doi:10.11959/j.issn.1000-436x.2016109

面向网络空间的访问控制模型

李凤华[1]，王彦超[1]，殷丽华[1]，谢绒娜[2]，熊金波[1]
(1. 中国科学院信息工程研究所信息安全国家重点实验室，北京 100093；2. 北京电子科技学院信息安全系，北京 100070)

摘 要：提出一种面向网络空间的访问控制模型，记为 CoAC。该模型涵盖了访问请求实体、广义时态、接入点、访问设备、网络、资源、网络交互图和资源传播链等要素，可有效防止由于数据所有权与管理权分离、信息二次/多次转发等带来的安全问题。通过对上述要素的适当调整可描述现有的经典访问控制模型，满足新的信息服务和传播模式的需求。给出了 CoAC 管理模型，使用 Z-符号形式化地描述了管理模型中使用的管理函数和管理方法。该模型具有极大的弹性、灵活性和可扩展性，并可进一步扩充完善，以适应未来信息传播模式的新发展。
关键词：网络空间安全；访问控制；管理场景；信息服务模式；信息传播模式
中图分类号：TP302 **文献标识码：**A

Novel cyberspace-oriented access control model

LI Feng-hua[1], WANG Yan-chao[1], YIN Li-hua[1], XIE Rong-na[2], XIONG Jin-bo[1]
(1. The State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China;
2. Department of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China)

Abstract: A novel cyberspace-oriented access control model was proposed, termed as CoAC, which avoided the threats by comprehensively considering vital factors, such as access requesting entity, general tense, access point, device, networks, resource, internet-based interactive graph and chain of resource transmission. By appropriately adjusting these factors, CoAC emulated most of typical access control models and fulfilled the requirements of new information service patterns and dissemination modes. The administrative model of CoAC was also presented and the functions and methods for administrating CoAC were described by utilizing Z-notation. CoAC is flexible and scalable, it can be further refined and expanded to figure out new opportunities and challenges in the upcoming access control techniques.
Key words: cyberspace security, access control, administrative scene, information service pattern, information dissemination mode

1 引言

云计算、大数据计算等新型计算技术的迅猛发展与移动通信、网络通信等通信手段的逐步交融不断推进着泛在网络的发展。借助泛在网络，通过“人”、“机”、“物”间的广泛互联互通，信息的计算与传播不再局限于单一的封闭环境，而是可以依据自身需求在任何时间、任何地点，使用任意终端设备、通过任意渠道接入任何网络获取相应的数据服务。这种无处不在的泛在网络服务模式必将进一步促使信息的计算和传播模式演化为通过“网络之网络”访问“系统之系统”。

收稿日期：2016-04-01；**修回日期：**2016-05-01
通信作者：殷丽华，yinlh_iie@163.com
基金项目：国家自然科学基金面上基金资助项目（No.61170251）；国家高技术研究发展计划（“863”计划）基金资助项目（No.2015AA016007）；国家自然科学基金-广东联合基金资助项目（No.U1401251）；国家自然科学基金青年基金资助项目（No.61502489）
Foundation Items: The National Natural Science Foundation of China Gener l Project(No.61170251), The National High Technology Research and Development Program of China (63 Program)(No.2015AA016007), The National Natural Science Foundation of China-Guangdong Joint Program (No.U1401251), The National Natural Science Youth Science Foundation of China (No.61502489)

然而具有动态开放特性的泛在网络在提供方便快捷的数据计算和管理服务的同时，也带来了相应的数据安全和隐私泄露等问题。因此，如何对这种动态开放环境下的用户访问行为进行有效管控、确保合法用户权益、防止非授权用户访问等问题亟待解决。

访问控制作为信息安全的核心技术之一，通过制定有效的访问控制策略，对用户的访问行为进行约束，实现对敏感资源访问的管控。自 20 世纪 70 年代以来，研究者提出了包括自主访问控制(DAC, discretionary access control)[1]、强制访问控制(MAC, mandatory access control)[2]、基于角色的访问控制(RBAC, role-based access control)[3]、基于任务的访问控制(TBAC, task-based access control)[4]、基于行为的访问控制(ABAC, action-based access control)[5]等大量的访问控制模型。然而，现有方案仅针对单一具体计算模式或应用场景，难以实现跨平台跨系统的细粒度、自适应的访问控制。

为了解决动态开放的跨域泛在网络中的细粒度访问控制问题，本文基于访问请求实体、广义时态、接入点、资源、访问设备、网络等要素提出了面向网络空间的访问控制（CoAC, cyberspace-oriented access control）模型，其特色与创新主要体现为以下 3 方面。

1) 本文提出了一种面向网络空间的访问控制模型，该模型综合考虑了访问控制过程涉及的各种要素，包括访问请求实体、广义时态、接入点、资源、访问设备、网络、网络交互图以及资源传播链等。该模型可对泛在网络中的信息及数据实施细粒度、多层次、灵活可变的访问控制。

2) 本文给出了管理场景的定义和 CoAC 管理模型的结构，描述了 CoAC 管理模型下的用户—管理场景和管理场景—管理权限的控制关系，形式化地描述了场景状态中的管理函数，同时给出了 CoAC 的管理方法。

3) 针对不同应用场景的实际需求，通过对访问请求实体、广义时态、接入点、访问设备、网络等访问控制要素进行适当调整，本文所提出的访问控制模型可对现有的 DAC、MAC、RBAC、ABAC 等访问控制模型进行有效描述。

2 相关工作

访问控制机制通过对用户访问信息资源的行为进行有效管控，使合法用户能够获得合理的系统访问权限，防止非授权用户访问系统资源。自 20 世纪 70 年代至今，访问控制技术大致经历了 4 个发展阶段。

第一阶段（20 世纪 70 年代至 90 年代）的研究主要针对大型主机中共享数据的访问权限管理问题。根据系统对机密性和完整性的不同需求，研究者提出了 BLP 模型和 Biba 模型对用户的读写操作进行限制。随着对计算机可信要求的不断提高，研究者又相应地提出了 DAC 和 MAC 模型。DAC 模型中，资源拥有者按照自己的意愿来决定是否将自己所拥有资源的访问权限授予其他用户，可以有选择地与其他用户共享其资源[1]。而 MAC 模型中，资源的访问权限是由享有标记权限的信息系统安全管理员进行分配[3]。DAC 可以提供较为灵活的访问控制策略，但是安全性较差。MAC 通过为用户和数据划分安全等级，实现了信息的单向流动，但由于 MAC 采用集中式管理方式，当系统用户数量增加时会给系统管理员带来极大的授权负担，同时权限管理效率偏低，缺少灵活性。

第二阶段（20 世纪 90 年代至 2000 年左右），随着信息系统与局域网技术的发展，DAC 与 MAC 的有限扩展特性已无法满足大规模系统中日益复杂的访问需求。因此，研究者在 DAC 和 MAC 的基础上引入角色和任务等概念，提出了 RBAC 模型[4~8]。RBAC 中通过角色对访问控制策略进行描述，系统中的用户和权限均对应于某些特定的角色。角色的引入实现了用户与权限之间的分离，简化了授权管理。在这些工作的基础上，为了解决多个 RBAC 系统间的分布式和跨域访问控制问题，研究者提出了面向分布式环境的角色访问控制(dRBAC, distributed role-based access control)[9,10]。

第三阶段，随着互联网技术的快速发展，信息的分布更加分散、用户的种类更加多元、访问控制策略也呈现出不同的形态，这种对象级粒度及策略多形态等新特性给访问控制带来了挑战。为了应对这一挑战，在考虑应用环境中的不同要素（如时空位置、用户属性、用户行为等）对访问控制的影响的基础上，研究者提出了如基于使用的访问控制[11~13]、基于时空关联的访问控制(temporal-based access control)[14~17]、基于属性的访问控制(attribute-based access control)[18~21]和基于行为的访问控制(action-based access control)[22]等模型。这些模型为解决复杂信息系统中的

细粒度访问控制和大规模用户动态扩展问题提供了较理想的解决方案。

第四阶段，随着云计算等新型计算环境的广泛普及，越来越多的用户通过云服务进行数据的计算与共享。虽然云服务为用户带来了便利，但由于其要求数据拥有者将数据上传至云服务器中，且无法保证云服务提供商完全可信，一旦数据上传，数据拥有者将无法保证其所拥有的数据不会被泄露。为了最大限度地保护数据的隐私安全，同时实现细粒度的访问控制，研究者提出了基于密码机制的访问控制模型，如基于时间的加密(TSE, time-specific encryption)[23~26]、基于身份的加密(IBE, identity-based encryption)[27]以及 ABE[28~35]等。ABE 机制使用属性作为构造加密算法的关键要素，利用非对称加密算法将属性及访问控制策略同密文和用户密钥相结合。当用户属性与密文属性的公共集合满足访问控制策略时才能对相应的密文进行解密，从而获取最终的结果。目前，ABE 研究大致可分为以下两类：基于密钥策略的 ABE(KP-ABE, key- policy attribute-based encryption)[28~30]和基于密文策略的 ABE(CP-ABE, ciphertext-policy attribute-based encryption)[31~35]。其中，CP-ABE 方案中数据拥有者可以利用不同的访问结构对其资源所对应的访问控制策略进行描述，并依据访问结构生成相应的加密密钥对其资源进行加密。相应的访问者则依据其自身属性集合生成解密私钥。当访问者具有的属性满足访问控制策略时，用户私钥可以对相应的密文进行解密。这种方式下访问控制策略由数据拥有者设定，数据拥有者自由度较高。

虽然目前的访问控制模型可有效解决单一封闭环境下的访问控制问题，但这些访问控制模型不足以应对泛在网络空间新的信息服务模式和传播方式所带来的新挑战（如数据的所有权和管理权分离、信息的二次/多次转发等），因此，需要提出一种新的访问控制模型，更为细粒度地控制信息的使用和传播。

3　系统模型介绍

本节首先对面向网络空间的系统模型进行描述，然后对模型中所涉及广义时态、访问设备、接入点、网络的概念及其层次结构等概念进行定义并给出相应的形式化描述。结合相关定义及模型描述，本文提出面向网络空间的访问控制模型。

3.1　系统模型

如图 1 所示，本文提出的面向网络空间的访问控制系统由访问请求实体、网络/广义网络及资源 3 部分组成。

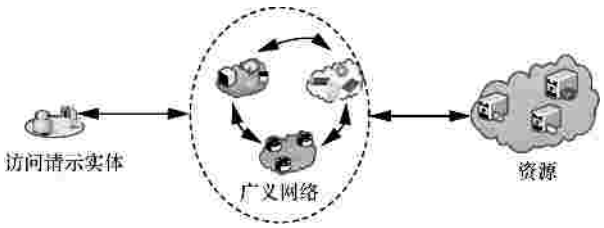

图 1　系统模型

访问请求实体指资源访问的发起方，访问实体依据生成访问请求时所使用的设备、广义时态、接入点、所要访问的资源等要素获取相应权限。

网络/广义网络指信息传播的载体。访问请求实体发起资源的访问请求经由网络/广义网络到达资源服务器。网络/广义网络可以是任意互联的网络传播通道的集合（如移动核心网、有线网络等），也可以是基于传统媒介的传播方式（如光盘、U 盘、纸张等）。

资源指访问的对象及其相关属性。

在该系统模型中，访问请求实体发起对相应资源的访问请求。该请求经由广义网络到达资源服务器。资源服务器将访问请求实体在生成访问请求中所使用设备、广义时态、接入点、所要访问的资源等信息与预先设定的访问控制策略进行匹配。如果匹配成功，则将资源通过广义网络返回给访问请求实体。反之，资源服务器将拒绝访问请求实体对资源的访问。

3.2　相关定义

定义 1　访问请求实体。资源访问的发起方，记为 $q=<u,a,r>$，其中，u 表示用户的唯一标识；a 表示访问代理的唯一标识，访问代理可以是一个装置、进程或用户等；r 为用户角色的唯一标识。

根据定义 1，网络空间中的用户集合记为 $U=\{u_i \mid i\in N^*\}$，访问代理集合记为 $A=\{a_i \mid i\in N^*\}$，角色集合记为 $R=\{r_i \mid i\in N^*\}$，访问请求实体集合记为

$$Q=\{<u,a,r> \mid u\in U, a\in A, r\in R\}$$

约定 $<u,\cdot,\cdot>$ 表示用户为 u 的所有访问请求实体，$<u,\cdot,r>$ 表示用户为 u、角色为 r 的所有访问请求实体。其他情况以此类推，不再详述。

定义 2　广义时态(general temporal factor)。访问请求实体进行资源访问时所有与时态相关的信息，记为

$T=\{<interval, period, duration> \mid interval \in 2^{T^{IN}}, period \in R^{+}, duration \in R^{+}\}$

其中，$interval \in 2^{T^{IN}}$ 表示起始时间和终止时间，$T^{IN}=\{[begin_i, end_i] \mid i \in N^{*}\}$，$period$ 表示时间周期，$duration$ 表示持续时间，有如下约定。

当 $|T^{IN}|=1$ 时，$t=<[begin, end], period, duration>$；当 $|T^{IN}|>1$ 时，$t=<[begin_1, end_1], [begin_2, end_2], \cdots, [begin_{|T^{IN}|}, end_{|T^{IN}|}], period, duration>$。

定义 3 接入点(access point)。资源访问请求实体在发起访问请求时首次接入网络系统中的空间位置和网络标识。接入系统通过网络标识唯一区分不同访问，网络标识记为 $l=<l^{SPID}, l^{NETID}>$，其中，$l^{SPID}=<x,y,z> \in L^{SPID}$ 表示三维空间位置坐标，例如 x 表示经度，y 表示纬度，z 表示高度；$l^{NETID} \in 2^{L^{NETID}}$ 表示网络接入唯一标识，包括手机唯一标识码 imei、基站 bs、网络号 nid、MAC 地址 mac、端口 port、IP 地址 ip、域名 domain 等。接入点集合记为

$$L=\{<l^{SPID}, l^{NETID}> \mid l^{SPID} \in L^{SPID}, l^{NETID} \in 2^{L^{NETID}}\}$$

定义 4 资源(resource)。访问的对象及其相关属性，记为 $o=<c^O, g^O, s^O>$，其中，$c^O \in C^O$ 表示资源的内容；$g^O \in G^O$ 表示资源的通用属性；$s^O \in S^O$ 表示资源的安全属性。资源的通用属性指资源的类别、来源等属性，记为

$$G^O=\{<g^{O_{SORT}}, g^{O_{SOURCE}}, g^{O_{SIZE}}, g^{O_{TIME}}, \cdots> \mid g^{O_{SORT}} \in G^{O_{SORT}}, g^{O_{SOURCE}} \in G^{O_{SOURCE}}, g^{O_{SIZE}} \in G^{O_{SIZE}}, g^{O_{TIME}} \in G^{O_{TIME}}, \cdots\}$$

其中，属性项集合 $G^{O_{SORT}}$ 指资源类别，包括数据库表、文件、网页等资源类别；属性项集合 $G^{O_{SOURCE}}$ 指信息的来源方式，包括创建、转发以及重组等；属性项集合 $G^{O_{SIZE}}$ 指资源的大小，记为 $G^{O_{SIZE}}=\{g_i^{O_{SIZE}} \mid i \in N^{*}\}$；属性项集合 $G^{O_{TIME}}$ 指资源的时态属性。资源的安全属性集合指资源允许执行的操作、是否允许转发、销毁方式等，记为

$$S^O=\{<s^{O_{OP}}, s^{O_{DIS}}, s^{O_{DE}}, s^{O_{SEC}}, s^{O_{ENC}}, \cdots> \mid s^{O_{OP}} \in 2^{s^{O_{OP}}}, s^{O_{DIS}} \in 2^{s^{O_{DIS}}}, s^{O_{DE}} \in S^{O_{DE}}, s^{O_{SEC}} \in S^{O_{SEC}}, s^{O_{ENC}} \in S^{O_{ENC}}, \cdots\}$$

其中，安全属性项集合 $S^{O_{OP}}$ 指允许对资源执行的操作，安全属性项集合 $S^{O_{DIS}}$ 指资源的分发方式，安全属性项集合 $S^{O_{DE}}$ 指资源的销毁方式，安全属性项集合 $S^{O_{SEC}}$ 指资源的安全等级，安全属性项集合 $S^{O_{ENC}}$ 指资源的加密方式。资源的集合可记为集合 $O=\{<c^O, g^O, s^O> \mid c^O \in C^O, g^O \in G^O, s^O \in S^O\}$。

定义 5 访问设备(device)。访问请求实体访问资源时所使用的设备，其组成特征和相关属性记为 $<g^D, s^D, t>$，其中，g^D 表示访问设备的通用属性，s^D 表示访问设备的安全属性，t 表示设备的时间属性。访问设备的组成特征和相关属性的集合记为

$$D=\{<g^D, s^D, t> \mid g^D \in 2^{G^D}, s^D \in 2^{S^D}, t \in T\}$$

其中，G^D 表示设备通用属性集合，包括处理器(CPU)、操作系统(OS)、接口(interface)、内存(memory)、硬盘(disk)、应用程序(app)等。S^D 表示设备安全属性集合，主要包括最小和最大风险容许系数(mincoe 和 maxcoe)、安全域(security domain)、安全等级(security level)、安全软件模块(security-soft module)、安全硬件模块(security-hard module)。T 为广义时态集合，表示访问设备的时间属性。

定义 6 网络(network)。访问控制过程中信息传播的载体，是局域网内、广域网内或者任意设备间信息传播通道的集合。网络可以用有向属性图 $NG=(V, E)$ 表示。

顶点 V 表示网络中的设备或子网，记为 $<n^V, g^V, s^V>$，其中，n^V 表示顶点名，指代一个设备或网络；g^V 表示顶点 v 的通用属性，顶点的通用属性集合记为

$$G^V=\{<g^{V_{NT}}, g^{V_{IO}}, g^{V_{NP}}> \mid g^{V_{NT}} \in G^{V_{NT}}, g^{V_{IO}} \in G^{V_{IO}}, g^{V_{NP}} \in 2^{G^{V_{NP}}}\}$$

其中，$G^{V_{NT}}$ 表示网络类型集合，包括 Lan、Wan、WLan 等；$G^{V_{IO}}$ 表示顶点类型集合，包括 in、out、inout，interior 等；$G^{V_{NP}}$ 表示网络协议集合，包括 TCP/IP、Bluetooth、802.11a/b/g/n、ISO11898、CDMA2000/WCDMA/TD-SCDMA、LTE 等；s^V 表示顶点 v 的安全属性，如果顶点表示设备，则安全属性如定义 5 所示，如果顶点表示网络，则顶点的安全属性集合记为

$$S^V=\{<s^{V_{CON}}, s^{V_{ENC}}, s^{V_{PT}}> \mid s^{V_{CON}} \in S^{V_{CON}}, s^{V_{ENC}} \in S^{V_{ENC}}, s^{V_{PT}} \in 2^{S^{V_{PT}}}\}$$

其中，$S^{V_{CON}}$ 表示管控信息，$S^{V_{ENC}}$ 表示加密类型集合，包括 3DES、RSA、ECC、AES、SM2/3/4，$S^{V_{PT}}$ 表示安全协议类型集合，包括 SSL、SSH、HTTPS、

MANCONFIRM 等，顶点集合记为 $V=\{<n_i^V, g_i^V, s_i^V>| n_i^V \in N^V, g_i^V \in G^V, s_i^V \in S^V, i \in N^*\}$。

边 E 表示顶点间的连通属性和安全属性，记为 $<v_m, v_n, g^E, s^E>$，其中 $v_m \in V$ 为边 e 的起点，$v_n \in V$ 为边 e 的终点，$g^E \in G^E$ 表示边 e 的连通属性，连通属性集合表示为

$$G^E=\{<g^{E_M}, g^{E_{NP}}>| g^{E_M} \in 2^{G^{E_M}}, g^{E_{NP}} \in 2^{G^{E_{NP}}}\}$$

其中，G^{E_M} 表示性能属性集合，包括 Bandwidth、QoS、Hop、Delay 等，$G^{E_{NP}}$ 表示协议属性集合包括 TCP/IP、Bluetooth、802.11a/b/g/n、ISO11898、CDMA2000/WCDMA/TD-SCDMA、LTE 等；$s^E \in S^E$ 表示边 e 的安全属性，安全属性集合 $S^E=\{<s^{E_{ENC}}, s^{E_{PR}}>| s^{E_{ENC}} \in S^{E_{ENC}}, s^{E_{PR}} \in S^{E_{PR}}\}$，其中，$S^{E_{ENC}}$ 表示加密类型集合，包括 3DES、RSA、ECC、AES、SM2/3/4 等，$S^{E_{PR}}$ 表示安全协议类型集合，包括 SSL、SSH、HTTPS、MANCONFIRM 等，边的集合可记为

$$E=\{<v_{i_m}, v_{i_n}, g_i^E, s_i^E>| v_{i_m}, v_{i_n} \in V, g_i^E \in G^E, s_i^E \in S^E, i, i_m, i_n \in N^*\}$$

定义 7　网络交互图(internet-based interactive graph)。网络中任意 2 个顶点间连通路径构成的网络子图，网络交互图由交互行为及网络传播链组成，具体定义如下。

交互行为指由 2 个连通且相邻的节点及其边组成的有向子图。具体定义如下：对于网络有向属性图 NG 上的顶点 v 和 w，存在 $<v, w, g^E, s^E> \in E$，则顶点 v 和 w 之间的交互行记为 $N=<v \rightarrow w, t>$，其中，t 表示交互行为的时间属性。网络有向属性图 NG 上的所有交互行为组成网络交互行为的集合，记为

$$N^G=\{<v_i \rightarrow w_i, t_i>| \forall e_i=<v_i, w_i, g_i^E, s_i^E> \in E, i \in N^*, t_i \in T\}$$

网络传播链指基于网络节点的有序交互行为的集合，实际指图中的一条有向路径，定义如下。

设 v 为信息发起点，w 为信息接收点，v 和 w 之间的网络传播链集合记为

$$N(v,w)=\{<N_{i_1}, N_{i_2}, \perp, N_{i_j}, \perp, N_{i_k}>| i \in N^*, k \in N^*, i_j \in N^*, \forall 1<j \le k, N_{i_j}=<v_{i_j} \rightarrow w_{i_j}, t_{i_j}> \in N^G\}$$

其中，$\forall 1<j \le k-1$，$w_{i_j}=w_{i_{(j+1)}}$ $v_{i_1}=v$，$w_{i_k}=w$ 且 $t_{i_j} \in 1$ 网络传播链上的交互行为集合记为

$$N^C(v,w)=\{<v_{i_j} \rightarrow w_{i_j}, t_{i_j}>| \forall N_i(v,w)=<N_{i_1}, N_{i_2}, \perp, N_{i_j}, \perp, N_{i_k}> \in N(v,w), i \in N^*, k \in N^*, i_j \in N^*, \forall 1<j<N\}$$

网络有向属性图 NG 中边是单向或双向的，顶点 v 和 w 之间的网络交互图指 v 和 w 的所有连通传播链组成的有向属性图，网络交互图是单向边和双向边的任意组合，记为 $NG_N=(V(v,w), E(v,w))$，其中

$$V(v,w)=\{<n_{i_j}^V, g_{i_j}^V, s_{i_j}^V>| i_j \in N^*, \forall N_{i_j}=<v_{i_j} \rightarrow w_{i_j}, t_{i_j}> \in N^C(v,w), v_{i_j} \in V\} \cup \{w\}$$

$$E(v,w)=\{<v_{i_j}, w_{i_j}, g_{i_j}^E, s_{i_j}^E>| i_j \in N^*, \forall N_{i_j}=<v_{i_j} \rightarrow w_{i_j}, t_{i_j}> \in N^C(v,w), e_{i_j} \in E\}$$

定义 8　资源传播链(resource chain)。用于描述资源传播过程中信息交换过程。资源交换指资源在 2 个资源访问请求实体之间的一次传输，记为 $<s \rightarrow r, o, t>$，其中，s 表示资源的发起或转发者，r 表示资源的接收者，o 表示资源，t 表示广义时态状态。

某一资源的某次传播链是资源交换的有序集合，记为

$$O_i^C(s_i, r_i, o)=\{<I_{i,1}, I_{i,2}, \perp, I_{i,k}>| o \in O, I_{i,l}=<s_{i,l} \rightarrow r_{i,l}, o, t_{i,l}>, s_{i,l}=r_{i,l+1}, s_{i,1}=s_i, r_{i,k}=r_i, s_i \in Q, r_i \in Q, s_{i,l} \in Q, r_{i,l} \in Q, 1<l \le k-1, t_{i,l} \in T\}$$

其中，s_i 为资源传播起者，r_i 为资源传播的接收者。

资源传播链的集合记为 $O^C=\{O_i^C(s, r_i, o)| i \in N^*\}$，资源传播发起者为 s，资源传播的接收者为 $r_1, r_2, \perp, r_i \perp$。

定义 9　场景(scene)。指信息访问实体 q 启动会话 s 获得权限 p 时所需要的广义时态、接入点、设备以及网络信息，记为 sc，可用四元组 (t, l, d, ng) 表示，其中，$t \in T$, $l \in L$, $d \in D$, $ng \in NG$。

定义 10　场景约束(constraints-sc)。指启动会话 s 之后，信息访问实体仅能通过场景 sc 获取相应权限 p。

定义 11　资源访问实体—场景分配(qsc)。指对资源访问实体分配场景 sc 的过程，qsc 的集合记为 QSC。

定义 12　实体场景—权限分配(qscp)。指对实体场景 qsc 分配权限 p 的过程，$qscp$ 的集合记为 $QSCP$。

表 1 给出了场景约束的描述，其中，可用(enable)/不可用(disable)及激活(active)的定义与文献[22]类似。S 表示会话集；assign/deassign 表示分配和解分配关系；N_{active} 表示激活数量；N_{max} 表示所

表 1 场景约束描述

约束分类	约束		描述
场景可用约束	资源访问实体—场景约束		$(Q, S, T, L, D, NG, \text{assigin}_Q/\text{deassign}_Q\ sc\ \text{to}\ q)$
	场景可用/不可用		$(Q, S, T, L, D, NG, \text{enable/disable}\ sc)$
	资源访问实体、场景—权限分配		$(Q, S, T, L, D, NG, \text{assigin}_P/\text{deassign}_P\ p\ \text{to}\ sc)$
场景激活约束	激活场景的数量	用户	$(Q, S, T, L, D, NG, N_{\text{active}}, \text{active}_{Q\_\text{total}})$
		权限	$(Q, S, T, L, D, NG, N_{\text{active}}, \text{active}_{P\_\text{total}})$
	当前系统中激活场景的总数量	用户	$(Q, S, T, L, D, NG, N_{\max}, \text{active}_{Q\_\text{total}})$
		权限	$(Q, S, T, L, D, NG, N_{\max}, \text{active}_{P\_\text{total}})$

能激活的最大数量；$\text{active}_{Q\_\text{total}}$ 表示资源访问实体激活的所有场景的数量；$\text{active}_{P\_\text{total}}$ 表示得到某个权限的所有激活场景的数量。

3.3 层次结构及其继承关系

广义时态、接入点、访问设备和网络等要素具有层次结构，具体定义如下。

定义 13 广义时态层次结构 $TH \subseteq T \times T$ 是广义时态集合 T 上的偏序关系。对于任意的 $t_i, t_j \in T$，$(t_i, t_j) \in TH$ 当且仅当 $t_i \geq t_j$ 成立。如果 $(t_i, t_j) \in TH$，则称 t_i 是 t_j 的高级时态，t_j 是 t_i 的低级时态，记为 $t_i \geq t_j$。如果 $(t_i, t_j) \in TH$，且不存在 t_k 使 $t_i \geq t_k$ 与 $t_k \geq t_j$ 成立，则称 t_i 是 t_j 的直接高级时态。

定义 14 接入点层次结构 $LH \subseteq L \times L$ 是接入点集合 L 上的偏序关系。对于任意的 $l_i, l_j \in L$，$(l_i, l_j) \in LH$ 当且仅当 $l_i \geq l_j$ 成立。如果 $(l_i, l_j) \in LH$，则称 l_i 是 l_j 的高级接入点，l_j 是 l_i 的低级接入点，记为 $l_i \geq l_j$。如果 $(l_i, l_j) \in LH$，且不存在 l_k 使得 $l_i \geq l_k$ 与 $l_k \geq l_j$ 成立，则称 l_i 是 l_j 的直接高级接入点。

定义 15 访问设备层次结构 $DH \subseteq D \times D$ 是广义设备集合 T 上的偏序关系。对于任意的 $d_i, d_j \in D$，$(d_i, d_j) \in DH$ 当且仅当 $d_i \geq d_j$ 成立。如果 $(d_i, d_j) \in DH$，则称 d_i 是 d_j 的高级设备，d_j 是 d_i 的低级设备，记为 $d_i \geq d_j$。如果 $(d_i, d_j) \in DH$，且不存在 d_k 使 $d_i \geq d_k$ 与 $d_k \geq d_j$ 成立，则称 d_i 是 d_j 的直接高级设备。

定义 16 网络层次结构 $NGH \subseteq NG \times NG$ 是网络集合 NG 上的偏序关系。对于任意的 $ng_i, ng_j \in NG$，$(ng_i, ng_j) \in NG$ 当且仅当 $ng_i \geq ng_j$ 成立。

如果 $(ng_i, ng_j) \in NGH$，则称 ng_i 是 ng_j 的高级网络，ng_j 是 ng_i 的低级网络，记为 $ng_i \geq ng_j$。如果 $(ng_i, ng_j) \in NGH$，且不存在 ng_k 使 $ng_i \geq ng_k$ 与 $ng_k \geq ng_j$ 成立。

由于场景综合考虑了以上要素，因此场景也具有层次结构，场景层次定义如下。

定义 17 场景层次结构 $SCH \subseteq SC \times SC$ 是场景集合 SC 上的偏序关系。对于任意的 $sc_i, sc_j \in SC$，$(sc_i, sc_j) \in SC$ 当且仅当 $sc_i \geq sc_j$ 成立。

如果 $(sc_i, sc_j) \in SCH$，则称 sc_i 是 sc_j 的高级场景，sc_j 是 sc_i 的低级场景，记为 $sc_i \geq sc_j$。如果 $(sc_i, sc_j) \in SCH$，且不存在 sc_k 使 $sc_i \geq sc_k$ 与 $sc_k \geq sc_j$ 成立，则称 sc_i 是 sc_j 的直接高级场景。

3.4 面向网络空间的访问控制模型形式化描述

根据“场景”的概念，参考文献[22]中的形式化描述方法，本节对面向网络空间的访问控制模型进行形式化描述。图 2 给出了网络空间访问控制模型的结构图，具体元素定义如下。

定义 18 面向网络空间的访问控制模型具有以下组件。

1) Q、SC、P、S（访问请求实体、场景、权限、会话），其中，$SC=(T, L, D, NG)$，Q、T、L、D、NG 分别表示访问请求实体、广义时态、接入点、资源、访问设备、网络，定义详见 3.1 节。

2) $QSC \subseteq Q \times SC$，表示多对多的访问请求实体—场景的分配关系。

3) $QSCP \subseteq QSC \times P$，表示多对多的实体场景—权限的分配关系。

4) $entity{:}session \to Q$，将会话 s 映射到单个访问请求实体 $entity(s)$ 的函数。

5) $scene: S \to 2^{SC}$，将会话 s 映射到场景集合的函数，其中

$$scene(s) \subseteq \{sc \mid (\exists sc' \geq sc)[entity(s), a' \in QSC]\}$$

会话 s 具有权限

$$\bigcup_{sc \in scene(s_i)} \{p \mid (\exists q' \leq q)[(q'', p) \in SCP]\}$$

除此之外，在面向网络空间的访问控制模型中，网络交互图通过限制资源在网络中的传输路径，约束访问请求实体对资源的访问权限。当访问

请求实体 q 通过网络向服务器提出资源 o 的访问请求时，服务器在得到访问请求的同时将获得 q 的网络位置信息，如 IP 地址、端口号等。服务器以自身地址为起点，以 q 的网络位置信息为终点发起“路径发现”，若发现的路径包含于资源 o 的网络交互图则该次访问请求被允许，否则被拒绝。例如，按访问控制策略，某公司高管 a 有权限访问 o。然而若 a 出差在外，其接入公司网络的链路不包含于 o 的网络交互图，此时 o 不能被 a 访问。

资源传播链通过限制资源在不同访问请求实体间的转发路径约束请求实体对资源的访问权限，实现资源的受控二次/多次分发、信息保护及溯源。当 q 向服务器提出 o 的访问请求，服务器判断 q 是否存在于 o 的资源传播链，若 q 存在于资源 o 的资源传播链，则该次访问请求被允许，否则访问请求被拒绝。当 q 向服务器请求 o 的转发操作权限，服务器将判断 q 转发资源的接收者是否存在于资源传播链，若存在，则允许转发操作，否则拒绝，从而实现资源的受控二次/多次分发。通过资源传播链，还能实现资源的溯源。资源在不同访问请求实体间进行转发，经由的每个访问请求实体的信息都将记录于资源的元数据中或被返回服务器，通过资源本身携带的元数据或者服务器中记录的资源元数据可以实现资源的溯源。

4　管理模型

4.1　管理场景与管理模型

在面向网络空间的访问控制模型中，管理场景用来对其他场景进行安全管理。所以管理场景自身的安全性关系到访问控制模型整体安全性。令 AQ 表示管理资源访问实体集合，通过引入受限的广义时态、接入点、访问设备和网络对管理场景进行定义。

定义 19　管理场景(ADSC，administration scene)。$ADSC$ 可以表示为一个五元组(aq, $limt$, $liml$, $limd$, $limng$)，其中，$aq\in AQ$, $limt\in T$, $liml\in L$, $limd\in D$, $limng\in NG$。$limt$ 的集合记为 $LIMT$，$liml$ 的集合记为 $LIML$，$limd$ 的集合记为 $LIMD$，$limng$ 的集合记为 $LIMNG$。$ADSC$ 是一种特殊的场景，满足场景的所有属性，但其广义时态、接入点、访问设备和网络属性是受限的。

通过在受限的场景中引入可信平台模块，场景中的管理场景可以提供更安全的服务，从而对一般场景进行可信的管理。借鉴文献[22]中的形式化描述方法，令 ADP 表示管理权限的集合，本文所提出的管理模型描述如下。

定义 20　管理模型具有以下组件。

Q：资源访问实体。

P：权限集合。

S：会话集合。

ADP：管理权限集合。

$constraints$：约束条件。

SC：一般场景集合，SC=(T，L，D，NG)。其中，T、L、D、NG 分别表示广义时态、接入点、访问设备和网络。

$ADSC$：管理场景集合，$ADSC$=(AQ，$LIMT$，$LIML$，$LIMD$，$LIMNG$)。其中，AQ 为管理资源访问实体，$LIMT$、$LIML$、$LIMD$、$LIMN$ 分别为受限广义时态、受限接入点、受限访问设备和受限网络。

模型中包含如下分配关系。

$SCSC\subseteq SC\times SC$:表示多对多的场景—场景的分配关系。

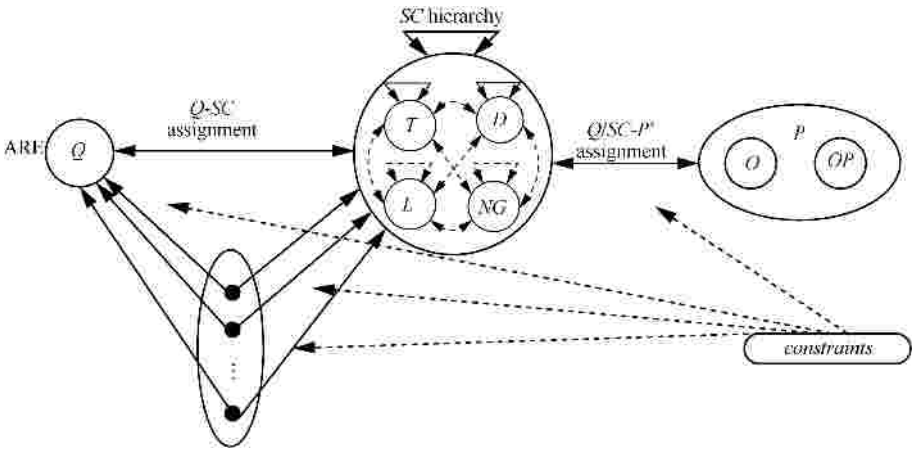

图 2　面向网络空间的访问控制模型

$QSC \subseteq Q \times SC$ ：表示多对多的资源访问实体—场景的分配关系。

$QADSC \subseteq Q \times ADSC$ ：表示多对多的用户—管理场景的分配关系。

$ADSCP \subseteq ADSC \times P$ ：表示多对多的管理场景—权限的分配关系。

模型包含以下偏振序列。

$SCH \subseteq SC \times SC$ ：表示场景集合 SC 上的偏序关系。

$ADSCH \subseteq ADSC \times ADSC$ ：表示管理场景 ADSC 上的偏序关系。

模型所涉及的映射函数定义如下。

$entity: S \to Q$：将会话 s 映射到单个资源访问实体 $entity(s)$ 的函数（会话生命周期内保持不变）。

$scene: S \to 2^{SC \cup ADSC}$ ：将会话 s 映射到场景集合的函数，其中，

$$scene(s) \subseteq \{sc \mid (\exists sc' \geq sc)[entity(s), a' \in QSC \cup QADSC]\}$$

会话 s_i 具有权限

$$\bigcup_{sc \in scene(s)} \{p \mid (\exists q'' \leq q)[(q'', p) \in SCP \cup ADSCP]\}$$

图 3 给出了场景管理模型的结构，其中包含了一般场景层次、管理场景层次、广义时态层次、访问设备层次和网络层次。从图中可知，场景管理模型通过管理场景集合 ADSC 对资源访问实体—场景分配、场景—权限分配和场景状态进行管理。场景管理模型利用 *constraints* 对资源访问实体—场景、场景—权限、资源访问实体—管理场景分配、管理场景—管理权限分配对管理场景进行控制。由于管理场景在受限的广义时态、访问设备、接入点和网络下进行一般的场景管理，可以保证管理场景的安全性。

4.2 管理模型的功能

基于文献[22]中管理模型下资源访问实体—场景分配、资源访问实体—场景撤销、场景—权限分配、场景—权限撤销的控制关系的相关定义，CoAC 中的资源访问实体—管理场景和管理场景—管理权限的控制关系的定义以及场景状态管理中的相关函数如下。

定义 21 先决条件是通过∧和∨操作符对 x 和 $\bar{x}$ 进行操作的布尔表达式。其中，$x \in SC$ 是一般场景。对于资源访问请求实体 q，有如下结论。

若 x 为真，则

$$(\exists x' \geq x)((q, x') \in QA \wedge (q, x') \notin QADSC)$$

若 $\bar{x}$ 为真，则

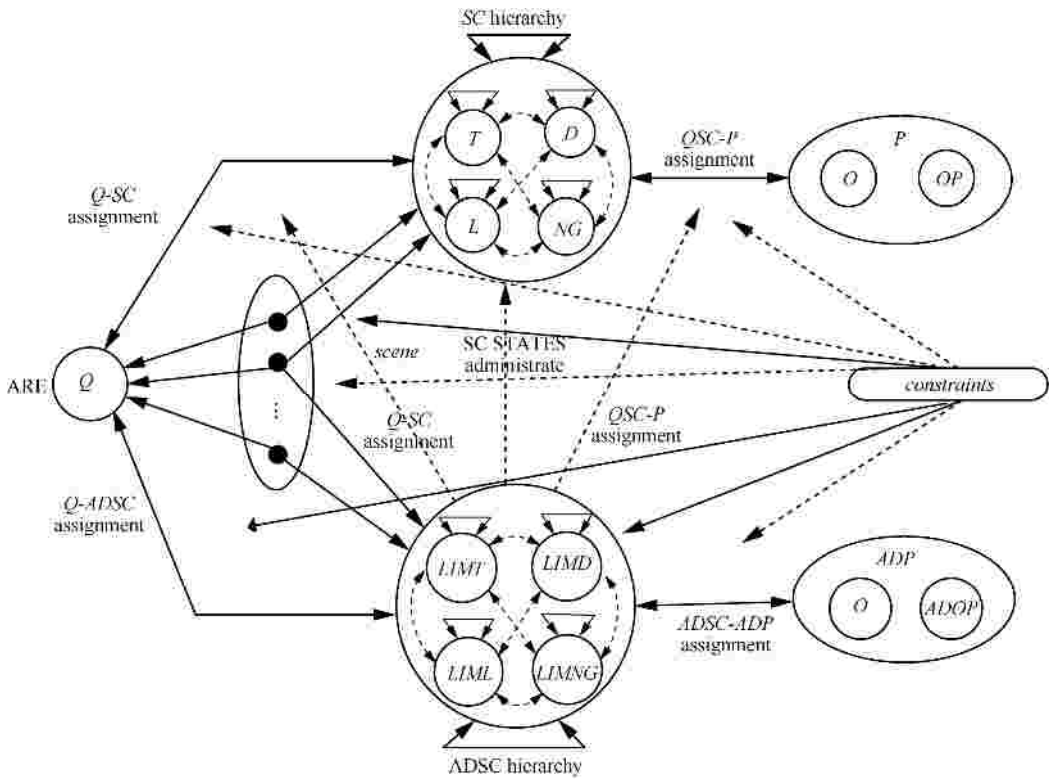

图 3 管理模型

$$(\forall x' \geq x)((q,x') \in QA \wedge (q,x') \notin QADSC)$$

对于给定一般场景集合 SC**，令** CSC **表示使用** SC **中场景可能得到的所有先决条件。**

$x \in ADSC$ **是管理场景，对于资源访问请求实体，若** x **为真，则**

$$(\exists x' \geq x)((q,x') \in QADSC \wedge (q,x') \notin QA)$$

若 $\overline{x}$ **为真，则**

$$(\forall x' \geq x)((q,x') \in QADSC \wedge (q,x') \notin QA)$$

对于给定的管理场景集合 $ADSC$**，令** $CADSC$ **表示使用** $ADSC$ **中管理场景可能得到的所有先决条件。**

定义 22　管理模型分别使用如下关系对资源访问实体—管理场景进行分配、对已经分配的资源访问实体—管理场景进行撤销。

$$\text{can.assignsq} \subseteq ADA' \cdot CADSC \cdot 2^{ADSC}$$

$$\text{can.revokesq} \subseteq ADA' \cdot 2^{\{ADSC \setminus \{\text{superadsc}\}\}}$$

其中， $ADA' = ADA\{a \mid \acute{o} a' \in ADA, a' < a\}$**，**superadsc **是系统设定的超级管理场景，位于管理场景层次结构的顶层，且不能被撤销。设** Z **表示“可被分配的管理场景”的集合，**can.assignsq(x, y, Z) **表示管理场景** x**(或** $\forall x' > x$**)可以对满足先决条件** y **的用户分配管理场景** $z \in Z$**。设** Z **表示撤销的管理行为集合，则** can.revokesq(x, Z)**表示管理场景** x **可以撤销分配给用户的管理场景集合** Z**。**

定义 23 管理模型分别使用如下关系对管理场景—管理权限进行分配和撤销。

$$\text{can.assignsp} \subseteq ADA' \cdot CADSC \cdot 2^{ADP}$$

$$\text{can.revokesp} \subseteq ADA' \cdot 2^{ADP}$$

其中， $ADA' = ADA\{a \mid \acute{o} a' \in ADA, a' < a\}$**，** ADP **表示各管理类权限的集合，包括资源访问实体管理、场景管理、权限管理、访问请求实体—场景分配管理、场景—权限分配管理、场景状态管理等。**

下面采用 Z**-符号对场景状态管理中的添加、修改和删除操作进行形式化定义。其中，** $NAME$ **是抽象数据类型，表示场景模型中的场景、资源访问请求实体、广义时态、接入点、访问设备、网络、会话、权限等组件，** $QUERYS$ **为访问请求实体集合，** $SCENES$ **为场景集合，** $TSTAES$ **为广义时态状态集合，** $LOCATES$ **为接入点集合，** $DEVICES$ **为访问设备集合，** $NETGRAPHYS$ **为网络集合，** $SESSIONS$ **为会话集合，** OPS **为操作集合，** OBS **为对象集合。**

AddScene(*scene*:*NAME*) <

scene∉ *SCENES*

if *scene.query*∉ *QUERYS*

then *QUERY*'=*QUERYS* ∪ {*role*}

if *scene.temporalstate*∉ *TSTAES*

then *TSTATES*'=*TSTATES* ∪ {*temporalstate*}

if *scene.locate*∉ *LOCATES*

then *LOCATES*'=*LOCATES* ∪ {*locate*}

if *scene.device*∉ *DEVICES*

then *DEVICES*'=*DEVICES* ∪ {*device*}

if *scene.netgraphy*∉ *NETGRAPHYS*

then *NETGRAPHY*'=*NETGRAPHYS* ∪ {*netgraphy*}

SCENES'=*SCENES* ∪ {*scene*}

QSC'=*QSC* ∪ {$scene \rightarrow f$ }

SCP=*SCP* ∪ {$scene \rightarrow f$ } >

ModifyScene(*scene*, *query*, *temporalstate*, *locate*, *device*, *netgraphy*: *NAME*) <

scene∈ *SCENES*

if *scene.query*∉ *QUERYS*

then *QUERY*'=*QUERYS* ∪ {*query*}

if *scene.temporalstate*∉ *TSTAES*

then *TSTATES*'=*TSTATES* ∪ {*temporalstate*}

if *scene.locate*∉ *LOCATES*

then *LOCATES*'=*LOCATES* ∪ {*locate*}

if *scene.device*∉ *DEVICES*

then *DEVICES*'=*DEVICES* ∪ {*device*}

if *scene.netgraphy*∉ *NETGRAPHYS*

then *NETGRAPHY*'=*NETGRAPHYS* ∪ {*netgraphy*}

[∀ *s* ∈ *SESSIONS*　*scene* ∈ *SCENE*　*scene*(*s*) ⇒ DeleteSession(*s*)]

Scene'=(*temporalstate*, *locate*, *device*, *netgraphy*)

SCENE'=*QSC*\{*scene*} ∪ {*scene*'}

QSC'=*QSC* ∪ { ∀ *q* ∈ *QUERY*　$scene \rightarrow q$} ∪ {$scene' \rightarrow f$ }

SCP'=*SCP* ∪ { ∀ *op* ∈ *OPS*; ∀ *ob* ∈ *OBS*　$scene \rightarrow (op, ob)$} ∪ {$scene' \rightarrow f$ } >

DeleteScene(*scene*:*NAME*) <

scene∈ *SCENES*

"[*s* ∈ *SESSIONS.action* ∈ *SCENE.action*(*s*) ⇒ DeleteSession(*s*)]"

[" ∀ *sc* ∈ *SCENES*\\{*scene*"}"*sc.q* ≠ *scene.q* ⇒ *QUERYS*'=*QUERYS*\{*scene.q*}]"

["∀ *sc*∈ *SCENES*\\{*scene*"}"*sc.temporalstate* ≠ *scene.temporalstate* ⇒ *TSTATES*'=*TSTATES*\ {*scene.temporalstate*}]"

["∀ *sc*∈ *SCENES*\\{*scene*"}"*sc.locate* ≠ *scene. locate*⇒ *LOCATES*'=*LOCATES*\{*scene.locate*}]"

["∀ *sc*∈ *SCENES*\\{*scene*"}"*sc.device* ≠ *scene. device*⇒ *DEVICES*'=*DEVICES*\{*scene. device*}]"

["∀ *sc* ∈ *SCENES*\\{*scene*"}"*sc.netgraphy* ≠ *scene. netgraph* ⇒ *NETGRAPHY*'=*NETGRAPHYS*\{*scene.netgraphy*}]"

"*QSC*'=*QSC*\\{∀ *q*∈ *QUERY.scene* → *q*}"

"*SCP*'=*SCP* ∪ "{" ∀ *op* ∈ *OPS*; ∀ *ob* ∈ *OBS scene* → " ("*op,ob*")}

"*SCENES*'=*SCENES*\\{*action*}" >

通过识别访问请求实体的用户身份、访问代理、角色信息、广义时态、接入点、访问设备、网络等，利用表 2 所示相关函数可以实现场景的访问请求实体—场景、场景—权限和场景状态进行管理。

5 CoAC 可扩展性分析

本文提出的 CoAC **模型考虑了泛在网络环境中广义时态、接入点、访问设备、网络等要素，具有通用性，现有典型的访问控制模型是** CoAC **模型的子集。通过对** CoAC **模型进行适当约束，可方便地描述已有典型模型，示例化如下。**

5.1 用 CoAC 模型描述 DAC 模型

由定义 1 **和定义** 4，**令** $A=R=G^O=S^O=F$ **，则自主访问控制模型（**DAC**）等价于**$<Q,O,OP>$**，即** $DAC \cong <Q,O,OP>$**。**

$Q=\{q=<u,\cdot,\cdot>\}$**可表示** *DAC* **模型中的主体，**u **表示主体的用户名。**

$O=\{o=<c^O,\cdot,\cdot>\}$**可表示** *DAC* **中的客体，**$c^O$ **表示客体的内容。**

OP **表示操作类型。**

表 2 管理方法使用的函数

函数名	描述	函数名	描述
verifyid	**若用户身份和证书合法则返回** True，**否则返回** False verifyid(*userid*,*certification*:*NAME*;outresult:BOOLEAN) < result=(*userid*∈ *U*) (isvalid(*certification*)) >	verifyng	**若请求的网络** *reqng* **满足网络** verifyng **的要求则返回** True，**否则返回** False verifyng(*reqng*: *NAME*; out result: BOOLEAN) < *reqng*∈ *NGSTATES* result=(∃ng_1, ng_2∈ *validng*·ng_1<*reqng*<ng_2) ∧ (*q*∈ *Q*; *d*∈ *DSTATES*; *t*∈ *TSTATES*; *l*∈ *LSTATES*; *ng*∈ *NGSTATES*; *p*∈ *PERMISSIONS*(*q*, *sc*= (*q*, *t*, *l*, *d*, *reqng*))∈ *QSC* ∧ (*sc*=(*q*, *t*, *l*, *d*, *reqng*), *p*) ∈ *SCP*) >
isnable	**若场景** *scene* **可用则返回** True，**否则返回** False isnable(*scene*:*NAME*;out result:BOOLEAN) < *scene*∈ *SCENE* result=*scene*∈ *ENABLE** >	n.activescbyu	**返回用户** *user* **激活场景数量** n.activescbyu(*user*:*NAME*;out result:*N*) < *user*∈ *USERS* result=$N_{activeU\_total}$(*user*) >
verifyt	**若请求的广义时态** *reqt* **满足广义时态状态** verifyt **的要求则返回** True，**否则返回** False verifyt(*reqt*:*NAME*;out result:BOOLEAN) < *reqt*∈ *TSTATES* result=(∃t_1,t_2∈ *validt*·t_1<*reqt*<t_2) ∧ (*q*∈ *Q*; *t*∈ *TSTATES*; *l*∈ *LSTATES*; *d*∈ *DSTATES*; *ng*∈ *NGSTATES*; *p* ∈ *PERMISSIONS*(*q*, *sc*=(*reqt*, *l*, *d*, *ng*)) ∈ *QSC* ∧ (*sc*=(*q*, *reqt*, *l*, *d*, *ng*), *p*) ∈ *SCP*) >	maxn.activescbyu	**返回用户** *user* **最多能激活场景数量** maxn.activescbyu(*user*:*NAME*;out result:*N*) < *user*∈ *USERS* result=N_{maxU_total}(*user*) >
verifyl	**若请求的接入点** *reql* **满足接入点** verifyl **的要求则返回** True，**否则返回** False verifyl(*reql*:*NAME*;out result:BOOLEAN) < *reql*∈ *LSTATES* result=(∃l_1, *l*∈ *validl*·l_1<*reql*<l_2) ∧ (*q*∈ *Q*;*t*∈ *TSTATES*; *l*∈ *LSTATES*; *d*∈ *DSTATES*; *ng*∈ *NGSTATES*; *p*∈ *PERMISSIONS*(*q*, *sc*=(*q*, *t*, *reql*, *d*, *ng*)) ∈ *QSC* ∧ (*sc*=(*q*, *t*, *reql*, *d*, *ng*), *p*)∈ *SCP*) >	n.activescbyp	**返回激活权限** *permission* **的场景数量** n.activescbyp(*user*:*NAME*;out result:*N*) < *user*∈ *USERS* result=N_{maxP_total}(*user*) >
verifyd	**若请求的访问设备** *reqd* **满足访问设备** verifyd **的要求则返回** True，**否则返回** False verifyd(*reqd*:*NAME*;out result:BOOLEAN) < *reqd*∈ *DSTATES* result=(∃d_1,d_2∈ *validd*·d_1<*reqd*<d_2) ∧ (*q*∈ *Q*; *d*∈ *DSTATES*; *t*∈ *TSTATES*; *l*∈ *LSTATES*; *ng*∈ *NGSTATES*; *p*∈ *PERMISSIONS*(*q*,*sc*=(*q*,*t*,*l*,*reqd*,*ng*)) ∈ *QSC* ∧ (*sc*=(*q*, *t*, *l*, *reqd*, *ng*), *p*)∈ *SCP*) >	maxn.activescbyp	**返回最多能激活权限** *permission* **的场景数量** *P*_total maxn.activescbyp(*user*:*NAME*;out result:*N*) < *permission*∈ *PERMISSIONS* result=N_{maxP_total}(*user*) >

5.2　用 CoAC 模型描述 MAC 模型

由定义 1 和定义 4，令 $A=S^O=F$ ，则强制访问控制模型（MAC）等价于$<Q, O, OP>$，即 $MAC \cong <Q, O, OP>$。

$Q=\{q=<u,\cdot,r>\}$表示 MAC 中的主体，其中，u 和 r 分别表示主体的用户名和角色。

$O=\{o=<c^O,\cdot, s^O>\}$表示 MAC 中的客体，c^O 和 s^O 分别表示客体的内容和安全等级。

OP 表示操作类型。

5.3　用 CoAC 模型描述 TRBAC/RBAC 模型

由定义 1、定义 2 和定义 4，令 $G^O=S^O=F$ ，则面向时态的基于角色的访问控制模型（TRBAC）等价于$<Q,O,T,OP>$，即 $TRBAC \cong <Q,O,T,OP>$。

$Q=\{q=<u,\cdot,r>\} \cup \{q=<\cdot,a,\cdot>\}$表示 $TRBAC$ 中的主体，其中，u、a 和 r 分别表示主体的用户名、访问代理和角色。

$T=\{t=<interval,period,duration>\}$ 表示 $TRBAC$ 的时态。

$O=\{o=<c^O,\cdot,\cdot>\}$表示 TRBAC 的资源，$c^O$ 表示资源的内容。

OP 表示操作类型。

如上所述，在 $TRBAC$ 中，令 $T=F$ 则基于角色的访问控制模型（RBAC）等价于$<Q, O, OP>$，即 $RBAC \cong <Q, O, OP>$。

5.4　用 CoAC 模型描述 ABAC 模型

由定义 1~定义 6，令 $L^{\mathrm{NETID}}=S^D=G^O=S^O=F$ ，则基于行为的访问控制模型（ABAC）等价于$<Q, O, A, OP>$，即

$$ABAC \cong <Q, O, A, OP>$$

其中，$Q=\{q=<u, a, r>\}$表示 $ABAC$ 中的主体，u、a 和 r 分别表示主体的用户名、访问代理和角色。

R 表示 Q 中的角色的集合。

$L=\{l=<l^{\mathrm{SPID}}, l^{\mathrm{NETID}}>\}$表示 $ABAC$ 中的接入点属性信息。

$D=\{d=<g^D, s^D, t>\}$表示 $ABAC$ 中的设备及其相关属性信息。

$NG=<V, E>$表示网络集合，V 和 E 分别表示网络有向属性图的顶点集合和边集。

$T=\{t=<interval, period, duration>\}$表示广义时态。

令 $A=<R, L, D, NG, T>$ 表示 $ABAC$ 中的行为。

$O=\{o=<c^O,\cdot,\cdot>\}$表示 $ABAC$ 的资源，c^O 表示资源的内容。

OP 表示操作类型。

6　结束语

针对新型信息服务模式与传播模式（如数据所有权与管理权分离、信息二次/多次转发模式等）所带来的数据安全和隐私泄露问题，详细分析了访问请求实体、广义时态、接入点、访问设备、网络、资源、网络交互图和资源传播链等要素，提出了一种面向网络空间的访问控制模型，该模型可有效控制用户在何时、何地、使用何种设备、经由何种网络、采用何种操作访问何种资源，有效满足了分布式计算、移动计算、云计算等新型泛在网络服务模式中的细粒度、多层次、灵活多变的信息及数据共享中的访问控制需求。通过调整控制要素，该模型可描述现有经典访问控制模型（如 DAC、MAC、RBAC、ABAC 等）。同时，给出了管理场景的定义和相应管理模型。该模型可实现网络空间中访问对象细粒度、访问模式自适应的信息安全服务与数据资源共享。

参考文献：

[1] National Computer Security Center. Glossary of computer security terms NCSC-TG-004)[EB/OL].http://csrc.nist.gov/secpubs/rainbow/tg004.txt

[2] BELL D E, LAPADULA L J. Secure computer systems: mathematical foundations[R]. MITRE CORP BEDFORD MA, 1973.

[3] STALLINGS W.Network and internetwork security: princip and practice[M]. Englewood Cliffs: Prentice Hall, 1995.

[4] FERRAIOLO D F, KUHN D R. Role-based access control[C]//National Computer Security Conference. c1992:554-563.

[5] OH S, SANDHU R,ZHANG X. An effective role administration model using organization structure[J]. ACM Transactions on Information and System Security (TISSEC), 2006, 9(2): 113-137.

[6] SANDHU R, BHAMIDIPATI V, MUNAWER Q. The ARBAC97 model for role-based administration of roles[J]. ACM Transactions on Information and System Security, 1999, 2(1):105-135

[7] SANDHU R, MUNAWER Q, The ARBAC99 model for administration of roles[C]//Annual Computer Security Applications Conference. c1999: 229-238.

[8] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control models[J]. Computer, 1996 (2): 38-47.

[9] FREUDENTHAL E, PESIN T, PORT L, et al. dRBAC: distributed role-based access control for dynamic coalition environments[C]//International Conference on Distributed Computing System, c2002: 411-420.

[10] LIU S, HUANG H. Role-based access control for distributed cooperation environment[C]//International Conference onComputational Intelligence and Security. c2009:455-459.

[11] PARK J, SANDHU R. The UCON ABC usage control model[J]. ACM Transactions on Information and System Security (TISSEC), 2004,

7(1):128-174.

[12] KATT B, ZhANG X W, BREU R, et al. A general obligation model and continuity: enhanced policy enforcement engine for usage control[C]//ACM Symposium on Access Control Models and Technologies, Estes Park, CO, USA, c2008:683-695.

[13] LOVAT E，PRETSCHNER. Data-centric multi-layer usage control enforcement: a social network example[C]//ACM Symposium on Access Control Models and Technologies. Innsbruck, Austria, c2011: 151-152

[14] XU C, WANG Q, ZHANG W, et al. Temporal access control based on multiple subjects[C]//International Conference on Multimedia Information Networking and Security. c2009:438–441.

[15] BERTINO E, BONATTI P A, FERRARI E. TRBAC: a temporal role-based access control model[J]. ACM Transactions on Information and System Security (TISSEC), 2001, 4(3):191-233.

[16] **王小明, 赵宗涛. 基于角色的时态对象存取控制模型**[J]. **电子学报**, 2005, 33(9): 1634-1638.
WANG X M, ZHAO Z T. Role-based access control model of temporal object[J].Acta Electronica Sinica,2005,33(9):1634-1638.

[17] XU C, WANG Q, ZHANG W, et al. Temporal access control based on multiple subjects[C]//International Conference on Multimedia Information Networking and Security. c2009:438-441.

[18] YUAN E, TONG J. Attributed based access control (ABAC) for Web services[C]//The IEEE International Conference on Web Services. FL, USA, c2005:561-569.

[19] **李晓峰, 冯登国, 陈朝武, 等. 基于属性的访问控制模型**[J]. **通信学报**, 2008, 29(4): 90-98.
LI X F,FENG D G,CHEN Z W, et al. Model for attribute based access control[J].Journal on Communications,2008,29(4):90-98.

[20] **王小明, 付红, 张立臣. 基于属性的访问控制研究进展**[J]. **电子学报**, 2010, 38(7): 1660-1667.
WANG X M, FU H, ZHANG L C, et al. Research progress on attribute-based access control[J]. Acta Electronica Sinica, 2010, 38(7): 1660-1667.

[21] PIRRETTI M, TRAVNOR P, MCDANIEL P, et al. Secure attribute-based systems[J]. Journal of Computer Security. 2010, 18(5): 799-837.

[22] **李凤华, 王巍, 马建峰, 等. 基于行为的访问控制模型及其行为管理**[J]. **电子学报**, 2008,36(10): 1881-1890.
LI F H, WANG W, MA J F, et al. Action-based access control model and administration of actions[J].Acta Electronica Sinica,2008, 36(10): 1881-1890.

[23] RIVEST R, SHAMIR A, WAGNER D A. Time-lock puzzles and timed-release crypto[R]. MIT LCS Tech. Report MIT/LCS/TR-684, 1996.

[24] CATHALO J, LIBERT B, QUISQUATER J J. Efficient and non-interactive timed-release encryption[M]. Information and Communications Security, 2005: 291-303.

[25] PATERSON K G, QUAGLIA E A. Time-specific encryption[M]// Security and Cryptography for Networks, 2010: 1-16.

[26] ZHOU L, VARADHARAJAN V, HITCHENS M. Enforcing role-based access control for secure data storage in the cloud[J]. The Computer Journal, 2011, 54(10): 1675-1687.

[27] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[C]//CRYPTO. California, USA, c2001: 213-229.

[28] ROUSELAKIS Y, WATERS B. Practical constructions and new proof methods for large universe attribute-based encryption[C]//ACM Conference on Computer and Communications Security. Berlin, Germany, c2013: 463-474.

[29] LEWKO A, WATERS B. Unbounded HIBE and attribute-based encryption[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Tallinn, Estonia, c2011: 547-567.

[30] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//ACM Conference on Computer and Communications Security. VA, USA, c2006: 89-98.

[31] BETHENCOURT J, WATERS B. Ciphertext-policy attribute-based encryption[C]//IEEE Symposium on Security and Privacy. California, USA, c2007:321-334.

[32] **洪澄, 张敏, 冯登国**. AB-ACCS **一种云存储密文访问控制方法**[J]. **计算机研究与发展**, 2010, 47(Z1): 259-265.
HONG C, ZHANG M, FENG D G. AB-ACCS: a cryptographic access control scheme for cloud storage[J].Journal of Computer Research and Development,2010,47(Z1):259-265.

[33] CHENG Y, REN J, WANG Z, et al. Re-encryption optimization in CP-ABE based cryptographic cloud storage[C]//International Conference on Cloud and Green Computing. Huanan, China, c2012: 173-179.

[34] CHASE M, CHOW S S M. Improving privacy and security in multi-authority attribute-based encryption[C]//ACM conference on Computer and Communications Security. Illinois, USA, c2009: 121-130.

[35] LIU X, ZHANG Y, WANG B, et al. Mona: secure multi-owner data sharing for dynamic groups in the cloud[J]. IEEE Transaction on Parallel and Distributed Systems, 2013, 24(6): 1182-1191.

作者简介：

李凤华（1966-），男，湖北浠水人，博士，中国科学院信息工程研究所副总工、研究员、博士生导师，主要研究方向为网络与系统安全、信息保护、隐私计算。

王彦超（1980-），男，河北邯郸人，中国科学院信息工程研究所博士生，主要研究方向为访问控制与云数据安全。

殷丽华（1973-），女，辽宁朝阳人，博士，中国科学院信息工程研究所副研究员、硕士生导师，主要研究方向为信息安全、安全性评估。

谢绒娜（1976-），女，山西永济人，北京电子科技学院副教授、硕士生导师，主要研究方向为密码应用、网络与系统安全。

熊金波（1981-），男，湖南益阳人，中国科学院信息工程研究所博士后，福建师范大学副教授、硕士生导师，主要研究方向为云数据安全与隐私保护技术。