

# 基于堆结构的域间访问控制模型

刘思聪<sup>1</sup>, 郑日忠<sup>2</sup>, 张启坤<sup>1</sup>, 蔡增玉<sup>1</sup>, 甘勇<sup>1</sup>

(1. 郑州轻工业学院 计算机与通信工程学院 河南 郑州 450001;

2. 河南建筑职业技术学院 河南 郑州 450064)

**摘要:** 访问控制是保障秘密信息免受非法访问及获取的关键技术之一, 基于信任机制的访问控制是其常用的方法。鉴于堆结构具有较快的收敛速度, 能高效地反馈信息, 以及贝叶斯算法能够有效地预测未知访问者的可靠度和信任度, 提出基于堆结构的多域间访问控制模型。通过改进贝叶斯算法, 建立一种更加准确的信任度预测方法。将堆结构和改进的贝叶斯算法相结合, 建立基于堆结构的信任体制。通过堆的性质及固有的计算效率, 以及贝叶斯信任度预测算法的准确性, 提高信任度的收敛速度及准确度。依据信任度的可靠性, 快速、有效地约束域间资源访问, 以实现域间访问控制的目的。实验结果表明, 与相关技术相比, 提出的方案具有高效性和较高的准确率。

**关键词:** 访问控制; 多域; 贝叶斯; 堆

中图分类号: TP393

文献标识码: A

文章编号: 1673-629X(2018)02-0130-05

doi: 10.3969/j.issn.1673-629X.2018.02.028

## Inter-domain Access Control Model Based on Heap Structure

LIU Si-cong<sup>1</sup>, ZHENG Ri-zhong<sup>2</sup>, ZHANG Qi-kun<sup>1</sup>, CAI Zeng-yu<sup>1</sup>, GAN Yong<sup>1</sup>

(1. School of Computer and Communication Engineering, Zhengzhou University of

Light Industry, Zhengzhou 450001, China;

2. Hennan Technical College of Construction, Zhengzhou 450064, China)

**Abstract:** Access control is one of the key technologies to protect confidential information from unauthorized access and stealing. Trust-based access control is a common approach. In consideration of the heap structure with fast convergence speed and efficient information feedback, and the Bayesian algorithm which can effectively predict the reliability and trust of unknown visitors, in this paper we propose a heap-based access control model of multi-domain. We improve the Bayesian algorithm and establish a more accurate trust forecasting. Then combined both heap structure and the improved Bayesian algorithm, a trust system based on heap structure is constructed. For the nature of the heap and its inherent computational efficiency, as well as the accuracy of the Bayesian trust degree prediction algorithm, the convergence speed and accuracy of the trust degree are improved. According to the reliability, it can be fast and effective constraint of resource access between different domains, to achieve the purpose of inter-domain access control. Experiment shows that the proposed scheme is more effective and accurate compared with the related technology.

**Key words:** access control; multi-domain; Bayesian; heap

## 0 引言

访问控制研究是信息安全领域一项十分重要的应用基础研究。访问控制是信息系统安全的核心策略之一, 它与身份认证、入侵检测、安全审计、信息加密、系统恢复、安全保障和风险分析等理论和技术有机结合, 构成信息安全的基础设施, 实现信息系统的信息存储

访问和安全传输信息的可靠性, 防止非授权访问信息和信息泄密, 以确保国家政治军事和经济以及个人隐私的信息安全性。

自20世纪70年代以来, 研究者提出了包括自主访问控制<sup>[1]</sup>、强制访问控制<sup>[2]</sup>、基于角色的访问控制<sup>[3]</sup>、基于任务的访问控制<sup>[4]</sup>、基于行为的访问控制<sup>[5]</sup>

收稿日期: 2016-12-22

修回日期: 2017-04-27

网络出版时间: 2017-10-19

基金项目: 国家自然科学基金资助项目(61572445, 61501406, 61672471); 河南省自然科学基金(162300410322); 河南省高等学校重点科研项目(15A520032, 15A510015)

作者简介: 刘思聪(1985-), 男, 硕士研究生, 研究方向为网络安全; 郑日忠, 讲师, 研究方向为信息安全; 张启坤, 副教授, 研究方向为信息安全; 蔡增玉, 副教授, 研究方向为信息安全; 甘勇, 教授, CCF会员(06714S), 研究方向为信息安全。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20171019.1559.008.html>

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。

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。多域访问控制应运而生,其研究主要集中在多域访问控制系统建模和系统安全策略管理上。在多域访问控制系统建模上,主要通过安全协商来实现安全域间的信任关系,通过角色映射来建立安全域间的安全互操作。安全协商是角色映射的基础和前提。角色映射是域间互访的中介和纽带。因此,安全协商和角色映射成为多域访问控制系统建模的重要研究内容。JOSHI等在研究角色映射方面做了很多开创性的工作,提出了基于策略合并建立多域网络访问控制模型的方法<sup>[6]</sup>,利用角色映射实现策略合并,构建全局的访问控制策略。基于策略合并的建模方法要求参与合并的安全域角色系统具有透明性、稳定性和一致性的特点,但是,由于分布式环境的复杂性和动态性,这种建模方法不能满足多域多应用的动态需求。彭维平等<sup>[7]</sup>对多域环境下基于属性的访问控制模型存在的敏感属性泄露等问题,提出了基于信任度的跨域安全访问控制模型,但系统初始化时效率较低。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,研究者提出了基于使用的访问控制<sup>[8]</sup>、基于时空关联的访问控制<sup>[9]</sup>、基于量化用户和服务的访问控制<sup>[10]</sup>、基于属性的访问控制<sup>[11-13]</sup>和基于行为的访问控制<sup>[14]</sup>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。李凤华等<sup>[15]</sup>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。史姣丽等<sup>[16-17]</sup>在保证数据机密性、防止共谋攻击的前提下,基于CP-ABE方法,在云存储环境中尝试设计多用户协作访问控制方案。

文中提出了一种基于信任堆结构的访问控制模型,在传统访问控制研究基础上,采用改进贝叶斯算法建立一种信任体制。通过调整贝叶斯概率参数提高信任度收敛速度及准确度,通过域内及域外信任权值建立堆结构模型,进而通过信任堆的性质进行有效的资

源访问权限控制。

## 1 改进贝叶斯信任度计算

### 1.1 贝叶斯决策理论

假设总体的概率分布为 $f(x|\theta)$ ,其中 $\theta$ 为未知参数,从整体抽出的样本为 $X_1, X_2, \dots, X_n$ ,用这些样本及其分布概率密度函数对参数 $\theta$ 进行参数估计。

(1) 把未知参数 $\theta$ 看作是一个随机变量(或随机向量),且在抽样之前,对 $\theta$ 有一定的相关信息,称事先得到的这些信息为先验知识。用 $\theta$ 的某种概率分布来表示这种先验知识,记为 $h(\theta)$ ,称概率分布为 $\theta$ 的“先验分布”。该分布反映了在实验之前对未知参数 $\theta$ 所获得的信息的概率分布。

(2) 根据贝叶斯理论,在给定 $X_1, X_2, \dots, X_n$ 的条件下, $\theta$ 的条件概率密度为:

$$h(\theta|X_1, X_2, \dots, X_n) = \frac{h(\theta)f(x_1|\theta) \cdots f(x_n|\theta)}{p(X_1, \dots, X_n)} \quad (1)$$

称该公式为 $\theta$ 的“后验概率密度”。这个条件概率密度表示在有样本 $X_1, X_2, \dots, X_n$ 后对 $\theta$ 的知识概率分布,综合反映了 $\theta$ 的先验分布 $h(\theta)$ 与由样本带来的信息。

(3) 利用后验分布 $h(\theta|X_1, X_2, \dots, X_n)$ 对 $\theta$ 进行推断。

### 1.2 域信任度计算

采用Bayesian决策理论评估某种服务的成功率和失败率,进行域信任度的计算。设节点域 $i$ 与节点域 $j$ 每次交互访问都是随机的,节点域 $i$ 对节点域 $j$ 的评估结果序列为 $ES_{ij}^{rat} = \{es_{ij}^{1, rat}, es_{ij}^{2, rat}, \dots, es_{ij}^{N, rat}\}$ ,  $ES_{ij}^+ = \{es_{ij}^n | es_{ij}^n \in ES_{ij}^{rat}, \text{且} es_{ij}^n, rat = 1\}$ 表示节点域 $i$ 对节点域 $j$ 的积极评价序列集合,  $ES_{ij}^- = \{es_{ij}^n | es_{ij}^n \in ES_{ij}^{rat}, \text{且} es_{ij}^n, rat = 0\}$ 表示节点域 $i$ 对节点域 $j$ 的消极评价序列集合。设积极评价次数 $X_{ij} = |ES_{ij}^+|$ ,消极评价次数 $Y_{ij} = |ES_{ij}^-|$ 。如果完成每次交互成功的概率为 $p$ ,失败的概率为 $q$ ,那么 $p$ 和 $q$ 的Bayesian条件期望估计值 $\tilde{p}$ 和 $\tilde{q}$ 为:

$$\begin{cases} \tilde{p} = \frac{X_{ij} + 1}{N_{ij} + 2} \\ \tilde{q} = \frac{Y_{ij} + 1}{N_{ij} + 2} \\ \tilde{p} + \tilde{q} = 1 \end{cases} \quad (2)$$

则节点域 $i$ 可以对节点域 $j$ 的交互成功概率 $p$ 做出评估推测。

随着节点域 $i$ 对节点域 $j$ 的评价增多,即 $X_{ij}$ 和 $Y_{ij}$ 的值不断增加,对节点域 $j$ 就更加了解,使得对 $p$ 的估

计较为准确。

节点信任评估的最终目标是检测出网络中的恶意节点并将其进行隔离,因而检测率、误检率及漏检率是衡量一个信任评估模型的重要指标。一般来说,检测率越高,误检率越低,信任评估模型就越可靠。然而,原有的基于 Beta 分布的信任评估方案忽略了非入侵因素带来的不合作影响,即由于网络自身故障所带来的节点异常行为或恶意评估等可能会造成较大的误检率。为此,引入异常衰减因子的概念。异常衰减因子记为  $\gamma$ ,表示网络中节点行为异常行为造成的概率。

$$\gamma = \frac{N_{\text{spite}}}{N_{\text{detection}}} \quad (3)$$

其中,  $N_{\text{detection}}$  为网络检测中不合作节点的总数;  $N_{\text{spite}}$  为恶意行为中节点不合作的次数。

直接信任度计算: 令  $Z_{ij}$  和  $F_{ij}$  分别表示节点域  $i$  对节点域  $j$  的评价序列  $ES_{ij}$  中的积极评价次数和消极评价次数,  $\alpha = X_{ij} + 1$  和  $\beta = Y_{ij} + 1$ 。  $p$  和  $q$  为节点域  $i$  对节点域  $j$  完成任务成功和失败的概率,  $E(h(p | \alpha, \beta))$ ,  $E(h(q | \alpha, \beta))$  分别表示 Bayesian 估计的数学期望。那么节点域  $i$  对节点域  $j$  的信任度的计算为:

$$\text{DTV}_{ij} = \begin{cases} E(h(p | \alpha, \beta)) - E(h(q | \alpha, \beta) \gamma) = \frac{\alpha - \gamma\beta}{\alpha + \beta} & \alpha > \lambda \\ 0 & \text{其他} \end{cases} \quad (4)$$

## 2 基于堆结构的访问控制

堆结构是一种重要的集合型数据结构,采用完全二叉树的形式存储可比较的数据,满足如下性质:

(1) 大根性: 令数据节点  $n$  所对应的数据权值为  $f(n)$ , 则对于  $\forall n' \in \text{ancestor}(n)$ , 满足  $f(n') \geq f(n)$ , 任何从低层次节点到高层次节点都要经过一条不减路径, 树根的权值为整个堆的最大权值。

(2) 路径长度有界性: 由于堆采用完全二叉树来存储数据, 因此对于有  $n$  个数据节点的堆, 从堆底(叶节点)到堆顶(根节点)的路径长度不会超过  $\log(n+1)$ , 为对数级, 因此随数据量的增长而增长缓慢。这一特性使得堆结构为数据集的排序(反复摘顶)、插入、修改、删除算法提供了良好的高效率支持, 使得对  $n$  个节点的数据集合排序的算法复杂度能够稳定在  $O(n \log n)$ , 插入、删除、修改的复杂度均稳定在  $O(\log n)$ 。

### 2.1 基于堆结构的信任访问控制模型

在本模型中, 根据贝叶斯决策理论建立各域的信任度, 将网络中多个域按照可信度的高低顺序组合成一个大根堆, 使得可信度越高的域离堆顶越近, 堆顶对

应于可信度最高的域。此时, 对于每个域, 其相对可信度区间为  $[0, 1]$ 。为方便计算, 本模型定义该信任度区间为  $[0, 10]$ , 模型结构如图 1 所示。其中的空心箭头描述了请求的传递路径, 而灰色箭头描述了令牌的传递路径。  $W_i$  ( $i = A, B, C, D, E$ ) 分别表示域内节点  $A, B, C, D, E$  的权值;  $AS_i$  ( $i = 1, 2, \dots, 5$ ) 表示域  $i$  的授权服务器, 用于接收用户的权限请求, 并根据该请求计算出所需的最小角色;  $SrcID$  表示域身份信息;  $Token$  表示令牌, 用于将用户的请求信息、身份信息和角色信息封装为请求, 并沿堆层次向上传递;  $DV$  表示域信任度;  $RSV$  表示请求资源权值;  $ASV$  表示访问资源权值。

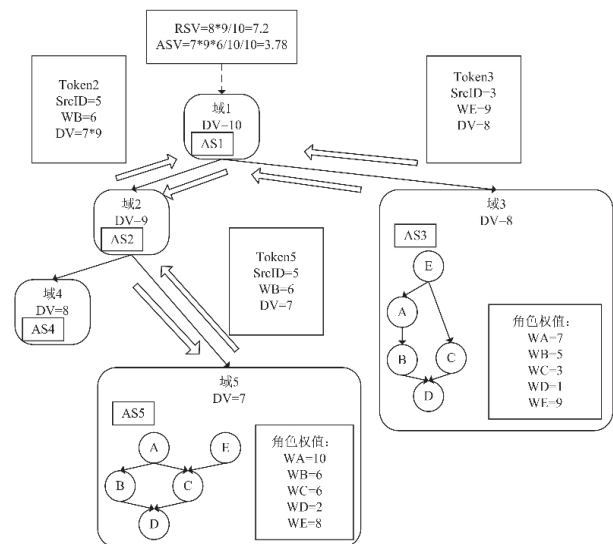


图 1 基于堆结构的访问

### 2.2 资源访问控制过程

如图 1 所示, 当域 3 中具有角色  $E$  的用户请求访问域 5 中的资源  $B$  时, 模型的工作流程如下:

(1) 路径探查: 域 3 中的用户  $U$  将请求发送至路径计算模块, 该模块为其计算出从  $U$  所在的域到目标资源所在的域的堆路径, 返回给  $U$ , 由树节点间路径的唯一性可知, 该路径是唯一的。

(2) 请求发送: 域 3 中具有角色  $E$  的用户将其身份信息、角色信息以及请求的权限按照该路径传递给域 5 的授权服务器。

(3) 最小角色获取: 域 5 的授权服务器(Authority Server)根据用户请求和自身的角色层次结构计算出角色  $B$  为包含用户请求权限的最小角色。

(4) 域 3 中的令牌生成模块为用户创建一个令牌, 将其角色权值及域信任度写入其中, 并沿堆路径向其祖先域传递, 直到传递到域 1, 也即域 3 和域 5 在堆中的最小公共祖先域, 域 1 根据对域 3 的信任程度, 在令牌中写入一个相对可信值。

(5) 与步骤(4)类似, 域 5 的令牌生成模块为  $B$  创建一个令牌, 同样逐层向上传递, 直至传递到域 1, 每

次传递中经过的域也都向该令牌写入对下层域的相对可信值。

(6) 来自域3和域5的令牌最终都到达了域1,域1将每个令牌中的角色权值和所有经过域信任度值相乘,并按信任值上界,假设为10,进行归一化处理,最终得出域3用户的资源请求值  $RSV = 8 * 9 / 10 = 7.2$ ,域5中角色B的资源访问权值  $ASV = (7 * 6 * 9) / 10 / 10 = 3.78$ ,由于  $RSV > ASV$ ,因此判定该用户有权获得角色B的资源。域5的授权服务器向其签发角色证书,并开启一个新的会话。

(7) 在域3中的用户对域5中的资源进行访问时,域5的授权服务器对其行为进行监控,如果该用户有严重威胁该域资源安全的行为,则可将其角色证书撤销,并沿着步骤(1)中的路径中由域3到域1的部分路径发送遣控令牌(Assest Token),该路径中的所有域都会接收到该令牌。

(8) 当一个域接收到过多的遣控令牌后,该域的信任值会自动下降,此时可通过堆调整或删除操作来重新调整堆结构。

(9) 当用户对资源的访问结束后,会话被终止,该用户的角色证书也随即被撤销。域5的管理员可以写入一些审计信息。

代码框架如下:

```
requestPrim( target) {
    path = askForPath( target); //计算堆路径
    createRequest( priv); //创建对特定权限的请求
    createToken( credentials); //根据自身角色证书初始化令牌
    primeToken( path, LCA( this, target)); //沿路径向上传递令牌
}

requestHandle( request, path) {
    mini_role = calculate_mini_role( request); //根据请求和自身角色层次结构计算出可能的最小角色映射
    createToken( mini_role); //根据该角色生成一个角色令牌
    primeToken( path, LCA( this, request.source)); //沿路径向上传递令牌
}

writeCredential( token) {
    write( token, this, token.source); //向令牌中写入对子域的信任评价
}

tokenJustify( tokenSource, tokenTarget) {
    src = calculateTokenCredential( tokenSource);
    dst = calculateToken( Credential( tokenTarget)); //计算两个令牌的归一化信任评价
    if( src >= dst) { allow access; }
    else{ deny access; } //如果源令牌的信任评价高于目的角色令牌,则允许访问,否则拒绝访问
}
```

### 3 实验与分析

实验中构建60个实体域,诚实数量和不诚实数量各占50%,观察随着实体间交互次数的不断增加,信任模型中某一节点域*i*对诚实实体域*j*和不诚实实体域*k*的信任度的变化情况,仿真实验参数如表1所示。

表1 实验参数表

域实 体数	诚实 实体	不诚实 实体	初始信 任度	信任度 阈值	取值
60	50%	50%	0.5	0.4	0.9

图2中显示的是随着访问次数的增多,节点*i*对诚实节点*j*和不诚实节点*k*的信任度的变化趋势。由于初始信任度为0.5,满足实体间相互访问的阈值为0.4的要求,所以在一开始,各个实体是能够相互访问的。

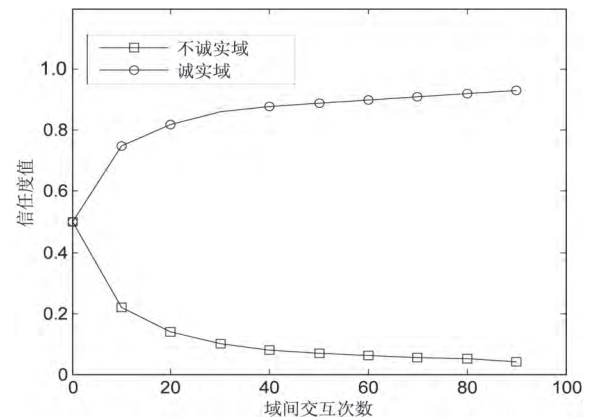


图2 随着交互次数增加节点*i*对两类节点的信任度的变化曲线

从图2中可以看出,随着访问次数的增多,被访问节点对诚实节点的信任度逐渐升高,而对不诚实节点的信任度逐渐降低。由此,在以后的访问中,被访问的节点就可以预先识别出访问节点是否诚实,从而预先做出允许访问还是拒绝访问的判断。

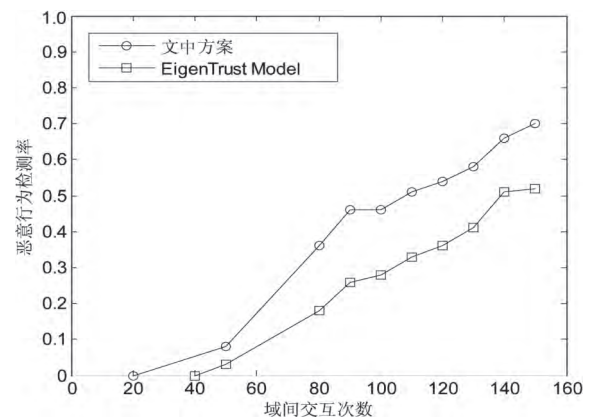


图3 两种模型恶意行为检测准确率对比曲线

观察随着实体间交互次数的不断增加,文中提出的信任度模型和采用EigenTrust模型检测出恶意行为

的准确率的变化的情况。实验参数的设置与实验 1 相同,结果如图 3 所示。

由图 3 可见,采用提出的信任度模型预测不诚实实体的准确率比 EigenTrust 信任度模型收敛的速度快。

## 4 结束语

分析了现有访问控制模型,在已有研究的基础上提出改进贝叶斯信任度计算及对模型构建域间访问控制模型。信任度计算方法有所改进,一定程度上提高了检测的收敛速度,有利于根据信任度的变化进行模型的调整和重构,具有效率高、速度快的特点。

## 参考文献:

- [1] 张宏, 贺也平, 石志国. 基于周期时间限制的自主访问控制委托模型[J]. 计算机学报, 2006, 29(8): 1427-1437.
- [2] 陈俊欣, 张凤荔, 刘渊. 基于角色的空间信息强制访问控制模型研究[J]. 计算机应用研究, 2016, 33(7): 2170-2174.
- [3] 熊厚仁, 陈性元, 杜学绘, 等. 基于角色的访问控制模型安全性分析研究综述[J]. 计算机应用研究, 2015, 32(11): 3201-3208.
- [4] 邓集波, 洪帆. 基于任务的访问控制模型[J]. 软件学报, 2003, 14(1): 76-82.
- [5] 熊金波, 姚志强, 马建峰, 等. 基于行为的结构化文档多级访问控制[J]. 计算机研究与发展, 2013, 50(7): 1399-1408.
- [6] JOSHI J B D. A generalized temporal role based access control model for developing secure systems [D]. USA: Purdue

University 2013.

- [7] 彭维平,刘雪贞,郭海儒,等.基于信任度的跨域安全访问控制模型研究[J].计算机应用研究,2016,33(6):1797-1796.
- [8] 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:ACM,2008:683-695.
- [9] 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.
- [10] 刘庆云,沙泓州,李世明,等.一种基于量化用户和服务的大规模网络访问控制方法[J].计算机学报,2014,37(5):1195-1205.
- [11] YUAN E,TONG J.Attributed based access control (ABAC) for Web services[C]//IEEE international conference on web services.FL,USA:IEEE,2005:561-569.
- [12] 房梁,殷丽华,郭宇川,等.基于属性的访问控制关键技术研究综述[J].计算机学报,2017,40(7):1680-1698.
- [13] 黄保华,贾丰玮,王添晶.云存储平台下基于属性的数据库访问控制策略[J].计算机科学,2016,43(3):167-173.
- [14] 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.
- [15] 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.
- [16] 史姣丽,黄传河,王晶,等.云存储下多用户协同访问控制方案[J].通信学报,2016,37(1):88-99.
- [17] 王晶,黄传河,王金海.一种面向云存储的动态授权访问控制机制[J].计算机研究与发展,2016,53(4):904-920.

(上接第 106 页)

- 题研究[J].电信科学, 2003, 19(7): 22-27.
- [5] 杨胜文, 史美林. 一种支持 QoS 约束的 Web 服务发现模型[J]. 计算机学报, 2005, 28(4): 589-594.
- [6] KUIPERS F A. Quality of service routing in the internet: the-ory, complexity and algorithms [M]. [s.l.]: IOS Publisher, 2004.
- [7] 朱慧玲, 杭大明, 马正新, 等. QoS 路由选择: 问题与解决方法综述[J]. 电子学报, 2003, 31(1): 109-116.
- [8] 闵应骅. 计算机网络路由研究综述[J]. 计算机学报, 2003, 26(6): 641-649.
- [9] MASIP-BRUIÑ X, YANNUZZI M, DOMINGO-PASCUAL J, et al. Research challenges in QoS routing [J]. Computer Communications, 2006, 29(5): 563-581.
- [10] YU C, LUMEZANU C, ZHANG Y, et al. FlowSense: monitoring network utilization with zero measurement cost [C]//International conference on passive and active network measurement. Berlin: Springer, 2013: 31-41.
- [11] SUH J, KWON T T, DIXON C, et al. OpenSample: a low-late-

- tency, sampling-based measurement platform for commodity SDN [C]//International conference on distributed computing systems. Madrid, Spain: IEEE, 2014: 228–237.
- [12] 崔勇, 吴建平, 徐恪, 等. 互联网络服务质量路由算法研究综述 [J]. 软件学报, 2002, 13(11): 2065–2075.
- [13] EGILMEZ H E, DANE S T, BAGCI K T, et al. OpenQoS: An OpenFlow controller design for multimedia delivery with end-to-end quality of service over software-defined networks [C]//Signal & information processing association summit and conference. Hollywood, California, USA: IEEE, 2012.
- [14] CUI H Y, ZHU Y, YAO Y, et al. Design of intelligent capabilities in SDN [C]//International conference on wireless communications, vehicular technology, information theory and aerospace & electronic systems. Aalborg, Denmark [s. n.], 2014: 1–5.
- [15] YAN Jinyao, ZHANG Hailong, SHUAI Qianjun. HiQoS: an SDN-based multipath QoS solution [J]. China Communications, 2015, 12(5): 123–133.