物联网中基于受控对象的分布式访问控制

王 浩，吴 博，葛劲文，王 平

(重庆邮电大学工业物联网与网络化控制教育部重点实验室 重庆 南岸区 400065)

【摘要】提出了一种基于受控对象的分布式访问控制方法，将访问主体的访问权限直接与节点的资源对象相关联，由节点管理用户的权限，简化权限的管理。将对称密码体制与非对称密码体制应用于分布式访问控制中，根据设备对象的能力分别采用不同的加密策略，在保证控制强度的同时减小节点计算能耗。性能分析表明，该方案能够在节点低开销的基础上对用户进行有效的接入控制和权限限制，简化用户的权限管理，并有效减少用户DOS攻击和重放攻击对网络的威胁。

关 键 词 受控对象； 分布式访问控制； 权限； 安全； 物联网

中图分类号 TP309.2 **文献标识码** A doi:10.3969/j.issn.1001-0548.2012.06.015

Distributed Access Control Scheme Based on Controlled Object in the Internet of Things

WANG Hao, WU Bo, GE Jin Wen, and WANG Ping

(Key Labratory of Indurstrial Internet of Thing and Networked Control, Ministry of Education,

Chongqing University of Posts and Telecommunications Nan'an Chongqing 400065)

Abstract In this paper, we propose a distributed access control scheme based on controlled object, in which we make all of the nodes manage the user's right to simplify the right management, and adopt different encryption policy according to the ability of the device object to realize high level of control and low consumption of calculation. The analysis shows that proposed scheme can effectively control the user's access based on node's low cost, and mitigate DOS attack and reply attack of users.

Key words controlled object; distributed access control; privilege; security; the Internet of Things

物联网(the Internet of Things，IoT)是通信网和互联网的拓展应用和网络延伸，它利用感知技术与智能装置对物理世界进行感知识别，通过网络传输互联，进行计算、处理和知识挖掘，实现人与物、物与物信息交互和无缝链接。

物联网的一端是由大量传感节点组成的传感网，它们根据不同的应用对部署的区域进行信息采集和监控，外部用户可以对其进行远程访问。因网络中可能存在大量恶意用户，传感网内部需要对外部用户进行访问控制。由于物联网上的传感节点资源有限、数量众多，且资源分散程度高，传统的访问控制策略难以满足其安全性的要求。如何在这种环境下阻止非法的访问，是物联网在实际应用中必须解决的主要问题之一。本文在分析传统访问控制模型应用在物联网安全中的不足基础上，提出了一种基于受控对象的分布式访问控制方案，在传感节点低开销时上实现对用户严格的接入控制和权限限制，并有效减少了用户DoS攻击和重放攻击对网络的威胁。

1 相关工作

目前访问控制策略主要有自主访问控制(DAC)、强制访问控制(MAC)和基于角色的访问控制(RBAC)3种。DAC的核心思想是拥有资源的主体能自主地将权限的某子集授予其他主体，授予过程称为权限委托。其缺点是权限配置粒度小，配置工作量大、效率低。MAC定义了主体对客体访问的4种方式，上读、下读、上写、下写。因这种策略配置粒度大，且缺乏灵活性，不适用物联网应用的深入和多样化导致的控制策略多样化的需求，所以不能全部照搬，但可有选择地加以应用。RBAC适用于数量多且变动频繁的策略中，通过给用户分配合适的角色，让用户与访问权限相联系。该策略系统所管理的资源集中，因此系统可以很方便地完成对

收稿日期：2012－01－11；修回日期：2012－05－04
基金项目：国家科技重大专项(2010ZX03006-001)；重庆市自然科技基金(cstc2011jjA40040)；重庆市科技攻关计划(cstc2011AB2096)
作者简介：王浩(1975－)，男，副教授，主要从事无线传感器网络安全方面的研究.

所有用户的控制任务。物联网中资源的拥有者是各个节点，且资源的分散程度远大于现有访问控制系统[1]，网络管理者难以对每个用户进行权限控制。

目前已有的适用于物联网访问控制方案中，文献[2]采用椭圆曲线密码体制(elliptic curve cryptography，ECC)实现用户访问网络时需要的签名与认证过程，但节点计算开销过大，网络容易遭受用户的DOS攻击。文献[3]的ENABLE方案解决了文献[2]中存在的节点开销过大的问题，同时设计了防止用户DOS攻击与重放攻击的方法，并提供了用户与节点的双向鉴别机制，但仍然引入了不必要的网络开销问题。FDAC[4]是一种基于细粒度的访问控制方案，它根据一系列预定义的属性划分节点，并根据该属性指定用户的访问权限。同时，将用户与节点安全通信所用的密钥和节点属性挂钩，当用户访问结构与节点属性一致时，才有权解密消息。但该方案仍然存在两个问题：1) 属性的定义依赖于传感网所处的环境；2) 根据各个属性预定义密钥的方法使得具有多个属性的节点需要管理多个密钥，既增大了密钥管理的难度，又增加了节点的存储开销，没有平衡好节点开销与控制强度的问题。

本文针对以上问题，采用一种基于受控对象的访问控制模型(object-based access control，OBAC)[5]，采纳传统控制策略中的部分思想，由网络管理中心与节点共同对用户进行分布式控制，解决了物联网在节点低开销时如何对用户进行有效的接入控制和权限限制的问题。

2 系统模型

2.1 研究假设

本文的研究基于以下假设：1) 用户已向访问控制服务器注册，并得到访问控制服务器的公共密钥；2) 访问控制服务器负责管理用户注册信息，有权对用户颁发授权证书；3) 访问控制服务器拥有强大的计算能力和存储能力，且带宽很高；4) 网络管理中心已与访问控制服务器共享了公共密钥，根据网络应用环境确定了所有节点的资源安全级别，并将其汇报给访问控制服务器；5) 网络管理中心是拥有最大访问权限的特殊用户。

2.2 网络模型

为了保证在节点低开销的基础上对用户访问进行严格控制，本文引入了基于受控对象的访问控制模型。通过采用ECC公钥密码体制与对称密码体制相结合的方法，在不需要对传感网内部密码体制改动的情况下，保证对用户访问的有效控制。网络模型如图1所示。

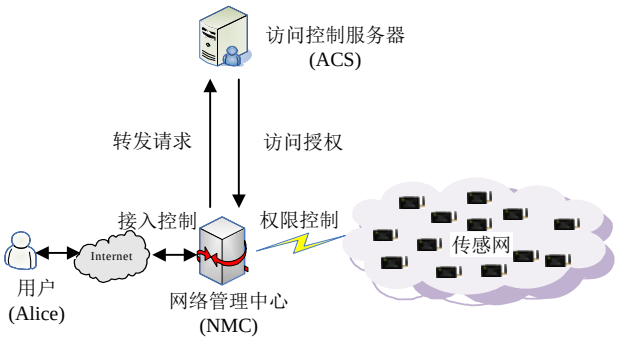

图1 分布式访问控制网络模型

访问控制服务器ACS首先需要在有限域GF(p)(p为一素数)上确定一个特定的椭圆曲线方程和基点G，然后随机选择$k_{ACS}\in$GF(p)作为自己的私钥，并由$Q_{ACS}=k_{ACS}G$计算得到自己的公钥，最后在网络组网阶段和用户Alice注册时确定公开安全参数，并将自己的公钥Q_{ACS}发送给网络管理中心NMC与用户Alice。Alice收到后保存该信息，NMC根据该信息用同样的方法计算得到公私密钥对k_{NMC}、Q_{NMC}，并将公钥Q_{NMC}发给ACS。

2.3 基于受控对象的访问控制模型

在基于受控对象的访问控制模型中，将访问控制列表(ACL)与受控对象相关联，并将访问控制项(ACE)设计成用户或用户组及其对应权限的集合，其结构如图2所示。

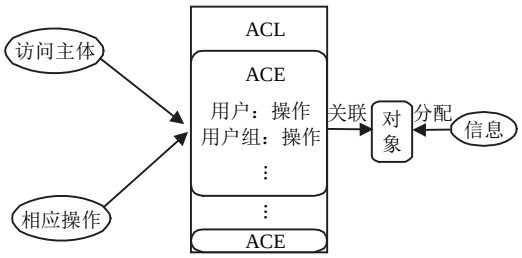

图2 OBAC模型结构

这种结构模型应用在物联网访问控制中的优点是，节点可以根据自己所拥有的资源将有权访问该资源的用户信息添加进ACL中，避免了RBAC模型中节点保存的角色所对应的资源可能跟节点资源毫无关系的情况；其次，引入用户组，使节点在有多个相同访问权限的用户存在情况下，减小节点的存储开销；再次，即使用户之间存在权限委托的行为，只要节点中的ACL不改变，被委托的用户仍然不可能有权访问到被授权的资源，避免了权限泄露问题；最后，在任务改变或监测到合法用户恶意行为的情况下，拥有最大访问权限的NMC可以主动发起更改

或撤销用户权限的命令。

3　受控对象的分布式访问控制方案

方案包括两个阶段：访问授权阶段和分布式访问控制阶段。访问授权的目的是为了使节点之间建立起对用户的信任。在分布式访问控制中，NMC对用户进行接入控制，传感节点对用户进行权限限制。

3.1　访问授权阶段

1) 用户Alice从获得的椭圆曲线方程参数和基点G生成公私密钥对K_{A}、Q_{A}，K_{A}为Alice的私钥，Q_{A}为公钥，并构造访问申请消息发送给NMC，访问申请消息包含Alice的身份标识ID_{A}、Alice的当前时间T_{A}和Q_{A}，表示为：

$$\mathrm{Alice}\rightarrow\mathrm{NMC}:M_{\mathrm{AA}}=T_{\mathrm{A}}\,||\,E_{Q_{\mathrm{ACS}}}(\mathrm{ID}_{\mathrm{A}}\,||\,Q_{\mathrm{A}})$$

式中，$E_{Q_{\mathrm{ACS}}}(\mathrm{ID}_{\mathrm{A}}\,||\,Q_{\mathrm{A}})$表示使用ECC加密算法和公钥$Q_{\mathrm{ACS}}$对$\mathrm{ID}_{\mathrm{A}}$与$Q_{\mathrm{A}}$进行加密；||表示连接符；$M_{\mathrm{AA}}$为访问申请消息。

2) 当NMC收到Alice的访问申请消息后，先判断T_{A}是否是有效的时间值，若$T_{\mathrm{N}}-T_{\mathrm{A}}>\mathrm{Delay_}T_{\max}$，则直接丢弃消息；若$T_{\mathrm{N}}-T_{\mathrm{A}}<\mathrm{Delay_}T_{\max}$，则将$\mathrm{ID}_{\mathrm{A}}\,||\,Q_{\mathrm{A}}$发送给访问控制服务器ACS：

$$\mathrm{NMC}\rightarrow\mathrm{ACS}:\mathrm{ID}_{\mathrm{A}}\,||\,Q_{\mathrm{A}}$$

式中，T_{N}为NMC的当前时间；$\mathrm{Delay_}T_{\max}$表示用户最大传输时延。

3) 当ACS收到NMC发来的消息后，用自己的私钥k_{ACS}解密，根据ID_{A}查看注册信息中是否有Alice的记录，若没有则拒绝访问申请；若有则构造签名的授权证书$\mathrm{Cert}_{\mathrm{A}}$发送给NMC，同时设置用户访问状态$\mathrm{State}_{\mathrm{A}}$=Access_In，Access_In表示允许访问网络。证书内容包括Alice的身份标识ID_{A}、公钥Q_{A}、访问时限$\mathrm{Time_Bound}_{\mathrm{A}}$，资源类型标识$R_\mathrm{ID}_i$和对应权限的标识$P_\mathrm{ID}_i$ ($1<i<\cdots<m$)，发送消息表示为：

$$\mathrm{ACS}\rightarrow\mathrm{NMC}:\mathrm{Cert}_{\mathrm{A}}=E_{k_{\mathrm{ACS}}}(\mathrm{ID}_{\mathrm{A}}\,||\,Q_{\mathrm{A}}\,||\,\mathrm{Time\_Bound}_{\mathrm{A}}\,||\{\{R\_\mathrm{ID}_1,P\_\mathrm{ID}_1\},\{R\_\mathrm{ID}_2,P\_\mathrm{ID}_2\},\cdots,\{R\_\mathrm{ID}_m,P\_\mathrm{ID}_m\}\})$$

其中，资源类型和对应权限是ACS根据Alice的用户级别与资源的安全级别确定的。用户级别分为重要级、高级、中级、普通4种。资源安全级别也分为：绝密级、机密级、秘密级、无密级4种。用户级别与资源安全级别是一一对应关系。资源类型和访问权限的确定原则是用户对同级的资源只具有读取权限，对低级别的资源具有读取、写入和删除权限。

4) 当NMC收到ACS签名的授权证书后，用ACS的公钥Q_{ACS}认证签名，若认证失败则丢弃证书；若认证成功，则为Alice建立用户信息表，表中保存的信息如表1所示。

然后构造证书消息B_{cert}广播发送给所有节点N_i (i=1,2,$\cdots$,n)，证书消息包含Alice的身份标识ID_{A}、访问时限$\mathrm{Time_Bound}_{\mathrm{A}}$以及资源类型标识$R_\mathrm{ID}_i$和对应权限的标识$P_\mathrm{ID}_i$ ($1<i<\cdots<m$)：

$$\mathrm{NMC}\rightarrow N_i:\mathrm{CERT}=F_{\mathrm{Net\_Key}}(\mathrm{ID}_{\mathrm{A}}\,||\,\mathrm{Time\_Bound}_{\mathrm{A}}\,||\,\{\{R\_\mathrm{ID}_1,P\_\mathrm{ID}_1\},\{R\_\mathrm{ID}_2,P\_\mathrm{ID}_2\},\cdots,\{R\_\mathrm{ID}_m,P\_\mathrm{ID}_m\}\})$$

其中，$F_{\mathrm{Net_Key}}$表示使用对称加密算法和全网密钥Net_Key对消息进行加密。

表1　用户信息表

用户身份标识	用户公钥	访问时限
ID_{A}	Q_{A}	$\mathrm{Time\_Bound}_{\mathrm{A}}$

5) 当网络中的节点收到NMC广播的证书消息后，用Net_Key解密消息，将自己存储的资源类型标识与证书中的进行比较，没有相同的则丢弃证书消息；相同则保存对应的资源类型标识和权限标识，添加进访问控制列表，并返回确认信息。访问控制列表如表2所示。

表2　节点的访问控制列表

用户组标识(可选)	用户身份标识	访问时限	资源类型标识	权限标识
\	ID_{A}	$\mathrm{Time\_Bound}_{\mathrm{A}}$	$R\_\mathrm{ID}_{\mathrm{S}}$	$P\_\mathrm{ID}_{\mathrm{S}}$
	⋮	⋮		
G_ID_1	ID_{N}	$\mathrm{Time\_Bound}_{\mathrm{N}}$	$R\_\mathrm{ID}_{\mathrm{x}}$	$P\_\mathrm{ID}_{\mathrm{x}}$

表中，$R_\mathrm{ID}_{\mathrm{S}}$与$P_\mathrm{ID}_{\mathrm{S}}$分别表示节点$N_{\mathrm{S}}$的资源类型标识与用户Alice对该资源所拥有的权限的标识，G_ID_2对应的是其他组用户的信息。

6) 为了与Alice建立共享密钥，当所有节点收到证书消息并进行响应后，NMC用自己的私钥k_{NMC}点乘Alice的公钥Q_{A}得到：

$$k_{\mathrm{NMC}}Q_{\mathrm{A}}=(x_{\mathrm{NMC}},y_{\mathrm{NMC}})$$

将x_{NMC}作为与Alice的共享密钥，并将自己的公钥Q_{NMC}作为响应消息发送给用户Alice：

$$\mathrm{NMC}\rightarrow\mathrm{Alice}:Q_{\mathrm{NMC}}$$

至此，访问授权阶段结束。

3.2　访问控制阶段

当Alice收到NMC的响应后，用自己的私钥k_{A}点乘NMC的公钥Q_{NMC}：

$$k_{\mathrm{A}}Q_{\mathrm{NMC}}=(x_{\mathrm{A}},y_{\mathrm{A}})$$

因为$k_{\mathrm{NMC}}Q_{\mathrm{A}}=k_{\mathrm{NMC}}k_{\mathrm{A}}G=k_{\mathrm{A}}Q_{\mathrm{NMC}}$，所以$x_{\mathrm{A}}=x_{\mathrm{NMC}}$，于是Alice便与NMC在不进行密钥传输的情况下建

立起双方的共享密钥。

1) Alice构造读请求消息 M_{AQ}，用与NMC的共享密钥 x_{A} 加密发送给NMC，其中 T_{A}' 代表当前时间，O代表用户的请求操作，下标R表示读请求：

$$\mathrm{Alice}->\mathrm{NMC}: M_{\mathrm{AQ}} = T_{\mathrm{A}}' \,||\, F_{x_{\mathrm{A}}}(\mathrm{ID}_{\mathrm{A}} \,||\, T_{\mathrm{A}}' \,||\, O_{\mathrm{R}})$$

2) NMC收到访问请求消息后，首先判断 T_{A}' 是否为有效的时间值，若NMC的当前时间 $T_{\mathrm{N}}' - T_{\mathrm{A}}' >$ Delay_ $T_{\max}$，则直接丢弃消息；若 $T_{\mathrm{N}}' - T_{\mathrm{A}}' <$ Delay_ $T_{\max}$，则用与Alice的共享密钥 x_{NMC} 解密消息，得到 $\mathrm{ID}_{\mathrm{A}}{}^{*}$ 与 $T_{\mathrm{A}}'^{*}$，比对 T_{A}' 与 $T_{\mathrm{A}}'^{*}$ 是否相等，若不相等丢弃消息；相等则继续根据 $\mathrm{ID}_{\mathrm{A}}{}^{*}$ 查找用户信息表中是否有Alice的记录，没有返回失败回应；有则构造广播消息 B_{REQ} 发送给所有节点 N_i (i=1,2,⋯, n)：

$$\mathrm{NMC} \rightarrow N_i: B_{\mathrm{REQ}} = F_{\mathrm{Net\_Key}}(\mathrm{ID}_{\mathrm{A}} \,||\, O_{\mathrm{R}})$$

3) 当网络中的节点收到 B_{REQ} 后，用全网密钥Net_Key解密得到 ID_{A} 与 Q_{R}，根据 ID_{A} 查找访问控制表中是否有Alice的记录，没有则返回失败回应；有则根据读请求R将响应消息 M_{REP} 发送给NMC：

$$N_{\mathrm{S}} \rightarrow \mathrm{NMC}: M_{\mathrm{REP}} = F_{K_{\mathrm{S,NMC}}}(R\_\mathrm{ID}_{\mathrm{S}} \,||\, \mathrm{data}_{\mathrm{S}})$$

其中，$\mathrm{data}_{\mathrm{S}}$ 代表了节点 N_{S} 采集的数据。

4) 当NMC收到节点的响应消息后，用个体密钥 $K_{\mathrm{S,NMC}}$ 解密消息，并判断 $R\_\ \mathrm{ID}_{\mathrm{S}}$ 是否正确，不正确则丢弃消息；正确构造访问响应消息 M_{AP} 发送给用户Alice：

$$\mathrm{NMC} \rightarrow \mathrm{Alice}: M_{\mathrm{AP}} = E_{x_{\mathrm{NMC}}}(\mathrm{ID}_{\mathrm{NMC}} \,||\, \{R\_\mathrm{ID}_{\mathrm{S}} \,||\, \mathrm{data}_{\mathrm{S}}\}, \cdots, \{R\_\mathrm{ID}_{\mathrm{T}} \,||\, \mathrm{data}_{\mathrm{T}}\})$$

其中，$\{R\_\ \mathrm{ID}_{\mathrm{T}} \,||\, \mathrm{data}_{\mathrm{T}}\}$ 表示除节点 $\mathrm{data}_{\mathrm{S}}$ 外的其他节点的响应消息。Alice收到访问响应消息后，用与NMC的共享密钥 x_{A} 解密，然后判断 $\mathrm{ID}_{\mathrm{NMC}}$ 是否正确，不正确则说明访问响应消息被篡改或是伪造的，Alice将丢弃此消息；若正确则保存资源类型标识及其对应的数据。当用户再次发起访问时，可以针对特定的资源类型发起访问请求，过程同上。

4 性能分析

本节将从安全性、节点存储量、计算与通信开销等几个方面对本文方案进行性能评估。安全性是网络满足预期的访问控制需求和权限管理需求。

4.1 安全性分析

安全性包括NMC对用户的接入安全和网络对用户权限控制和管理的安全两个方面。接入安全包括防止非法用户接入网络，减轻恶意用户在接入过程中对网络所造成的危害。权限控制和管理安全是用户权限的安全分配以及恶意用户权限撤销。

4.1.1 网络接入的安全分析

为了防止非法用户接入网络，合法用户事先需要与NMC共享密钥作为加入网络的凭证，并且在共享过程中保证密钥的安全。在访问授权阶段，基于ECC的签名认证机制使NMC只有在成功认证授权证书之后才会接受用户的公钥。在用户与NMC获得对方公钥后，通过ECDH协议[6]得到彼此的共享密钥以保证密钥的安全。

用户向网络发送请求消息时，可能在短时间内发送大量的报文达到DOS攻击的目的。本文方案在访问授权阶段处理用户请求消息时，NMC首先判断访问申请消息中的时间戳 T_{A} 是否有效，有效则直接转发请求消息给ACS，对时间戳的判断能够保证请求消息的新鲜性，防止重放攻击。文献[3]在处理同类情况时用消息认证码算法[7]生成MAC值后才进行转发，因此本文方案处理用户请求消息效率更高，更能减少恶意用户DOS攻击的威胁。而在分布式访问控制过程中，当NMC收到用户的访问请求消息，在判断用户时间戳 T_{A}' 基础上进行一次对称加解密操作。目前测得在MICA2节点上执行一次对称加解密操作只需0.52 ms，是文献[3]中处理同类情况所花时间(约为3.12 ms)的1/6，因此与文献[3]相比仍然能够减少DOS攻击的威胁。

4.1.2 用户权限控制和管理安全

本文方案中，NMC和节点中不会存在未注册用户的信息，未注册用户不可能完成接入认证和权限控制。在权限下发过程中，采用加解密机制保护信息的安全传输。对于合法用户的非授权访问，NMC可以设定一个阈值，若在一段时间内收到的节点对某个用户的失败响应次数超过该阈值，说明该用户可能从合法用户转为恶意用户，NMC则向网络广播撤销该用户权限的命令，相关节点收到后删除访问控制表中对应用户的信息，以禁止用户访问，同时NMC也将删除用户信息表中该用户的信息，并将回馈消息发送给ACS，ACS收到回馈消息后，将用户的访问状态 $\mathrm{State}_{\mathrm{A}}$ 设置为Access_Out状态，表明禁止该用户访问网络。

4.2 存储量分析

当访问网络的用户越多时，节点要存储的用户信息就越多。在文献[2-3]中，节点不仅需要存储与用户安全交互的密钥，还需要保存每个用户的权限信息，当网络中用户规模很大时，节点所需要的存储量就会很大。而本文方案因为采用了NMC与用户

的交互模式，用户的认证过程以及信息的安全传输由NMC负责，因此节点不再需要保存与用户安全交互的密钥，只需要存储用户的权限信息即可，表3给出了节点以单用户形式存储的存储量。

表3　单用户形式的存储量

Octets: 2	2	2	2
ID	Time_Bound	*R*_ID	*P*_ID

可以看出，对于以单用户形式存储的情况，节点对每个用户需要保持8字节的信息。若采用组的形式进行存储，当n个具有相同权限(n>0)的用户同时访问时，根据表2的存储显示，节点需要存储的量为(4n+6) byte，相对于以单用户形式存储的8n byte，可节省(4n–6) byte大小的存储空间。

4.3　计算开销

因为用户与NMC一般都是电源供电设备且处理能力强大，因此方案只需要考虑节点的计算开销。表4列出了每项安全操作在Mica2节点上[8-10]的执行时间。

表4　Mica2上安全项的运行时间

标号	含义描述	时间/ms
T_{H}	执行一次单向散列函数所需要的时间	3.636
T_{MAC}	生成校验码所需时间	3.12
T_{RC5}	执行RC5加密或解密算法所需时间	0.26
T_{MUL}	执行ECC点乘算法所需时间	810

将本文方案(DACBCO)与方案MAACE[11]和ECCAC[12]中节点的计算开销进行对比，并依据表4中已经测得的实际应用的数据，得到如表5所示的传感节点总的计算时间。

表5　总计算时间对比

	DACBCO	MAACE	ECCAC
用户认证	None	$2T_{\mathrm{MAC}}+T_{\mathrm{H}}+T_{\mathrm{RC5}}$	$2T_{\mathrm{H}}+2T_{\mathrm{MAC}}+T_{\mathrm{RC5}}+3T_{\mathrm{MUL}}$
节点鉴别	None		None
权限分发	T_{RC5}	None	None
权限控制	$2T_{\mathrm{RC5}}$	None	None
总计	$3T_{\mathrm{RC5}}$	$2T_{\mathrm{MAC}}+T_{\mathrm{H}}+T_{\mathrm{RC5}}$	$2T_{\mathrm{H}}+2T_{\mathrm{MAC}}+T_{\mathrm{RC5}}+3T_{\mathrm{MUL}}$
时间总计/ms	0.78	10.136	2 415.04

从表5容易看出，由于方案采用了分布式访问控制机制，节点不再需要参与对用户的认证，只是在权限分发阶段和权限控制阶段利用对称加密机制保障信息的传输安全。而在MAACE方案中，因为提供了用户与节点的双向鉴别机制，因此节点的计算开销为$2T_{\mathrm{MAC}}+T_{\mathrm{H}}+T_{\mathrm{RC5}}$，节点总的计算时间约是本文方案的13倍。ECCAC方案中因为采用了节点直接控制用户进行访问的模式，使得节点既要对用户进行认证还要对用户进行权限控制，且认证采用的是基于ECC公钥密码体制的认证签名算法，其计算时间约为本文方案的3 096倍。所以，对比之前的方案，本文方案降低了节点的计算开销，很好地平衡了节点计算能耗和对用户的有效控制。

5　结　论

本文提出了基于受控对象的分布式访问控制方案，通过ECC密钥交换协议[13]在不需要对密钥进行传输的情况下建立网络管理中心与用户的共享密钥，以此用于网络管理中心对用户的接入控制和信息交互的安全。通过对称密码体制保证了网内权限分发的安全，使得节点能依据正确的权限信息对用户进行权限限制。采用基于受控对象的访问控制模型，在简化权限管理的同时减少了节点的存储量，也解决了权限泄露的问题。性能分析表明，该方案能够在节点低开销的基础上保证对用户进行有效的接入控制和权限限制，同时还能减少用户DOS攻击和重放攻击对网络的威胁。

参　考　文　献

[1] 苏仕平. 无线传感器网络的访问控制机制研究[D]. 兰州: 兰州大学, 2007.
SHU Shi-ping. The study of WSN access control mechanism [D]. Lanzhou: Lanzhou University, 2007.

[2] WANG H, SHENG B, LI Q. Elliptic curve cryptography-based access control in sensor networks[J]. Security and Networks, 2006(1): 127-137.

[3] LE Xuan-hung, LEE Sung-young, BUTUN I, et al. An energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography[J]. Communications and Networks, 2009, 6(11): 599-606.

[4] YU Shu-cheng, REN Kui, LOU Wen-jing. FDAC: Toward fine-grained distributed data access control in wireless sensor networks[J]. Institute of Electrical and Electronics Engineers, 2011, 22(4): 673-686.

[5] 杨洋, 丁仁杰, 闵勇. 基于受控对象的访问控制模型[J]. 电力系统自动化, 2003, 27(7): 36-40.
YANG Yang, DING Ren-jie, Min Yong. Object-based access control model[J]. Automation of Electric Power Systems, 2003, 27(7): 36-40.

[6] WANG H, LI Q. Distributed user access control in sensor networks[C]//IEEE International Conference on Distributed Computing in Sensor Systems. San Francisco, CA. USA: IEEE, 2006: 305-320.

[7] GURA N, PATEL A, WANDER A, et al. Comparing elliptic curve cryptography and RSA on 8-bit CPUs[J]. LNCS, 2004, 3156: 119-132.

[8] VAIDYA B, SILVA J S, RODRIGUES J J P C. Robust dynamic user authentication scheme for wireless sensor networks[M]. New York, NY, USA: ACM Press, 2009.

[9] CHAKRAVORTY R. A programmable service architecture for mobile medical care[C]//4th IEEE International Conference on Pervasive Computing and Communications. [S.l.]: IEEE, 2006.

[10] LE Xuan-hung, KHALID M, SANKAR R. An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare[J]. Journal of Networks, 2011, 6(3): 355-364.

[11] 孙利民, 李建中, 陈渝, 等. 无线传感器网络[M]. 北京: 清华大学出版社, 2005.
SUN Li-ming, LI Jian-zhong, CHENG Yu, et al. A. Wireless sensor networks[M]. BeiJing: Tsinghua University Press, 2005.

[12] 吴世忠, 祝世雄, 张文政. 应用密码学[M]. 北京: 机械工业出版社, 2000.
WU Shi-zhong, ZHU Shi-xiong, ZHANG Wen-zheng. Applied cryptography[M]. Beijing: Mechanical Industry Press, 2000.

[13] LIU Dong-gang. Efficient and distributed access control for sensor networks[J]. Wireless Networks, 2010, 16(8): 2151-2167.

编 辑 漆 蓉