 和 E. 即存在

$$|\varepsilon_i - \varepsilon_{i-1}| < negl(f_v) + negl(E) \tag{6}$$

$Game_h$:

假设 A'_{in}已进行了 h 轮游戏,由于在整个推导过程中,敌手 A'_{in}始终无法区分从挑战者处得到密钥材料是真实密钥材料还是等长随机值,因此,在 $Game_h$ 的过程中,不存在任何公共信息被敌手 A'_{in}利用,推导得到真实的密钥材料,即 $Game_h$ 中 A'_{in}成功猜测挑战者返回的信息是真实密钥 k_h 的优势 $Adv_{A'_{\text{in}},h}$可表示为:

$$\varepsilon_h = \Pr[k'_h = k_h] - 1/2 \tag{7}$$

合并式(4) ~ (7),得到

$\varepsilon_0 < negl(f_v) + (h-1) \cdot (negl(f_v) + negl(E)) - 1/2$,命题得证.

通过命题 1 和命题 2 的证明,我们认为本文设计方案在内部攻击和外部攻击情况下是可证明安全的.

4 性能分析

4.1 安全分析

本文提出的访问控制方案中,每个用户仅需保存单个用户密钥,且多用户之间密钥材料获取相互独立,密钥材料获取安全性由 f_v 的单向不可逆性保证,因此能够很好的防止重放攻击、Dos 攻击等攻击行为.此外,一旦用户密钥失窃,CA 可通过撤销其对应的哈希链防止敌手的访问,同时不影响其他用户的正常密钥材料获取过程.

每个层次节点也仅需存储单个密钥材料,利用 f_v 生成本层保护密钥和下层推导密钥,能够有效避免共谋攻击的风险.此外,由于整个推导过程涉及的中间层次节点不需产生保护密钥,从而能够降低密钥泄露的风险.整个推导过程在标准模型下是可证明安全的.

4.2 效率分析

本文设计的访问控制方案中,每个用户的存储开销和每个层次节点的存储开销均是 $O(1)$,而感知层网络的公共存储开销则由用户数和节点数确定,随着数量的增加,仅呈线性增加趋势.设感知层网络用户数为 m,层次节点个数为 n,则整个网络的私有信息存储开销为 $O(m+n)$,网络的公共信息存储开销至多为 $O(m+n)$.而计算开销方面,每个用户获取密钥材料的计算量至多为 m 次解密运算,$\lceil \log_2^m \rceil$ 次哈希运算;一次密钥材料推导过程也仅需要一次哈希和一次解密运算,相比较文献[8]等采用的模数运算更有优势.

从安全性、效率两个方面,与类似方案做比较,如表 1 所示.

表 1 方案比较

访问控制方案	公共开销	节点存储开销	用户存储开销	一次密钥推导开销	用户密钥材料获取	密钥更新	动态扩展	可证明安全
文献[16]	$2k\|e\|$	k	NO	$H+2XOR$	NO	ALL	NO	NO
文献[18]	$k\|e\|$	k	NO	$H+XOR$	NO	ALL	NO	NO
文献[20]	$k\|e\|$	k	NO	$2H$	NO	ALL	NO	NO
文献[23]	$k\|e\|$	k	NO	$3H+E$	NO	L	YES	YES
本方案	$k\|e\|+m$	k	uk	$H+E$	$\lceil \log_2^m \rceil + 1$	L	YES	YES

注:"YES"表示方案考虑该要素,"NO"表示方案未考虑;"ALL"表示全局,"L"表示局部;本文的 k 表示密钥材料,其他方案表示密钥值.

5 总结

物联网感知层在物联网体系中处于信息采集的最前端,对物联网的实现起到根本作用.针对感知层节点数量庞大,计算、存储能力有限,信息资源通常只允许用户"读"等特性,本文在考虑多用户访问前提下,将信息资源按等级划分,利用密码学手段,提出可动态扩展的分层访问控制方案,并通过详细的分析验证该方案的安全、有效,比其他现有方案更适合物联网感知层环境的应用.

参考文献

[1] 工业和信息化部.物联网"十二五"发展规划[EB/OL]. http://www.gov.cn/zwgk/2012-02/14/content-2065999.htm.[2012-02-14].

[2] M Tuters, K Varnelis. Beyond locative media: Giving shape to the internet of things [J]. Leonardo, 2006, 39(4): 357 – 363.

[3] 孙其博,刘杰,等.物联网:概念、架构与关键技术研究综述[J].2010,33(3):1 – 9.
SUN Qibo, LIU Jie, et al. Internet of things: Summarize on concepts, architecture and key technology problem[J]. Journal of Beijing University of Posts and Telecommunications, 2010, 33(3): 1 – 9. (in Chinese)

[4] 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.
Wu Zhenqiang, Zhou Yanwei, Ma Jianfeng. A securitytransmission model for internet of things [J]. Chinese Journal of Computers, 2011, 34(8): 1351 – 1364. (in Chinese)

[5] N Gershenfeld, R Krikorian, D Cohen. The internet of things [J]. Scientific American, 2004, 291(4): 76 – 81.

[6] Ashton K. That 'internet of things' thing[J]. RFID Journal, 2009: 97 – 114.

[7] L Atzori, A Iera, G Morabito. The internet of things: A survey [J]. Computer Networks, 2010, 54(15): 2787 – 2805.

[8] S Akl, P Taylor. Cryptographic solution to a problem of access control in a hierarchy[J]. ACM Transactions on Computer Systems, 1983, 1(3): 239 – 248.

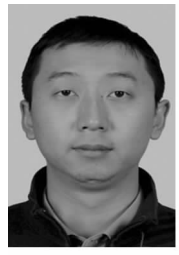
[9] A De Santis, A Ferrara, B Masucci. Cryptographic key assignment schemes for any access control policy[J]. Information Processing Letters (IPL), 2004, 92(4): 199 – 205.

[10] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[A]. Advances in Cryptology [C]. Berlin Heidelberg: Springer, 1985. 10 – 18.

[11] 阎军智,李凤华,马建峰.基于 Diffie Hellman 算法的分层密钥分配方案[J].电子学报,2011,39(1):119 – 123.
Yan Junzhi, Li Fenghua, Ma Jianfeng. Ahierarchical key as-

signment scheme based on diffie-hellman algorithm[J]. Acta Electronica Sinica,2011,39(1):119 – 123.(in Chinese)
[12] M Hwang, W Yang. Controlling access in large partially ordered hierarchies using cryptographic keys[J]. Journal of Systems and Software,2003,67(2):99 – 107.
[13] 姬东耀,张福泰,王育民.多级安全系统中访问控制新方案[J].计算机研究与发展,2001,38(6):715 – 720.
JI Dongyao, ZHANG Futai, WANG Yumin. Anew scheme for access control in multilevel security system[J]. Journal of Computer Research & Development, 2001, 38(6): 715 – 720. (in Chinese)
[14] 李凤华,王巍,马建峰.适用于传感器网络的分级群组密钥管理[J].电子学报,2008,36(12):2405 – 2411.
LI Fenghua, WANG Wei, MA Jianfeng. Leveled group key management for wireless sensor networks[J]. Acta Electronica Sinica, 2008, 36(12): 2405 – 2411. (in Chinese)
[15] S Y Wang, C S Laih. Cryptanalysis of Hwang-Yang scheme for controlling access in large partially ordered hierarchies[J]. Journal of Systems and Software, 2005, 75(1 – 2): 189 – 192.
[16] Chen T S, Huang J Y. A novel key management scheme for dynamic access control in a user hierarchy[J]. Applied Mathematics and Computation, 2005, 162(1): 339 – 351.
[17] Hwang M S, Yang W P. Controlling access in large partially ordered hierarchies using cryptographic keys[J]. Journal of Systems and Software, 2003, 67(2): 99 – 107.
[18] Chien H Y, Jan J K. New hierarchical assignment without public key cryptography[J]. Computers & Security, 2003, 22(6): 523 – 526.
[19] Sorniotti A, Molva R, Gomez L, et al. Efficient access control for wireless sensor data[J]. International Journal of Wireless Information Networks, 2009, 16(3): 165 – 174.
[20] Zou X, Ramamurthy B, Magliveras S S. Chinese remainder theorem based hierarchical access control for secure group communication[A]. Proceedings of the Third International Conference Information and Communications Security[C]. London, UK: Springer, 2001. 381 – 385.
[21] Gudes E. The design of a cryptography based secure file system[J]. IEEE Transactions on Software Engineering, 1980, SE – 6(5): 411 – 420.
[22] Atallah M J, et al. Incorporating temporal capabilities in existing key management schemes[A]. Proceedings of the 12th European Symposium on Research in Computer Security[C]. Berlin Heidelberg: Springer, 2007. 515 – 530.
[23] De Santis A, Ferrara A L, Masucci B. Efficient Provably-secure Hierarchical Key Assignment Schemes[M]. Berlin Heidelberg: Springer, 2007. 371 – 382.
[24] Sa ndhu R, Coyne E, Feinstein H, et al. Role-based access control models[J]. IEEE Computer, 1996, 29(2): 38 – 47.
[25] Martínez-García C, Navarro-Arribas G, Borrell J. Fuzzy role-based access control[J]. Iformation Processing Letters, 2011, 111(10): 483 – 487.
[26] Goyal V, PandeyO, et al. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proceedings of the 13th ACM Conference on Computer and Communications Security[C]. Alexandria, Virginia, USA: ACM, 2006. 89 – 98.
[27] XIONG Jin-bo1, YAO Zhi-qiang, MA Jian-feng1, et al. Multi-level access control model for video database[J]. Journal on Communications, 2012, 33(8): 147 – 154.
[28] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[A]. Proceedings of Public Key Cryptography-PKC[C]. Taormina, Italy: Springer, 2011. 53 – 70.
[29] Goldreich O, et al. How to construct random functions[J]. Journal of the ACM, 1986, 33(4): 792 – 807.
[30] Mrkle R C. A certified digital signature[A]. Proceedings of Advances in Cryptology—CRYPTO [C]. New York: Springer, 1990. 218 – 238.
[31] Jakobsson M, Leighton T, et al. Fractal merkle tree representation and traversal[A]. Proceedings of Topics in Cryptology—CT-RSA[C]. Berlin Heidelberg: Springer, 2003. 314 – 326.
[32] Atallah M J, Frikken K B, Blanton M. Dynamic and efficient key management for access hierarchies[A]. Proceedings of the 12th ACM Conference on Computer and Communications Security[C]. NY, USA: ACM, 2005. 190 – 202.

作者简介



马　骏　男.1981 年 1 月出生,山西阳泉人.西安电子科技大学博士生.主要从事无线网络安全、密钥管理有关研究.
E-mail: sijunhan@163.com

郭渊博　男.1975 年 7 月出生,陕西周至人.解放军信息工程大学副教授、硕士生导师.主要从事容忍入侵、无线网络安全、态势感知有关研究.
E-mail: yuanbo_g@hotmail.com