doi:10.11959/j.issn.1000-436x.2015295

# 基于贝叶斯决策理论的风险最小化的授权映射方法

赵斌[1,2]，何泾沙[1]

（1. 北京工业大学 软件学院，北京 100124；2. 济宁学院 计算机科学系，山东 曲阜 273155）

**摘 要**：授权决策是访问控制理论研究中的关键问题之一。为了有效提高基于信任的访问控制中授权的安全性，依据最小风险贝叶斯决策理论，将访问控制中客体对主体的授权视为最优决策的发现问题，提出基于风险最小化授权映射方法，实现访问控制中准确的授权操作。通过算例分析和仿真实验表明，该方法能够在降低风险的情况下比较准确地给出交互的最终授权。

**关键词**：访问控制；贝叶斯决策理论；信任；风险；授权映射

**中图分类号**：TN301.6 **文献标识码**：A

# Bayes decision theory based risk minimization authorization mapping

ZHAO Bin[1,2], HE Jing-sha[1]

(1. School of Software Engineering, Beijing University of Technology, Beijing 100124, China;
2. Department of Computer Science, Jining University, Qufu 273155, China)

**Abstract:** Authorization decision was one of the key issues in the control access. In order to effectively enhance the security of authorization in trust based access control authorization, according to minimization risk Bayes decision theory, authorization was the object to the subject in access control as found that the problem of optimal decision. A method that minimizates risk based authorization mapping to realize correct authorization operation in the access control was proposed. Example analysis and simulation experiment show that the method is able to reduce risk accurately to interaction final authorization.

**Key words:** access control; Bayes decision theory; trust; risk; authorization mapping

## 1 引言

近年来，随着网络技术和通信技术的发展，网络安全问题成为人们关注的焦点，而作为授权管理的基于信任的访问控制技术成为网络安全中的研究热点[1~3]。

授权决策是访问控制理论研究中的关键问题之一。目前，国内外在访问控制中访问授权方面的研究成果较多。王婷等在文献[4]中通过比较分析已有的访问控制模型中的关键技术，研究了开放式网络中访问主体和访问客体交互过程中客体资源管理的重要性，指出客体资源管理是开放式网络环境中实现统一授权管理的基础。在基于信任的动态访问控制组成架构的基础上，文献[5]考虑交互历史参数、奖惩因子、推荐实体评价可信度等多影响因子实现信任的计算，引入平衡权重因子解决直接信任和推荐信任的权重分配问题，提出了面向开放式网络基于平衡权重的动态信任综合度量方法。为满足云计算领域内访问控制需求，文献[6]提出了一个云社区用户授权解决方案及其系统安全性分析。对

**收稿日期**：2015-10-24

**基金项目**：国家高技术研究发展计划（“863”计划）基金资助项目（2015AA017204）；国家自然科学基金资助项目（61272500）；山东省自然科学基金资助项目（ZR2013FQ024）；北京自然科学基金资助项目（4142008）；山东省高校科技计划基金资助项目（J12LN70, J14LN80）；北大方正集团有限公司数字出版技术国家重点实验室开放课题基金资助项目

**Foundation Items:** The National High Technology Research and Development Program of China (863 Program) (2015AA017204); The National Natural Science Foundation of China (61272500); The Natural Science Foundation of Shandong Province (ZR2013FQ024); The Natural Science Foundation of Beijing (4142008); The Opening Project of State Key Laboratory of Digital Publishing Technology

RBAC 用户授权查询(UAQ)问题，文献[7]提出一个更全面的方法，该方法包括不可约性、角色基数和权限基数约束等优化。

但是，基于决策理论研究授权映射问题较少，唐杰等在文献[8]中提出最小风险的本体映射模型，将映射发现问题转换成风险最小化问题，提供了一个基于贝叶斯决策理论多策略的本体映射方法。宋利康等在文献[9]中提出了一种企业模型与 ERP 系统间的映射元模型, 给出权限的映射信息和映射规则方法。鲍翊平等在文献[10]中采用本体映射技术提出了一种基于本体映射处理推荐信任信息的模型，实现开放分布式的网络环境中基于不同信任本体的各实体间的有效交互，满足实体间推荐信任信息的共享和交流。结合位置与身份分离映射理论，在分析了位置与身份分离协议中可能存在的映射欺骗威胁所带来的安全隐患的情况下，文献[11]提出了一种基于信任度模型的新型映射机制。以上的研究者们主要集中在映射方法和模型的建立与设计，忽视了访问控制中授权的风险性安全问题。

在访问控制中，访问客体将资源提供给访问主体以获得最大收益，在长期的交互过程中，访问客体希望提供资源共享的最小化，收益最大化，并且尽可能的减少映射开销，维持交互的负载均衡，这就是访问客体授权映射算法的主要目标[12]。为了有效提高基于信任的访问控制中授权的安全性，使访问客体获得最大化的收益，本文依据最小风险贝叶斯决策理论，将访问控制中客体对主体的授权视为最优决策的发现问题，提出基于风险最小化授权映射方法，实现访问控制中准确的授权操作。

## 2 贝叶斯决策理论

决策理论是基于概率统计方法和决策代价进行分类的理论之一。贝叶斯决策理论是利用概率论中的贝叶斯公式，决策得出风险最小化的分类规则。贝叶斯决策理论为不确定性推理决策提供了坚实的基础[13]。贝叶斯决策评价决策有多种准则，贝叶斯决策常用的准则有：最小错误率准则、最小风险准则、Neyman-Pearson 准则和最小最大决策准则。对于同一个问题，采用不同的决策准则会得到不同意义下的“最优”决策。最小风险贝叶斯决策是考虑各种错误决策造成的损失不同而提出的一种决策规则。

**定义 1** （贝叶斯公式）。在连续情况下，假定要识别的向量样本 $\boldsymbol{x}=[x\_1,x\_2,\cdots,x\_m]^{\mathrm{T}}$，类型空间为：$\Omega=(\omega_1,\omega_2,\cdots,\omega_c)$，有如下定义。

1) 先验概率 $P(\omega_i)$，表示由样本的先验知识得到的类别分布。

2) 类条件概率密度 $P(\boldsymbol{x}\mid\omega_i)$，表示样本在 $\omega_i$ 类条件下的分布。

3) 后验概率 $P(\omega_i\mid\boldsymbol{x})$，表示样本 $\boldsymbol{x}$ 属于 $\omega_i$ 类别的概率。

4) 贝叶斯公式

$$P(\omega_i\mid\boldsymbol{x})=\frac{P(\boldsymbol{x}\mid\omega_i)P(\omega_i)}{\sum_1^c P(\boldsymbol{x}\mid\omega_i)P(\omega_i)} \tag{1}$$

由上面的定义可知，贝叶斯决策有 2 个基本条件：每个类别的总体概率分布是已知的，也就是先验概率和类条件概率密度已知；决策分类的类别数是一定的。因此，依据贝叶斯公式，得到贝叶斯决策规则如下。

当 $c$=2，样本 $\boldsymbol{x}$ 出现时，通过后验概率 $P(\omega_1\mid\boldsymbol{x})$ 和 $P(\omega_2\mid\boldsymbol{x})$ 的大小判断 $\boldsymbol{x}\in\omega_1$ 还是 $\boldsymbol{x}\in\omega_2$。形式化描述为

$$\begin{cases}\boldsymbol{x}\in\omega_1, P(\omega_1\mid\boldsymbol{x})>P(\omega_2\mid\boldsymbol{x})\\ \boldsymbol{x}\in\omega_2, P(\omega_1\mid\boldsymbol{x})<P(\omega_2\mid\boldsymbol{x})\end{cases}$$

因此，多类问题的贝叶斯决策规则形式化描述为

$$P(\omega_i\mid\boldsymbol{x})=\max_{j=1,2,\cdots,c}P(\omega_j\mid\boldsymbol{x}),\quad \boldsymbol{x}\in\omega_i \tag{2}$$

由式(2)可知，贝叶斯决策规则依据后验概率最大做出判决，得到了分类错误率最小的结果，即贝叶斯公式保证了错误率最小，但是最小的错误率并不一定代表最好的指标，因为，有些情况下分类错误引起的“损失”可能比错误本身对决策起的影响作用更大，因此引入与损失关联的风险来衡量决策，使决策造成的损失最小。

**定义 2** （条件风险函数）。向量样本 $\boldsymbol{x}=[x\_1, x\_2,\cdots, x\_m]^{\mathrm{T}}$，给定类型状态空间 $\{\omega_1,\omega_2,\cdots,\omega_c\}$ 有 $c$ 个有限的类别，决策空间 $\{a_1,a_2,\cdots,a_k\}$ 有 $k$ 种决策，样本 $\boldsymbol{x}$ 属于 $\omega_j$ 时，采取 $\alpha_i$ 决策引起的损失为 $\lambda(\alpha_i\mid\omega_j)$，则 $x$ 的条件风险函数为

$$R(\alpha_i\mid\boldsymbol{x})=\sum\nolimits_j\lambda(\alpha_i\mid\omega_j)P(\omega_j\mid\boldsymbol{x}) \tag{3}$$

将决策 $\alpha$ 视作随机向量 $\boldsymbol{x}$ 的函数，记为 $\alpha(\boldsymbol{x})$。式(3)可改写为

$$R(\alpha(\boldsymbol{x})\mid\boldsymbol{x})=\sum\nolimits_j\lambda(\alpha(\boldsymbol{x})\mid\omega_j)P(\omega_j\mid\boldsymbol{x}) \tag{4}$$

**定义 3**　期望风险。期望风险 $R$ 反映对整个特征空间中所有向量样本 $\boldsymbol{x}$ 的取值都采用相应的决策 $\alpha(\boldsymbol{x})$ 所带来的平均风险。

$$R=\int R(\alpha(\boldsymbol{x})\,|\,\boldsymbol{x})p(\boldsymbol{x})\mathrm{d}\boldsymbol{x}$$

最小风险贝叶斯决策指如果在所有对 $\boldsymbol{x}$ 的决策过程中，每一个决策行为 $\alpha$ 都使其条件风险 $R(\alpha(\boldsymbol{x})\,|\,\boldsymbol{x})$ 最小，则其期望风险 $R$ 也是最小，最小风险贝叶斯决策规则形式化描述为

$$R(\alpha_k\,|\,\boldsymbol{x})=\min_{j=1,2,\cdots,c}R(\alpha_k\,|\,\boldsymbol{x}),\quad \alpha\in\alpha_k$$

因此，最小风险贝叶斯决策就是考虑各种错误造成的损失不同而提出的一种决策规则。

## 3　基于风险最小化授权映射方法

### 3.1　算法分析

在开放式网络基于信任的访问控制授权问题中，要识别的向量样本数据为交互实体 *entity*（主体 $s$ 和客体 $o$）的所有属性及属性组合对应的信任组合 $at_i$，将信任—权限的信任条件策略（如表 1 所示访问授权许可决策表 $S_i$）看作一个分类类别，表示一种状态 $\omega_j$。每个可以分类到某个分类类别 $\omega_j$，即表示存在信任组合 $at_i$ 到类别 $\omega_j$ 的映射。使用 $P(\omega_i\,|\,at_i)$ 表示实体所有属性及属性组合对应的信任组合 $at_i$ 映射到状态 $\omega_j$ 的后验概率。令 $Risk(\alpha_i,\omega_j)$ 表示在状态 $\omega_j$ 下做出 $\alpha_i$ 授权决策得到的损失，即条件风险函数，其定义为

$$R(\alpha_i\,|\,at_i)=\sum\nolimits_j Risk(\alpha_i,\omega_j)P(\omega_i\,|\,at_i)\quad(5)$$

期望风险为

$$R=\int Risk(\alpha_i,\omega_j)p(at_i)\mathrm{d}(at_i)$$

**表 1**　　访问授权许可决策表

| 策略 | 属性 | | | | |
|---|---|---|---|---|---|
| | $A_1^D$ | $A_2^D$ | … | $A_n^D$ | $Q_i^P$ |
| $S_1$ | T | GT | … | BT | Y |
| $S_2$ | | FT | … | | Y |
| $S_3$ | | GT | … | BT | Y |
| $S_4$ | T | | … | BT | Y |
| … | … | … | … | … | … |
| $S_m$ | GT | GT | … | GT | Y |

注：$A_i^D$ 表示访问许可的决策属性；$Q_i^P$ 是访问主体的访问请求权限许可集合；$S_i$ 表示对 $Q_i^P$ 的访问控制策略规则。Y 代表赋权，N 代表拒绝。$U$=3 表示信任未知，T=4 表示信任，GT=5 表示比较信任，BT=6 表示非常信任，FT=7 表示完全信任；$S_i$ 表示对 DA 的访问控制策略规则。

风险最小化映射的优化策略为每个满足信任—权限的授权映射策略提供一个风险函数。

$$Risk(\alpha_i,\omega_j)=lost(\alpha_i,o,s,\omega_j,at_i)$$

其中，决策行为 $\alpha_i$ 表示客体 $o$ 在状态 $\omega_j$ 下对主体 $s$ 的授权决策行为。$at_i$ 表示交互实体所有属性及属性组合对应的信任组合。

风险值最小的授权决策问题就转化为对每个信任组合 $at_i$ 的最优决策行为 $\alpha_i$ 的求解，即寻找风险最小的行为许可，从而得到全局最优行为 $\{\alpha_i\}$，即风险最小的授权，形式化描述如下

$$R(\alpha_i\,|\,at_i)=\min_{i=1,2,\cdots,c}R(\alpha_i\,|\,at_i),\alpha=\alpha_i$$

$$\alpha_i=\arg_{\{\alpha_i\}}\min_{i=1,2,\cdots,c}R(\alpha_k\,|\,at_i)$$

风险函数的作用为：一是选择成功通过信任-权限的授权映射作为最终的授权许可映射，二是如果成功通过信任—权限的授权映射均低于设定的风险阈值，则主体将不能获得资源客体的最终权限许可。授权映射最优化问题就转化为授权决策行为最优化问题，即采取风险值最小的授权决策行为。

### 3.2　算法步骤

根据以上算法分析，基于风险最小化授权映射算法步骤如下。

**步骤 1**　初始化系统风险阈值 $\varepsilon$，$P(at_i\,|\,\omega_i)$ 和 $P(\omega_i)$ 等参数。

**步骤 2**　根据

$$P(\omega_i\,|\,at_i)=\frac{P(at_i\,|\,\omega_i)P(\omega_i)}{\sum_1^c P(at_i\,|\,\omega_i)P(\omega_i)}$$

求出 $P(\omega_i\,|\,at_i)$。

**步骤 3**　依据 $P(\omega_i\,|\,at_i)$ 和表 2 授权决策状态损失表，根据式（5）求解出采取 $\alpha_i$ 授权决策的条件风险 $R(\alpha_i\,|\,at_i)$。

**步骤 4**　对步骤 2 中的 $c$ 个条件风险值 $R(\alpha_i\,|\,at_i)$ 进行比较，求解出

$$\arg_{\{\alpha_i\}}\min_{i=1,2,\cdots,c}R(\alpha_k\,|\,at_i)$$

**步骤 5**　如果 $\arg_{\{\alpha_i\}}\min_{i=1,2,\cdots,c}R(\alpha_k\,|\,at_i)\leqslant\varepsilon$，进行授权，否则，拒绝授权。

**步骤 6**　算法结束。

**表 2 授权决策状态损失表**

| 状态 | 决策 | | | |
|---|---|---|---|---|
| | $\omega_1$ | $\omega_2$ | … | $\omega_c$ |
| $\alpha_1$ | $Risk(\alpha_1,\omega_1)$ | $Risk(\alpha_1,\omega_2)$ | … | $Risk(\alpha_1,\omega_c)$ |
| $\alpha_2$ | $Risk(\alpha_2,\omega_1)$ | $Risk(\alpha_2,\omega_2)$ | … | $Risk(\alpha_2,\omega_c)$ |
| ⋮ | ⋮ | ⋮ | … | ⋮ |
| $\alpha_i$ | $Risk(\alpha_i,\omega_1)$ | $Risk(\alpha_i,\omega_2)$ | … | $Risk(\alpha_i,\omega_c)$ |
| ⋮ | ⋮ | ⋮ | … | ⋮ |
| $\alpha_k$ | $Risk(\alpha_k,\omega_1)$ | $Risk(\alpha_k,\omega_2)$ | … | $Risk(\alpha_k,\omega_c)$ |

在某些情况下，客体对主体执行拒绝授权是比错误判别的决策造成的风险损失要小，所以，当$\arg_{\{\alpha_i\}}\min_{i=1,2,\cdots,c} R(\alpha_k \mid at_i)>\varepsilon$时，执行拒绝授权决策。

授权算法流程图如图 1 所示。

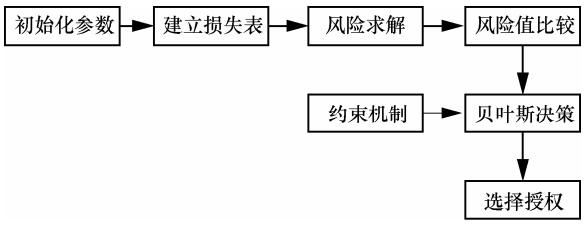


图 1 基于贝叶斯决策理论的风险最小化的授权映射流程

## 4 算例与仿真

### 4.1 算法实例

在面向开放式网络基于信任的访问控制中，客体根据主体$(s_1,s_2)$的综合信任值$at_i$判断是否对主体进行访问请求授权操作。

假设信任-权限策略的授权为$p_1$和$p_2$对应 2 种状态$p\omega_1$和$p\omega_2$，访问主体为$s_1$和$s_2$，系统风险阈值$\varepsilon$=0.7，根据已有知识和经验，系统初始化参数如表 3 所示。

**表 3 实体初始化参数**

| 主体 | $s_1$ | $s_2$ |
|---|---|---|
| $P(p\omega_1)$ | 0.9 | 0.005 |
| $P(p\omega_2)$ | 0.1 | 0.995 |
| $P(at_2 \mid p\omega_1)$ | 0.2 | 0.95 |
| $P(at_2 \mid p\omega_2)$ | 0.4 | 0.05 |
| $\varepsilon$ | 0.7 | |

访问主体$s_1$和$s_2$的授权决策状态损失表如表 4 所示。

**表 4 授权决策状态损失表**

| 状态 | | 决策 | |
|---|---|---|---|
| | | $p\omega_1$ | $p\omega_2$ |
| $s_1$ | $p_1$ | 0 | 1 |
| | $p_2$ | 6 | 0 |
| $s_2$ | $p_1$ | 0 | 1 |
| | $p_2$ | 6 | 0 |

根据最小风险贝叶斯决策规则求得$s_1$的后验概率为$s_1_P(p\omega_1 \mid at_1)$=0.82，$s_1\_P(p\omega_2 \mid at_1)=0.18$，则$s_1_R(p\omega_1 \mid at_1)$=1.1，$s_1\_R(p\omega_2 \mid at_1)$=0.82。所以，$at_1 \in p\omega_2$。

根据最小风险贝叶斯决策规则求得$s_2$的后验概率为$s_2_P(p\omega_1 \mid at_2)$=0.32，$s_2\_P(p\omega_2 \mid at_2)=0.68$，则$s_2_R(p\omega_1 \mid at_2)$=0.68，$s_2\_R(p\omega_2 \mid at_2)$ =1.88。所以，$at_2 \in p\omega_1$。

根据基于风险最小化授权映射方法，根据计算结果$at_1>\varepsilon$，$at_2<\varepsilon$，得出决策结果为对主体$s_1$拒绝访问，对主体$s_2$的访问请求进行$p_1$授权许可。

通过授权约束对所有预先授权进行评估，依据授权约束策略及实体间的关系，通过风险最小化下映射的优化策略进行最优综合授权决策，给出本次交互的最终授权。

### 4.2 仿真结果

为了降低访问控制中客体对主体授权的风险，提高授权的准确性，实现了基于信任的访问控制原型系统，进行了大量的实验。仿真实验环境同文献[5]，假设初始参数取值为：交互节点为 100 个；恶意节点为 0%，10%，20%，30%，40%，50%；每个周期内交互次数为 1 000。实验结果如图 2 所示。

**定义 4** （交互满意率）。指每个周期内所有网络实体节点交互的满意数与总交互数的比值。

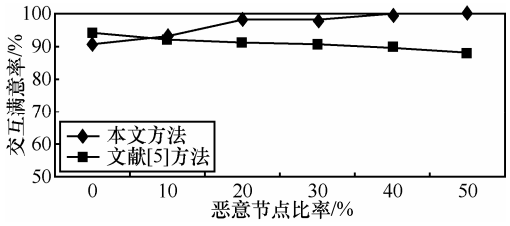


图 2 授权随着恶意节点变化情况

图 2 表示本文所提方法与文献[5]提出的方法在交互授权的满意率随着恶意节点的变化情况的比较。从仿真结果来看，利用本方法的授权随着恶

意节点的增加，交互的满意度越来越高，表明授权准确性越来越高，这种变化趋势是符合本文所提方法的思想；利用文献[5]方法的授权随着恶意节点的增加，交互的满意度降低，表明授权准确性降低；从表 5 中可看出，在授权的准确性方面本文所提的方法优于文献[5]的方法。

**表 5　本文与文献[5]方法的平均交互满意率**

| 实验所用方法 | 平均满意率 |
|---|---|
| 本文方法 | 96.72% |
| 文献[5]方法 | 90.83% |

## 5　结束语

基于最小风险贝叶斯决策理论，将基于信任的访问控制中客体对主体的授权视为最优决策的发现问题，提出基于风险最小化授权映射方法。该方法将最小风险贝叶斯决策运用于基于信任的访问控制授权映射中，为每个满足信任—权限的授权映射策略提供一个风险函数，授权映射最优化问题就转化为授权决策行为最优化问题，即采取风险值最小的授权决策行为。

实际的网络环境中必然会存在一定机率的恶意结点，通过算例分析和仿真实验表明，该方法能够在降低风险的情况下准确给出交互的最终授权，具有交互满意度较高的仿真结果，所以本文所提的方法在基于信任的访问控制授权过程中是有效的。

## 参考文献：


[1] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management[A]. Security and Privacy 1996[C]. 1996. 164-173.

[2] GLYNOS D, ARGYROUDIS P, DOULIGERIS C. Collaborative service evaluation with the two hop trust framework[J]. Security and Communication Networks, 2012,5(6): 594-613.

[3] HAN G, JIANG J, SHU L, *et al*. Management and applications of trust in wireless sensor networks: a survey[J]. Journal of Computer and System Sciences, 2014, 80(3): 602-617.

[4] 王婷, 陈性元, 张斌, 等. 授权与访问控制中的资源管理技术研究综述[J]. 小型微型计算机系统, 2011,32(4):619-625.
WANG T, CHEN X Y, ZHANG B, *et al*. Research of resource management in authorization and access control technology[J].Journal of Chinese Computer Systems, 2011,32(4):619-625.

[5] 赵斌, 何泾沙. 基于平衡权重的动态综合信任度量方法[J]. 北京邮电大学学报, 2015, 38(2):113-117.
ZHAO B, HE J S. Dynamic global trust evaluation based on balance weight[J]. Journal of Beijing University of Posts and Telecommunications, 2015, 38(2):113-117.

[6] MASOOD R, SHIBLI M A, GHAZI Y, *et al*. Cloud authorization: exploring techniques and approach towards effective access control framework[J]. Frontiers of Computer Science, 2015, 9(2): 297-321.

[7] LU J, JOSHI J B D, JIN L, *et al*. Towards complexity analysis of user authorization query problem in RBAC[J]. Computers & Security, 2015, (48): 116-130.

[8] 唐杰, 梁邦勇, 李涓子, 等. 语义 Web 中的本体自动映射[J]. 计算机学报, 2006, 29(11):1956-1976.
TANG J, LIANG B Y, LI J Z, *et al*. Automatic ontology mapping in semantic Web[J]. Chinese Journal of Computer, 2006, 29(11): 1956-1976.

[9] 宋利康, 崔德刚, 周儒荣. 企业模型与 ERP 系统间映射技术[J]. 航空学报, 2007, 28(6):1513-1520.
SONG L K, CUI D G, ZHOU R R. Mapping technology between enterprise model and ERP system[J]. Acta Aeronauticaet Astronau Tica Sinica, 2007, 28(6):1513-1520.

[10] 鲍翊平,张维明,姚莉. 一种基于本体映射处理推荐信任信息的模型[J].计算机科学, 2009, 36(6):185-187,195.
BAO Y P, ZHANG W M,YAO L. Model for processing recommendatory trust information based on ontology mapping[J]. Computer Science, 2009, 36(6):185-187, 195.

[11] 万明, 刘颖, 张宏科. 位置与身份分离协议下一种基于信任度模型的新型映射机制[J]. 通信学报, 2011, 32(7):133-145.
WAN M, LIU Y, ZHANG H K. New mapping approach based on reputation model under locator/ID separation protocol[J]. Journal on Communications, 2011, 32(7):133-145.

[12] 卿苏德, 廖建新, 朱晓民, 等. 网络虚拟化环境中虚拟网络的嵌套映射算法[J]. 软件学报, 2012,23(11):3045-3058.
QING S D, LIAO J X, ZHU X M, *et al*. Virtual network embedding algorithms in the network virtualization environment[J]. Journal of Software, 2012, 23(11):3045-3058.

[13] BERGER J O. Statistical Decision Theory and Bayesian Analysis[M]. Springer Science & Business Media, 2013.


## 作者简介：


**赵斌**（1979-），男，山东滕州人，北京工业大学博士生，济宁学院副教授，主要研究方向为网络安全、信息取证、云计算。

**何泾沙**（1961-），男，美籍华人，北京工业大学教授、博士生导师，主要研究方向为网络安全、测试与分析和云计算。