复杂网络环境下跨网访问控制机制

李凤华[1,2]，陈天柱[1,2]，王震[3]，张林杰[4]，史国振[5]，郭云川[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. 中国科学院大学网络空间安全学院，北京 100049；3. 杭州电子科技大学网络空间安全学院，浙江 杭州 310018；
4. 中国电子科技集团公司第五十四研究所，河北 石家庄 050081；5. 北京电子科技学院信息安全系，北京 100070）

摘 要：以天地一体化网络、物联网和复杂专用网络为代表的复杂网络环境（CNN, complex network environment）具有设备动态接入，网络异构、众多和信息跨网流动频繁等特点。上述特点给复杂网络环境下的访问控制技术带来细粒度控制、策略跟随和策略语义归一化等一系列新需求。针对这些需求，将面向网络空间的访问控制机制映射到复杂网络环境中。首先展示访问控制机制的具体映射过程，其次提出相应的访问控制管理模型，并用 Z 符号形式化地描述管理模型中的管理函数。实例分析表明，该访问控制机制可满足上述一系列新需求。

关键词：复杂网络环境；跨网；天地一体化网络；访问控制机制；管理模型
中图分类号：TP302
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018019

Cross-network access control mechanism for complex network environment

LI Fenghua[1,2], CHEN Tianzhu[1,2], WANG Zhen[3], ZHANG Linjie[4], SHI Guozhen[5], GUO Yunchuan[1]

1. The State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
3. School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China
4. The 54th Research Institute of China Electronics Technology Group Corporation 54, Shijiazhuang 050081, China
5. Department of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: Complex network environments, such as space-ground integrated networks, internet of things and complex private networks, have some typical characteristics, e.g., integration of multi-network and information flow in cross-network. These characteristics bring access control for complex network environment the new requirement of coarse-grained control, sticky policies and inconsistent operation semantics. To satisfy these requirements, cross-network access control mechanism in complex network environments (CACCN) was designed by mapping the cyberspace-oriented access control. First of all, the process of mapping was illustrated using the example of space-ground integrated networks. Next, a management model was proposed to manage the control elements in CACCN and a series of management functions were designed by using Z-notation. The analysis on practical example demonstrates that the mechanism can satisfy a series of access control requirements.

Key words: complex network environment, cross-network, space-ground integrated network, access control, management model

收稿日期：2017-10-28；**修回日期**：2018-01-09
通信作者：郭云川，guoyunchuan@iie.ac.cn
基金项目：国家重点研发计划基金资助项目（No.2016YFB0801001）；国家自然科学基金资助项目（No.61672515）
Foundation Items: The National Key R&D Program of China（No.2016YFB0801001）, The National Natural Science Foundation of China (No.61672515)

1 引言

近年来，以天地一体化网络[1]、物联网[2]、复杂专用网络为代表的复杂网络环境快速发展。美国卫星工业协会发布的《2016 年卫星产业状况报告》调查表明，从 2006 年到 2015 年全球卫星工业产值平均每年呈现 9%以上的增长率[3]；Gartner 预测物联网设备在 2015 年达到 50 亿台，2020 年将达到 250 亿台。复杂网络环境的快速发展给人们的日常生活带来了巨大便利，同时也产生了大量的安全问题，尤其是数据安全问题。因此，作为保护数据被合法访问的先进技术，研究复杂网络环境下的访问控制技术显得尤为必要。

复杂网络环境具有设备动态接入、网络异构、众多和信息跨网流动频繁等特点。例如，天地一体化网络由天基骨干网、天基接入网、地基节点网、地面互联网和移动通信网等异构网络组成。在该网络中，海量地面用户频繁动态接入，天基接入网获取的地面实时信息经由天基骨干网流向地基节点网。上述特点给复杂网络环境访问控制技术带来诸多新需求。1) 细粒度控制：复杂网络环境具有海量信息，不同用户对这些信息具有不同的使用权限，粗粒度控制会带来大量安全问题。2) 策略跟随：数据信息在网间频繁流动，其相应的控制策略未跟随数据信息本体到新网时会造成用户失去对数据的控制。3) 策略语义归一化：数据信息在流动过程中跨越不同网络，网络间策略语言的不一致性可能会造成策略在网间转化时出现错误。

研究者们基于传统访问控制模型，针对复杂网络环境的某些特点，提出了不同的访问控制机制。针对物联网设备动态接入特点，文献[4~6]基于访问控制列表[7]提出基于 Capability 的访问控制模型。在该模型中，组织或个人可对访问设备进行细粒度管理。针对智能电网跨安全网特点，文献[8]将角色[9]定义范围从局部微电网扩展到局部交互微电网和远程微电网。针对物联网网络异构和信息频繁流动的特点，文献[10]扩展可信[11]的概念，提出了终端到终端的安全交流和访问机制。针对天地一体化网络的动态性特点，文献[12]融合角色安全性和可用性、属性[13]灵活性等优势提出一种分布式的访问控制框架。文献[14]基于角色、上下文[15]和动态的偏好知识，提出一种用户可连续访问的控制模型。然而，上述基于传统访问控制模型提出的方案很难解决复杂网络环境下信息流跨网问题，例如，基于 Capability 的访问控制模型无法对流出该网的数据进行控制，新网中可能不存在与源网中该数据对应的角色，进而失去该数据原本的访问策略。

文献[16]提出了面向网络空间的访问控制机制（CoAC, cyberspace-oriented access control model）。该机制使用设备、接入点、时间、网络以及相关属性因素描述策略，实现了网络空间对细粒度控制、策略跟随和策略语义一致性等访问控制需求。本文将面向网络空间的访问控制机制映射到复杂网络环境上，呈现复杂网络环境下跨网访问控制机制（CACCN, cross-network access control mechanism for complex network environment）。天地一体化网络具有“节点海量、多异构网融合、信息跨网流动频繁”等特点，是一种典型的复杂网络环境。因此，本文以天地一体化网络为例，具体展示映射过程，主要贡献如下。

1) 针对复杂网络环境对细粒度控制、策略跟随和策略语义归一化等需求，通过映射面向网络空间的访问控制机制，提出了面向复杂网络环境下跨网访问控制机制，实现对复杂网络环境信息流跨网控制。实例分析表明，所提出的访问控制机制可解决上述需求。

2) 针对访问控制管理的复杂性，给出了访问控制管理模型，并用 Z 符号[17]形式化地描述了管理模型中的管理函数和管理方法。

2 基于 CoAC 的复杂网络环境下跨网访问控制

本节首先呈现从 CoAC 到 CACCN 的映射过程，然后详细给出 CACCN 的实施机制并分析其满足的安全需求。

2.1 从 CoAC 到 CACCN 的映射

下面，以天地一体化网络为例，具体展示从 CoAC 到 CACCN 的映射过程。该映射是由 8 个映射函数组成，每个映射函数的原像与像的主要区别在于访问控制属性。

访问控制属性是指访问请求实体通过网络对资源访问时所涉及的所有与权限分配相关的特征，分为 2 类：与安全相关的所有属性（*sAttr*）和与安全不相关的通用属性（*gAttr*）。一般地，*sAttr* 和 *gAttr* 可用向量表示，向量中的分量表示一种属性。例如，加密方式是 *sAttr* 的分量，传输带宽是 *gAttr* 的分量。

映射 1　访问请求实体映射。在天地一体化网络中，访问请求实体 *q* 包括 2 类：用户 *u* 和访问代理 *a*，记为 *q*=<*u*, *a*>，其中，用户 *u* 包括 3 类，空基用户、海基用户和陆基用户；*a* 表示部署在地面关口站、卫星和终端中的访问代理，可以是一个装置或进程；*Q* 表示所有的请求实体集。

映射 2　接入点映射。类似于 CoAC，接入点（AP, access point）是指资源访问请求实体首次接入天地一体化网络时路由网络首跳点所在的空间位置（space location）或网络标识（network identity）。

天地一体化网络接入点的通用属性 *gAttr* 包括接入速率（*aRate*）、接入类型（*aType*）、接入策略（*aPoli*）、接入协议（*aProt*）、通信频段（*aPect*）、支持的用户数量（*aUNum*）、接入总带宽（*aWidth*）等；安全属性与 CoAC 中接入点的安全属性相同，包括加密类型（*aEnc*）、安全传输协议（*aProt*）等。接入点的通用属性（*gAttr*）和安全属性（*sAttr*）可分别表示为

AP.gAttr=<*aRate*, *aType*, *aPoli*, *aProt*, *aPect*, *aUNum*, *aWidth*, …>

AP.sAttr=<*aEnc*, *aProt*, …>

其中，*aType* 包括光接入、微波接入和有线接入等；*aPoli* 包括控制信道接入和业务信道接入；接入协议集合 *aProt* 包括 FDMA、TDMA、CDMA 和 OFDMA 等；接入频段集合 *aPect* 包括 L 频段和 S 频段等。

映射 3　资源映射。资源是指天地一体化网络中访问请求实体访问的对象，如密码资源、侦查监视卫星和对地监测卫星所获得的数据等。资源（*res*）可用二元组<*rid*, *rcnt*>表示，其中，*rid* 表示 *res* 的唯一标识，*rcnt* 表示 *res* 的内容。

资源的通用属性包括资源拥有者（*rOwner*）、资源类型（*rType*）、资源访问策略（*rAccessPoli*）、资源大小（*rSize*）、资源是否在国土可见范围（*rVisi*）、存储地点（*Loc*）。资源的安全属性包括安全等级（*rSecLev*）、被允许操作（*rAllowedOper*）、加密方式（*rEncType*）等。*res* 的通用属性（*gAttr*）和安全属性（*sAttr*）可分别表示为

RES.gAttr=<*rOwner*, *rType*, *rAccessPoli*, *rSize*, *rVisi*, *rLoc*, …>

RES.sAttr=<*rSecLev*, *rAllowedOper*, *rEncType*,…>

其中，*rType* 包括管理类数据（*rManData*）和应用类数据（*rAppData*）。*rManData* 包括测控数据、位置数据、状态数据、申请数据、广播数据和网管数据等。按照流动方向，*rAppData* 可划分为前向数据和返向数据；按照内容，*rAppData* 可划分为文本、图片、语音和视频等。

映射 4　访问设备映射。访问设备（*dev*）是指天地一体化网络中访问请求实体访问资源时所使用的设备，主要包括高速航天器终端、天基骨干网地面终端、Ka 大容量宽带便携/固定终端、高轨卫星移动军用手持/民用车载终端、低轨星座手持/车载终端、Ku（FDMA）便携/固定终端、Ku（TDMA）便携/固定终端等。

设备 *dev* 的通用属性（*gAttr*）包括设备空间位置（*dLoc*）、设备移动速度（*dVel*）、设备移动方向（*dDir*）、通信频段（*dSpectrum*）、通信带宽（*dWidth*）、接入优先级（*aPrio*）等；设备安全属性包括加密机制（*dEncType*）、安全等级（*dSecLevel*）等。资源（*dev*）的通用属性（*gAttr*）和安全属性（*sAttr*）可分别表示为

DEV.gAttr=<*dLoc*, *dVel*, *dDir*, *dSpectrum*, *dWidth*, *aPrio*,…>

DEV.sAttr=<*dEncType*, *dSecLevel*, …>,

设备 *dev* 可用三元组<*di*, *dev.gAttr*, *dev. sAttr*>表示，其中，*di* 表示设备 ID。

映射 5　网络—天基骨干网络映射。天基骨干网络（SBN, space backbone network）是位于地球同步轨道的若干天基骨干节点（SBNO, space backbone node）通过激光通信或微波通信连接而成的网络，天基骨干节点是数据中继、路由交换、信息存储、处理融合的载体。天基骨干网络可表示为无向连通图 $G_{\mathrm{SBN}}=(V_{\mathrm{SBN}}, E_{\mathrm{SBN}})$，其中，$V_{\mathrm{SBN}}=\{sbno_1, \cdots, sbno_M\}$ 为图的顶点集，表示天基骨干节点集，$sbno_i$ 表示第 i 个天基骨干节点，$1\leqslant i\leqslant M$，$M\geqslant 3$；$E_{\mathrm{SBN}}=\{<sbno_i, sbno_{i+1}>|1\leqslant i\leqslant M, sbno_{M+1}=sbno_1\}$ 为边集，表示天基骨干节点间的传输链路。G_{SBN} 中任何顶点只与前后 2 个顶点相连，其含义是同步轨道上的天基骨干节点只与前后骨干节点通信。为了简洁，用 *esbn* 表示天基骨干网络的边。

天基骨干节点通用属性包括控制者（*sbnController*）、关口站是否可见（*sbnVisi*）、传输协议（*sbnProt*）、计算能力（*sbnCompAbility*）、存储能力（*sbnStoreCapa*）、功能（*sbnFunc*）、空闲信道数量（*sbnFreeChanNum*）等。天基骨干节点安全属性包括加密方式（*sbnEnc*）、所支持的安全传输协议（*sbnSecProt*）等。其中，*sbnController*

表示骨干节点由谁控制，包括受低轨卫星控制或受地面控制，*sbnProt* 包括卫星传输协议（STP, satellite transport protocol）等，*sbnFunc* 包括数据中继、路由交换、信息存储、处理融合等。顶点的通用属性（*gAttr*）和安全属性（*sAttr*）分别表示为

SBN.gAttr=<*sbnController*, *sbnVisi*, *sbnProt*, *sbnCompAbility*, *sbnStoreCapa*, *sbnFunc*, *sbnFree-ChanNum*, …>

SBN.sAttr=<*sbnEnc*, *sbnSecProt*, …>

天基骨干网络边 *esbn* 的通用属性（*gAttr*）包括通道类型（*eType*）、通信带宽（*eWidth*）、服务质量（*eQos*）、物理链路层协议（*ePhyProt*）、路由协议（*eRoutProt*）、网络层协议（*eNetProt*）、传输层协议（*eTranProt*）和通信频段（*eFreq*）等；天基骨干网传输的安全属性包括安全等级（*eSecLevel*）、加密类型（*eEncType*）、所支持的安全传输协议（*eSecProt*）等。边的通用属性（*gAttr*）和安全属性（*sAttr*）分别表示为

EBSN.gAttr=<*eType*, *eWidth*, *eQos*, *ePhyProt*, *eRoutProt*, *eNetProt*, *eTranProt*, *eFreq*, …>

EBSN.sAttr={<*eSecLevel*, *eEncType*, *eSecProt*,…> 其中，*eType* 包括 2 类：通信信道（*CommChan*）和控制信道（*ControlChan*），*ePhyProt* 包括 Laor 和 Dra 等，*eNetProt* 包括 IP 和 DTN 等，*eRoutProt* 包括 HQRP（hierarchical QoS routing protocol）和 LAOR（location-assisted on demand）协议等，*eTransprot* 包括 TCP 和 UDP 等，*eFreq* 包括 L 频段和 S 频段等。

映射 6 网络—天基接入网络映射。天基接入网络（SAN, space access network）由部署在低轨的若干接入节点通过激光通信或微波通信连接而成的网络。天基接入网络用无向图 $G_{\mathrm{SAN}}=(V_{\mathrm{SAN}}, E_{\mathrm{SAN}})$，其中，$V_{\mathrm{SAN}}=\{san_1^1,\cdots, san_1^{Q_1}, san_1^2,\cdots, san_2^{Q_2},\cdots, san_N^1,\cdots, san_N^{Q_N}\}$ 为顶点集，表示天基接入网络的接入节点集，Q_i 表示第 i 个低轨轨道卫星数量，N 表示低轨数量。E_{SAN} 为边集，表示天基接入网络间的传输链路。天基接入网络的节点处在低轨轨道上，这使天基接入网络的拓扑结构时刻在变化，这种变化造成了节点连接极为复杂，此处对节点间的连接方式不再介绍。天基接入网络顶点和边的属性类型与天基骨干网络定点和边的属性类型相同，但属性值存在差别，这里不再赘述属性类型。

映射 7 网络—地基节点网络映射。地基节点网络（GNN, ground node network）是由多个地面互连的地基骨干节点（GBN, ground backbone node）、Ku 宽带卫星关口站（KUG, Ku bandwidth satellite gateway）、Ka 大容量宽带卫星关口站（KAG, Ka satellite gateway）和 S 卫星关口站（SS, S satellite gateway）通过地面高速骨干网络等方式连接而成的网络，地基骨干节点包括关口站和信息港，主要完成网络控制、资源管理、协议转换、信息处理、融合共享等功能，并实现与其他地面系统的互联互通。

地基节点网络可用无向图 $G_{\mathrm{GNN}}=(V_{\mathrm{GNN}}, E_{\mathrm{GNN}})$ 表示，其中，$V_{\mathrm{GNN}}=V_{\mathrm{GBN}}\cup V_{\mathrm{KUG}}\cup V_{\mathrm{KAG}}\cup V_{\mathrm{SS}}$ 为图的顶点集，V_{GBN}、V_{KUG}、V_{KAG}、V_{SS} 分别表示地基骨干节点、Ku 宽带卫星关口站、Ka 大容量宽带卫星关口站、S 卫星关口站的对应节点。E_{GNN} 为 V_{GNN} 所构成完全图的边集，即 $E_{\mathrm{GNN}}=\{<V_{\mathrm{GBN}}, V_{\mathrm{KUG}}>, <V_{\mathrm{GBN}}, V_{\mathrm{KAG}}>, <V_{\mathrm{GBN}}, V_{\mathrm{SS}}>, <V_{\mathrm{KUG}}, V_{\mathrm{KAG}}>, <V_{\mathrm{KUG}}, V_{\mathrm{SS}}>, <V_{\mathrm{KAG}}, V_{\mathrm{SS}}>\}$，其中，$<V_{\mathrm{GBN}}, V_{\mathrm{KUG}}>\subseteq\{<gbn, kug>|gbn\in V_{\mathrm{GBN}}, kug\in V_{\mathrm{KUG}}\}$ 表示地基骨干节点和 Ku 宽带卫星关口站相连，由此类推，可得 $<V_{\mathrm{GBN}}, V_{\mathrm{KAG}}>$ 等的含义。

地基节点网络顶点和边的属性类型与天基骨干网络相同，但属性值存在差别，这里不再赘述属性类型。

映射 8 网络映射。天地一体化网络（SGIN, space-ground integrated network）是信息传播的载体，是所有信息传播通道的集合。宏观上，整个天地一体化网络可用无向图 $G_{\mathrm{SGIN}}=(V_{\mathrm{SGIN}}, E_{\mathrm{SGIN}})$ 表示，该网络的顶点包括天基骨干子网 V_{SBN}、天基接入子网 V_{SAN} 和地基节点子网 V_{GNN}，边是由 E_{SBN}、E_{SAN} 和 E_{GNN} 组成，即

$$V_{\mathrm{SGIN}}=V_{\mathrm{SBN}}\cup V_{\mathrm{SAN}}\cup V_{\mathrm{GNN}}$$

$E_{\mathrm{SGIN}}=E_{\mathrm{SBN}}\cup E_{\mathrm{SAN}}\cup E_{\mathrm{GNN}}\cup\{<sbno_i, san_{jk}>|1\leqslant i\leqslant M, 1\leqslant j\leqslant Q_k, 1\leqslant k\leqslant N$, 天基骨干节点 $sbno_i$ 和天基接入节点 san_k^i 可连$\}\cup\{<sbno_i, gnn>|gnn\in V_{\mathrm{GNN}}$,天基骨干节点 $sbno_i$ 与地基节点 gnn 可见$\}\cup\{<san_k^i, gnn>|gnn\in V_{\mathrm{GNN}}, 1\leqslant j\leqslant Q_k, 1\leqslant k\leqslant N, san_k^i$ 关口站和 gnn 相连$\}$

天地一体化网络中顶点属性为图 G_{SBN}、图 G_{SAN} 和图 G_{GNN} 中所有顶点属性的并集，边属性为图 G_{SBN}、图 G_{SAN} 和图 G_{GNN} 中所有边属性的并集。

2.2 CACCN 实施机制

访问控制的一个核心问题是如何高效地分配

和撤销访问权限，为了解决此问题，本文借鉴 CoAC 中的权限管理方式，通过场景来分配和撤销权限。场景由广义时态、接入点、设备、网络构成，在权限分配时，预先设定何种场景对何种客体能执行何种操作（即进行“场景—权限”分配）；当用户对客体执行某种操作时，权限决策点首先判定用户所在场景（即“用户—场景”判定），基于“用户—场景”和“场景—权限”，权限决策点判定用户是否具有对客体执行该操作的权限。关于基于场景的访问控制的形式定义，请参考文献[2]。图 1 详细给出了复杂网络环境下跨网访问控制机制。为了准确实施 CACCN，本文定义 CACCN 相关核心实施函数如下。

1) *AttrSelect*:(*DEV.gAttr*, *CNN.gAttr*, *RES.gAttr*, *DEV.sAttr*, *CNN.sAttr*, *RES.sAttr*)→*gAttr*∪*sAttr* 为属性选择函数，用来确定哪些属性可用作权限分配的依据。设备、资源和复杂网络环境均拥有大量的安全属性或通用属性，设计此函数是为了提高策略决策时的效率，需要依据控制需求选择其中部分安全属性或通用属性作为决策依据。

2) *AttrCheck*:(*DEV.gAttr*, *CNN.gAttr*, *RES.gAttr*, *DEV.sAttr*, *CNN.sAttr*, *RES.sAttr*, *Attr_value*)→{true, false}为属性检查函数，其中，*Attr_value* 表示所有属性值的集合。

3) *q-sceneCheck*(*Q*)→ *SCENE* 为访问请求实体—场景检查函数，用于检查访问请求实体所在的场景。

4) *scene-permissionAssign*(*SCENE*, *PERM*) → {true, false}为场景—权限分配函数，用于分配给定场景所用于的权限，其中，*SCENE* 和 *PERM* 分别表示所有场景的集合和所有权限的集合。返回结果为 true 表示分配成功，否则，分配失败。

5) *scene-permissionRevoke*(*SCENE*, *PERM*) → {true, false}为场景—权限吊销函数，用于吊销分配给定场景的指定权限。

2.3　CACCN 分析

下面分析 CACCN 如何满足引言部分所提出的访问控制需求以及其他需求。

1) 支持细粒度控制。资源以及场景中的接入点、网络等都包含大量细粒度的安全属性和通用属性，并且可依据需求扩展这些属性。

在实际应用中可预先定义或实时获取这些属性的动态变化值，因此，所提访问控制机制是细粒度的，可对访问过程作精准控制。

2) 支持策略跟随。由于资源通用属性作为控制因素包含在访问策略中，同时资源在流动过程中该属性始终伴随资源，因而该机制支持策略跟随。

3) 支持策略语义归一化处理。该机制定义大量共有属性，采用该机制的不同机构或组织均能理解这些属性。采用这些共有属性控制信息流动时可实现策略语义归一化处理。

本文所提访问控制机制除了支持这 3 种核心需求外，还能有效确保机密性和支持策略自定义。机密性方面，在设备、资源和网络的通用属性、安全属性中定义安全等级和加密算法，该安全等级包含

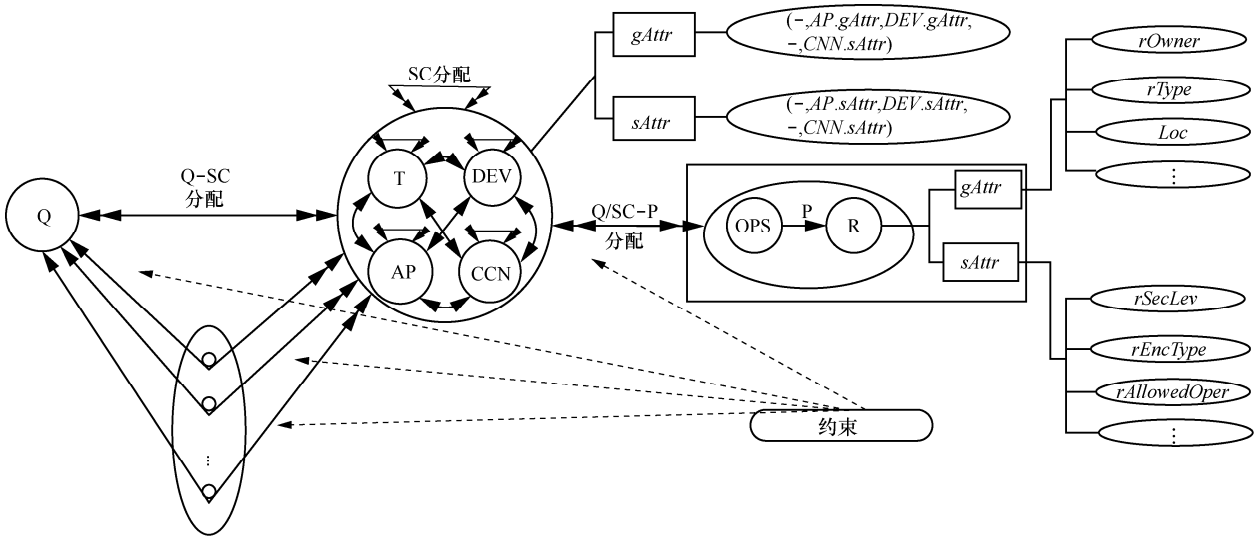


图 1　复杂网络环境下跨网访问控制机制

了设备、资源和传输通道的密级，通过实施策略可确保涉密信息只能在低于其密级的传输信道中传输，并且只能被具有相应角色的用户所接收，从而保障机密性。策略自定义方面，资源的通用属性中包含了资源拥有者的资源访问策略，因此，除了采用场景进行中心化访问控制授权之外，每个组织或机构可依据自身情况自定义对该资源的访问控制策略。

3 复杂网络环境下跨网访问控制管理

在复杂网络环境中设备动态接入，异构网络彼此连接，海量信息频繁跨网流动，这使复杂网络环境下跨网访问控制机制异常复杂，因此，需要设计一套相应的管理模型[18]和管理函数，确保复杂网络环境下跨网访问控制系统能高效安全运行。为确保管理函数语义准确，本文使用 Z 符号[17]描述管理函数。

3.1 复杂网络环境管理模型

在复杂网络环境中，管理员通过网络服务系统和运维管理系统在给定的时间段内利用特定的设备、特定网络对访问请求实体分配、撤销和更新特定资源的访问权限。由此可知，管理者通过特定的场景实现对访问控制的管理，简称为管理场景。

定义 1 管理场景(ADSC, administration scene)。定义为四元组（*admiT*, *admiAP*, *admiDEV*, *admiCNN*)，表示管理者在*admiT*时间利用*admiDEV*设备在*admiAP*这个访问点通过*admiCNN*网络对管理对象进行管理。

复杂网络环境管理者通过管理场景对访问过程进行管理，其管理流程如下。超级管理员为管理者分配、撤销管理场景，并维护管理场景对应的权限。管理者通过管理场景更新、删除和修改场景，选取设备、网络、资源的通用属性和安全属性。另外，管理者需要日常维护场景、会话对应的权限，检测场景的权限是否存在冲突。访问请求实体以某一时间点、接入点、设备、网络申请对资源的某一访问权限时，管理模型认证其身份，认证通过后为其分配会话，并激活会话对应的场景进而激活该权限对应的场景。管理模型检测访问请求实体的访问场景是否满足该权限对应的场景，如果满足则具有权限，反之不具有权限。图 2 详细给出了复杂网络环境下跨网访问控制管理模型。

根据管理流程，管理对象包括：1) 访问请求实

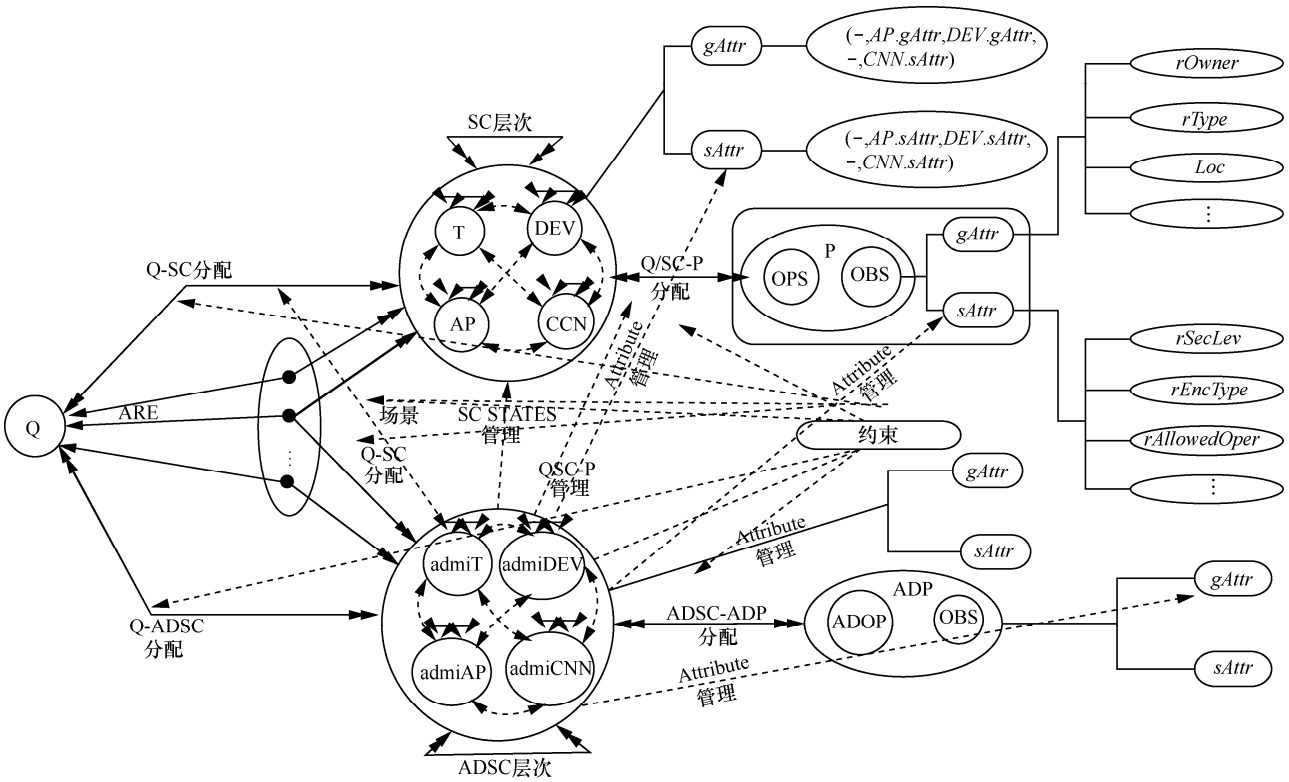


图 2 复杂网络环境下跨网访问控制管理模型

体身份、场景中的相关元素及属性、资源及属性和权限；2) 访问请求实体的场景分配、给当前访问请求实体分配会话、给当前会话分配场景、场景与权限的映射。

基于管理场景，可定义管理模型。由于本文所提模式是文献[2]的实例化，根据文献[2]和图 2 所示的管理模型，很容易定义管理模型组件，本文不再给出管理模型组件的定义。

在复杂网络环境中，不同管理者存在不同的管理权限，如超级管理员能够撤销所有管理员的权限。下面定义 4 个与场景相关的分配与撤销函数。

1) $can_assignUS{:}ADSC\times CAN\text{-}SC\times 2^{ADSC}\rightarrow\{\text{true, false}\}$为用户—场景分配函数，其中，*CAN-SC* 表示能够获得管理场景的先决条件。函数 can_assignUS (x, y, Z)为真时分配 Z 中的管理场景。注意：场景最低的管理员不能为其他管理员分配任何场景。

2) $can_revokeUS{:}ADSC\times 2^{ADSC\setminus\{superADSC\}}\rightarrow\{\text{true, false}\}$为用户—场景撤销函数，$can_revokeUS(x, Z)$表示具有管理场景 x 的管理者能够撤销分配某个用户的 Z 中的管理场景。注意：超级管理场景是分配其他管理场景的最初入口，是不能撤销的；另外，场景最低的管理员不能撤销其他管理员分配任何场景。

3) $can_assignSP{:}ADSC\times CANP\times 2^{ADP}\rightarrow\{\text{true, false}\}$为场景—权限分配函数，其中，*CANP* 表示能够获得管理权限的先决条件，*ADP* 表示所有管理权限的集合。函数 $can_assignSP(x, y, Z)$为真表示具有管理场景 x 的管理者能对满足条件 y 的场景分配 Z 中的管理权限。

4) $can_revokeSP{:}ADSC\times 2^{ADP}\rightarrow\{\text{true, false}\}$为场景—权限撤销函数，$can_revokeSP(x, Z)$表示具有管理场景 x 的管理者能够撤销分配某个场景的管理权限。

3.2　复杂网络环境管理函数

为了能够准确地管理访问控制过程，需要定义管理函数。本文将管理函数划分为 6 种：请求实体—场景管理、场景—权限管理、场景管理、会话管理、属性管理、认证管理。由复杂网络环境管理模型定义的 4 个管理函数以及与活动数量相关的管理函数（包括用户当前活动场景数量函数 *activescbyu.n*、用户活动场景数量上限函数 *maxactivescbyu.n*、拥有当前权限的场景数量函数 *activescbyp.n* 和给定权限所允许的活动场景数量上限函数 *maxactivescbyp.n*）[2]。下面详细给出相应的管理函数。

在请求实体—场景管理中，相应的管理函数为 *ass_QADSC*、*rev_QADSC*，如表 1 所示，其功能分别是为管理者分配管理场景、撤销管理者具有的管理场景。

表 1　　请求实体—场景管理类

函数名	描述
ass_QADSC	为管理者分配管理场景，若分配成功，返回 true，否则，返回 false *ass_QADSC*(*ADSC*?,*q*?:*NAME*, *result*!:*BOOLEAN*)◁ if (*q*?, *ADSC*?)∉*QADSC* then *QADSC*'=*QADSC*∪ {(*q*, *ADSC*)}, *result*=true else *result*=false▷
rev_QADSC	撤销管理者具有的管理场景 *rev_QADSC*(*ADSC*?, *q*?: *NAME*, *result*!:*BOOLEAN*)◁ if (*q*?, *ADSC*?)∈*QADSC* then *QADSC*'=*QADSC*\{(*q*, *ADSC*)} else *result*=false▷

在场景—权限管理中，管理函数为 *ass_ADSCP*、*rev_ADSCP*、*mod_ADSCP*、*perInherit*，如表 2 所示，其功能分别是为管理场景分配权限、撤销管理场景的权限、修改管理场景的权限、保证高场景继承低场景的权限。

表 2　　场景—权限管理类

函数名	描述
ass_ADSCP	为管理者分配管理者所在场景的权限，若分配成功，返回 true，否则，返回 false *ass_ADSCP*(*ADSC*?, *p*?: *NAME*; *result*!:*BOOLEAN*)◁ if (*ADSC*, *p*)∉*ADSCP* then *ADSCP*'=*ADSCP*∪ {(*ADSC*, *p*)}, *result*=true else *result*=false▷
rev_ADSCP	撤销管理者所在场景的权限，若撤销成功，返回 true，否则返回 false *rev_ADSCP*(*ADSC*?, *p*?:*NAME*; *result*!:*BOOLEAN*)◁ if (*ADSC*, *p*) ∈ *ADSCP* and *ADSCassignTo*((*ADSC*, *p*))≤*currentADSC*[1] then *ADSCP*'=*ADSCP*\{(*ADSC*, *p*)}, *result*=true else *result*=false▷
mod_ADSCP	修改管理者所在场景的权限，若修改成功，返回 true，否则，返回 false *mod_ADSCP*(*ADSC*?,*pb*?,*pa*?: *NAME*; *result*!: *BOOLEAN*)◁ if (*ADSC*, *pb*) ∈ *ADSCP* and *ADSCassignTo*((*ADSC*, *pb*))≤*currentADSC* then *ADSCP*'={(*ADSC*,*pa*)}∪*SCP*\{(*ADSC*,*pb*)}, *result*= true else *result*=false▷
perInherit	权限继承：高场景自动继承低场景的权限 *perInherit*(*scene*?:*NAME*)◁ ∀*sc*∈*scene*, if *sc*≤*scene*, *sc.p*⊆*scene.p*▷

注：函数 *ADSCassignTo*((*ADSC*,*p*))表示将权限 *p* 赋予管理场景 *ADSC* 的管理员所在的场景，*currentADSC*()表示执行当前操作的管理者所在的场景。

在场景管理中，管理函数为 *modT*、*modAp*、*modDev*、*modCnn*、*det_Conflict*、*che_Scene*，如表 3 所示，*modT*、*modAp*、*modDev*、*modCnn* 的功能分别是修改场景时间、接入点、设备、网络因素，*det_Conflict* 的功能是检测是否存在与该场景冲突的场景，*che_Scene* 功能是检查场景。

在会话管理中，管理函数为 *ass_QSe*、*ass_SeSc*，如表 4 所示，其功能分别是为访问请求实体分配会

表 3　　场景管理类

函数名	描述
modT	修改场景的时间因素 *modT*(*sc*?, *oldtime*?, *newtime*?: *NAME*)⊲ if *sc.oldtime*∈*TSTATES* and *sc.newtime*∉*TSTATES* then *TSTATES*'= *TSTATES*∪{*newtime*} *scene*'=(*newtime*, *ap*, *dev*, *cnn*) *SSC*'=*SSC*\{<*s*, *scene*>|*s*∈*session* (*sc*)}∪{<*s*, *scene*'>|*s*∈*session* (*sc*)} *QSC*'=*QSC*\{<*q*, *scene*>|*q*∈*entity*(*sc*)}∪{<*q*, *scene*' >|*q*∈*entity*(*sc*)} *SCP*'=*SCP*\{<*scene*, *p*>|*p*∈*permission*(*sc*)}∪{ <*scene*', *p*>|*p*∈*permission*(*sc*)} *SCENES*'=*SCENES*\{*scene*}∪{*scene*'}⊳
modAp	修改场景的接入点因素 *modAp*(*sc*?, *oldap*?, *newap*?: *NAME*)⊲ if *sc.oldap*∈*APSTATES* and *sc.newap*∉*APSTATES* then *APSTATES*'= *APSTATES*∪{*newap*} *scene*'=(*time*, *newap*, *dev*, *cnn*) *SSC*'=*SSC*\{<*s*, *scene*>|*s*∈*session* (*sc*) }∪{<*s*, *scene*'>| *s*∈*session* (*sc*)} *QSC*'=*QSC*\{<*q*, *scene*>|*q*∈*entity*(*sc*)}∪{<*q*, *scene*'>|*q*∈*entity*(*sc*)} *SCP*'=*SCP*\{<*scene*, *p*>|*p*∈*permission*(*sc*)}∪{ <*scene*', *p*>|*p*∈*permission*(*sc*)} *SCENES*'=*SCENES*\{*scene*}∪{*scene*'}⊳
modDev	修改场景的设备因素 *modDev*(*dev*?, *olddev*, *newdev*?: *NAME*)⊲ if *sc.olddev*∈*DEVSTATES* and *sc.newdev*∉ *DEVSTATES* then *DEVSTATES*'= *DEVSTATES*∪{*newdev*} *scene*'=(*time*, *ap*, *newdev*, *cnn*) *SSC*'=*SSC*\{<*s*, *scene*>|*s*∈*session* (*sc*)}∪{<*s*, *scene*'>|*s*∈session (*sc*)} *QSC*'=*QSC*\{<*q*, *scene*>|*q*∈*entity*(*sc*)}∪{<*q*, *scene*'>| *q*∈entity(*sc*) } *SCP*'=*SCP*\{<*scene*, *p*>|*p*∈*permission*(*sc*)}∪{ <*scene*', *p*>|*p*∈*permission*(*sc*)} *SCENES*'=*SCENES*\{*scene*}∪{*scene*'}⊳
modCnn	修改场景的网络因素 *modCnn*(*cnn*?, *oldcnn*, *newcnn*?: *NAME*)⊲ if *sc.oldcnn*∈*CNNSTATES* and *sc.newcnn*∉*CNNSTATES* then *CNNSTATES*'=*CNNSTATES*∪{*newcnn*} *scene*'=(*time*, *ap*, *dev*, *newcnn*) *SSC*'=*SSC*\{<*s*, *scene*>|*s*∈*session* (*sc*)}∪{<*s*, *scene*'>|*s*∈session (*sc*) } *QSC*'=*QSC*\{<*q*, *scene*>|*q*∈*entity*(*sc*)}∪{<*q*, *scene*'>| *q*∈*entity*(*sc*)} *SCP*'=*SCP*\{<*scene*, *p*>|*p*∈*permission*(*sc*)}∪{ <*scene*', *p*>|*p*∈*permission*(*sc*)} *SCENES*'=*SCENES*\{*scene*}∪{*scene*'}⊳
det_Conflict	检测是否存在与给定场景冲突的场景，若有则返回 true 以及与之相冲突的场景，否则，返回 false *det_Conflict*(*scene*?, *p*?:*NAME*, *resultdc*!: *BOOLEAN*, *resultsc*:*NAME*)⊲ ∀*sc*∈*SCENES*, if *sc* ≼ *scene* and *sc.p* ⊄ *scene.p* then *resultdc* =true, *resultsc*=*sc* else *outresult*=false⊳
che_Scene	检查场景 *che_Scene*((*t*, *ap*, *dev*, *cnn*)?: *NAME*; *outresult*!: *BOOLEAN*)⊲ if *CheckT*(*t*) and *CheckDev*(*dev*, *valuegAttr*, *valuesAttr*) and *CheckAp*(*ap*, *valuegAttr*, *valuesAttr*) and *CheckCNN*(*cnn*, *valuegAttr*, *valuesAttr*) then *outresult*!=true⊳

话、为会话分配场景。

表 4　　会话管理类

函数名	描述
ass_QSe	为访问请求实体分配会话 *ass_QSe*(*s*?: *NAME*, *q*?:*QUERY*)◁ if (*q*, *s*) ∉*QSE* then *QSE*'= *QSE*∪(*q*, *s*)▷
ass_SeSc	为会话分配场景 *ass_SeSc*(*s*?, *sc*?: *NAME*)◁ if (*s*, *sc*)∉*SESC* then *SESC*'=*SESC*∪ {(*s*, *sc*)}▷

在认证管理中，管理函数为 *gAttrSel*、*sAttrSel*，如表 5 所示，其功能分别是选择通用属性、安全属性作为控制要素。

在认证管理中，管理函数为 *checkT*、*checkDev*、*checkAp*、*checkCNN*，如表 6 所示，其功能分别是检查时间、设备、接入点、网络因素是否在允许的范围内。

4　结束语

复杂网络环境具有设备动态接入，网络异构、众多和信息跨网流动频繁等特点，上述特点对访问控制技术带来细粒度控制、策略跟随和策略语义归一化等需求。针对上述需求，本文以天地一体化网络为例，通过映射面向网络空间的访问控制机制，提出了面向复杂网络环境的访问控制机制，实现了对复杂网络环境信息流的跨网控制。该机制满足复杂网络环境下细粒度控制、策略跟随和策略语义归一化处理等一系列需求。针对访问控制管理的复杂性，给出了访问控制管理模型，并用 Z 符号形式化地描述了管理模型中的管理函数和管理方法。

表 5　　属性管理类

函数名	描述
gAttrSel	为通用属性选择函数，用来确定哪些通用属性可用作控制要素 *gAttrSel*:(*DEV*, *gAttr*)→*gAttr* /*如 *gAttrAss* (*mobile phone*, <*dLoc*, *dVel*, *dDir*, *dSpectrum*, *dWidth*, *aPrio*>)=<*dLoc*, - , - , -, -, *aPrio*>表示只选择移动手机的 2 个属性（所在的位置和接入优先级）作为控制要素*/ *gAttrSelect*:(*RES*, *gAttr*)→*gAttr* *gAttrSelect*:(*CNN*, *gAttr*)→*gAttr*
sAttrSel	为安全属性选择函数，用来确定哪些安全属性可用作控制要素 *sAttrSel*:(*DEV*, *gAttr*)→*sAttr* *sAttrSel*:(*RES*, *gAttr*)→ *sAttr* *sAttrSel*:(*CNN*, *gAttr*)→ *sAttr*

表 6　　认证管理类

函数名	描述
checkT	检查当前时间是否在允许范围内 *checkT* (*t*?: *NAME*; *outresult*!: *BOOLEAN*)◁ if *t*∈*TSTATES* then *outresult*!=true▷
checkDev	检查所使用的设备是否在允许范围内 *checkDev*(*dev*?, *valuegAttr*?, *valuesAttr*?: *NAME*; *outresult*!: *BOOLEAN*)◁ if (*valuegAttr*∈$allowedValue_{gAttr}$(*gAttrSelect*(*dev*, *gAttr*))) and (*valuesAttr*∈$allowedValue_{sAttr}$(*sAttrSelect*(*dev*, *sAttr*))) then *outresult*!=true▷
checkAp	检查所使用的接入点是否在允许范围内 *checkAp*(*ap*?, *valuegAttr*?, *valuesAttr*?): *NAME*; *outresult*!: *BOOLEAN*) ◁ if (*valuegAttr*∈$allowedValue_{gAttr}$(*gAttrSelect*(*ap*, *gAttr*))) and (*valuesAttr*∈$allowedValue_{sAttr}$(*sAttrSelect*(*ap*, *sAttr*))) then *outresult*!=true▷
checkCNN	检查所使用的接入网络是否在允许范围内 *checkCNN*(*cnn*?, *valuegAttr*?, *valuesAttr*?): *NAME*; *outresult*!: *BOOLEAN*) ◁ if (*valuegAttr*∈$allowedValue_{gAttr}$(*gAttrSelect*(*cnn*, *gAttr*))) and (*valuesAttr*∈$allowedValue_{sAttr}$(*sAttrSelect*(*cnn*, *sAttr*))) then *outresult*!=true▷

注：函数 $allowedValue_{gAttr}$(*gAttr*)表示通用属性中各个分量所允许的值；*CheckDev* 对∈进行了重载，本文不再定义。

参考文献：

[1] 沈荣骏. 我国天地一体化航天互联网构想[J]. 中国工程科学, 2006, 8(10): 19-30.
SHEN R J. Some thoughts of (Chinese) integrated space-ground network system[J]. Engineering Science, 2006, 8(10): 19-30.

[2] GUBBI J, BUYYA R, MARUSIC S, et al. Internet of things (IoT): a vision, architectural elements, and future directions[J]. Future Generation Computer Systems, 2013, 29(7): 1645-1660.

[3] 张蓉, 徐晔, 闵小峰. 美协会发表 2016 年卫星产业状况报告[J].中国航天, 2016, 8: 38-44.
ZHANG R, XU Y, MIN X F. 2016 SIA state of the satellite industry report[J]. Aerospace China, 2016, 8: 38-44.

[4] ANGGOROJATI B, MAHALLE P, PRASAO N R, et al. Capability-based access control delegation model on the federated IoT network[C]//Symposium on Wireless Personal Multimedia Communications. 2012: 604-608.

[5] GUSMEROLI S, PICCIONE S, ROTONDI D. IoT access control issues: a capability based approach[C]//The IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. 2012: 787-792.

[6] GUSMEROLI S, PICCIONE S, ROTONDI D. A capability-based security approach to manage access control in the internet of things[J]. Mathematical and Computer Modelling, 2013, 58(5): 1189-1205.

[7] SAMARATI P, VIMERCATI S D C D. Access control: policies, models, and mechanisms[C]//International School on Foundations of Security Analysis and Design. 2000: 137-196.

[8] CHEUNG H, YANG C, et al. New smart-grid operation-based network access control[C]//The IEEE International Conference on Energy Conversion Congress and Exposition. 2015: 1203-1207.

[9] FERRAIOLO D F, SANDHU R, GAVRILA S, et al. Proposed NIST standard for role-based access control[J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274.

[10] BERNABE B, RAMOS J, GOMEZ A F S, et al. TACIoT: multidimensional trust-aware access control system for the Internet of Things[J]. Soft Computing, 2016, 20(5): 1763-1779.

[11] GRANDISON T, SLOMAN M. A survey of trust in internet applications[J]. IEEE Communications Surveys & Tutorials, 2000, 3(4): 2-16.

[12] 封孝生, 刘德生, 乐俊, 等. 临近空间信息资源访问控制策略初探[J]. 计算机应用研究, 2008, 25(12): 3702-3704.
FENG X S, LIU D S, YUE J, et al. Exploration on access control to near space information resources[J]. Application Research of Computers, 2008, 25(12): 3702-3704.

[13] HUR J, NOH D K. Attribute-based access control with efficient revocation in data outsourcing systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(7): 1214-1221.

[14] QI H, MA H, LI J, et al. Access control model based on role and attribute and its applications on space-ground integration networks[C]//The IEEE International Conference on Computer Science and Network Technology. 2015: 1118-1122.

[15] KULKARNI D, TRIPATHI A. Context-aware role-based access control in pervasive computing systems[C]//The ACM Symposium on Access Control Models and Technologies. 2008: 113-122.

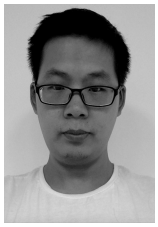
[16] 李凤华, 王彦超, 殷丽华, 等. 面向网络空间的访问控制模型[J]. 通信学报, 2016, 37(5): 9-20.
LI F H, WANG Y C, YIN L H, et al. Novel cyberspace-oriented access control model[J]. Journal on Communications, 2016, 37(5): 9-20.

[17] DORNYEI Z. Motivational strategies in the language classroom[M]. Cambridge: Cambridge University Press, 2001.

[18] SANDHU R S, COYNE E J. Role-based access control models[J]. Computer, 1996, 29(2): 38-47.

[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程师、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。



陈天柱（1987-），男，河北秦皇岛人，中国科学院信息工程研究所博士生，主要研究方向为信息安全。

王震（1984-），男，山东聊城人，博士，杭州电子科技大学副研究员、硕士生导师，主要研究方向为网络与系统安全、博弈论。

张林杰（1972-），女，河北乐亭人，中国电子科技集团公司第五十四研究所研究员，主要研究方向为网络安全、通信网络与系统。

史国振（1974-），男，河南济源人，博士，北京电子科技学院副教授、硕士生导师，主要研究方向为网络安全、嵌入式系统、访问控制。

郭云川（1977-），男，四川营山人，博士，中国科学院信息工程研究所副研究员，主要研究方向为物联网安全、形式化方法。