基于风险的 UCON 访问控制模型研究

高磊

（北京邮电大学网络与交换技术国家重点实验室，北京 100876）

摘要：使用控制（UCON）模型具有属性的可变性和可以连续授权的特点，它的出现弥补了传统的访问控制模型的缺点。UCON 是基于属性做出的决策，属性值可能在访问的过程中发生变化。然而，一些属性（例如主体的位置）可能是远程的，它们是由引用监视机的管理域之外的属性供应商管理。一些属性的变化可能会丢失或者延误。由于不能获得属性的最新值或者可信的值，决策结果可能会有一些错误发生，引用监控机可能错误地授予访问恶意用户，而禁止符合条件的用户访问。此外，现代的系统变得更加动态和分布式。我们的研究重点关注风险分析，使得 UCON 的访问决策更加可信和准确。我们提出应该使用贝叶斯网络为每个属性进行建模，然后进行风险分析。在本文中，我们提出了一个基于风险的 UCON 授权体系架构。

关键词：使用控制；风险；贝叶斯网络；可变属性

中图分类号：TP393.08

The Research of Risk Based on UCON

GAO Lei

(State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876)

Abstract: Usage control (UCON) model is emerged to cover some drawbacks of traditional access control models with features like attribute mutability and continuity of control. UCON is based on the idea that attributes required for decision-making can be changed over a period of usage. Some attributes (e.g., location of a subject) are remote, they are managed by attribute providers located outside the administrative domain of the reference monitor. Some attribute changes might be missed, corrupted, and delayed. Since it is not always possible to get a fresh and trustworthy value of attributes, a decision has to be done with some uncertainties in mind. As a result, the reference monitor may erroneously grant the access to malicious users and forbid it for eligible users. Moreover, modern systems become more distributed and dynamic. Our study concerns analysis of risks to make access decision of usage control more credible. To evaluate these risks we create a Bayesian network for modeling changes of attribute values for each attribute. In this paper we propose an architecture for the UCON system integrated with risk service.

Key words: UCON; Risk; Bayesian Network; Mutable Attribute

0 引言

访问控制的目的在于确保只有合法的用户才能访问资源。传统的访问控制模型，例如自主访问控制模型（DAC），强制访问控制模型（MAC）或是基于角色的访问控制模型（RBAC），都是在主体访问客体之间检查主体是否有足够的权限[1]。但是由于现在的网络是高度分布式和动态的，传统的访问控制受到的挑战越来越多。

为此，R. Sandhu 等人提出了 UCON 控制模型[2]，因为它拥有属性的可变性以及可连续授权的特点，被称作是下一代的访问控制模型。UCON 有以下核心组件：授权规则，条件和义务。决策是基于访问主体和客体的属性以及当前的执行环境做出的。

作者简介：高磊（1991-），男，硕士研究生，主要研究方向：服务计算与云计算，访问控制. E-mail: peakmuma@163.com

在 UCON 中获取到最新的属性值是一个关键的问题，但一些属性只能从远程的客户端获取到，并不在服务端的控制下，例如用户的位置信息。因此服务端获取属性值就会有一定的延时。有的时候，为了节省属性提供者（例如传感器）的资源（带宽，电量），属性值只能被周期性的发送给服务端。在这种情况下，部分属性值可能就被丢掉了。这样就有可能造成违背访问控制策略但是仍然能继续访问资源的情况发生，有时会给服务提供商造成很大的损失。因此 L. Krautsevich 等人提出了基于风险的 UCON[3]，在访问控制的过程中加入风险评估，并且对部分属性进行了马尔科夫建模。本文提出应该使用贝叶斯网络而不是马尔科夫链对属性进行建模，并给出了一个基于风险的 UCON 授权体系架构。

1 使用控制介绍

UCON，下一代访问控制模型的使用控制(usage control，简称 UCON)模型，也称其为 ABC 模型)。包含 3 个基本元素:主体(subject)、客体(object)、权限(right)和另外 3 个与授权有关的元素:授权规则(authorization rule)、条件(condition)、义务(obligation)。UCON 模型将义务、条件和授权作为使用决策进程的一部分，提供了一种更好的决策能力。授权是基于主体、客体的属性以及所请求的权利进行的，每一个访问都有有限的期限，在访问之前往往需要授权，而且在访问的过程中也可能需要授权[4]。

UCON 模型的两个显著特征是:决策的持续(Continuity)和属性的可变性(Mutability)[5]。可变属性(Mutable Attribute)的引入是 UCON 模型与其他访问控制模型的最大差别，可变属性会随着访问对象的结果而改变，而不可变属性仅能通过管理行为改变。

在主体对客体实施访问之前或实施访问操作的过程中，需要连续或重复性地检查主体是否具有继续访问的权力，从而决定是否继续访问操作，这称为使用决策的连续性；权利的使用过程中，主客体属性随时会随着环境信息被改变，因此需要及时进行更新属性的操作，这称为属性的易变性。

属性更新的方式可以是事前更新(preUpdate)，即在主体访问客体前，可以是事中更新(onUpdate)，即在主体访问客体的过程中，还可以是事后更新(postUpdate)，即在主体结束对客体的访问以后[6]。

2 访问控制中风险控制

2.1 风险的存在

UCON 中策略的执行依赖于正确可靠的属性值，而在实际应用中，如果一个属性值只能由一个远程的客户端来提供，那么属性值往往不能被及时的获取到或者只能被获取到一部分。随着网络的日益动态化和分布式化，要及时的获取到正确的属性值，将是一件很困难的事。可能由于部分资源（如带宽，能源等）的问题，造成属性的新值不能被及时得到，也有可能在网络中始终存在的一些恶意的用户，篡改信息或者利用系统的漏洞获取利益。这些人为的或者非人为的原因，都可能造成违反策略的行为执行。并且，如果授权一个违反策略的访问的话可能会引发恶果。

2.2 使用中更新的风险分析

文献[3]中提出了一类方法，从属性的更新信息的可信度的角度出发，认为当收到属性更新后的值时，认为这个新值是存在风险的，将风险分析的概念引入授权管理中来确定信息的可信度。文献[3]提出一种方法来对属性进行风险评估，具体方法如下

1) 对每一个属性值都创建一个马尔科夫链，来对属性值的变化进行模拟
2) 计算依赖于这个属性值做出决定的策略在特定时间点失败的可能性
3) 比较通过或者不通过该策略的代价
4) 应用一个方法来减少损失

对于一个正在访问的会话，决策结果有两种可能：继续或是取消此次会话，决策的结果依赖于决策模块接收到的属性值。有四种可能的情况：

- 会话应该继续访问，决策结果为继续访问
- 会话应该被取消，决策结果为继续访问
- 会话应该继续访问，决策结果为取消
- 会话应该被取消，决策结果为取消

每种情况的收益或者代价可以由文献[3]中的公式可以计算出，如表 1 所示：

表 1 决策代价

Tab.1 Decision matrix with costs

	满足策略 $(1-P)$	违背策略 (P)
继续访问	C^{CS}	$-C^{CF}$
取消访问	$-C^{RS}$	C^{RF}

其中 P 为当前属性违背策略的概率，C 为每种情况的收益或代价。

当满足不等式(1)，那么此次会话将会继续下去。

$$(1-P)*C^{CS}-P*C^{CF}>P*C^{RF}-(1-P)*C^{RS} \quad (1)$$

2.3 基于贝叶斯网络的属性模型

文献[3]中使用马尔科夫链对属性值进行建模。马尔科夫链描述了一种状态序列，其每个状态值取决于前面有限个状态。这种模型，对很多问题来讲是一种很粗略的简化。在现实的网络环境中，属性值的变化往往不能用一条链串起来，他们之间的转移可能是交叉的、错综复杂的。因此应当使用贝叶斯网络来对属性值进行建模。

从数学的层面讲，贝叶斯网络是一个加权的有向图，是马尔科夫链的扩展。而从认知论的层面看：贝叶斯网络克服了马尔科夫链那些机械的线性的约束，它可以把任何有关联的状态统一到它的框架下面。我们在计算贝叶斯网络中每个状态的取值时，只考虑了前面一个状态，这一点和马尔科夫链相同。但是，贝叶斯网络的拓扑结构比马尔科夫链灵活，它不受马尔科夫链的链状结构的约束，因此可以更准确的描述属性状态值之间的相关性。可以讲，马尔科夫链是贝叶斯网络的特例，而贝叶斯网络是马尔科夫链的推广。

2.4 贝叶斯网络的训练

使用贝叶斯网络必须先确定这个网络的拓扑结构，然后还要知道各个状态之间转移的概率参数。得到拓扑结构和这些概率参数的过程分别叫做结构训练和参数训练，统称训练。和训练马尔科夫模型一样，训练贝叶斯网络要用一些已知的数据。相比马尔科夫链，贝叶斯网络的训练比较复杂，从理论上讲，它是一个 NP 完备问题（NP-Complete），也就是说，对于现在的计算机是不可计算的。但是，对于某些引用，这个训练过程可以简化，并在计算机上实现。

训练结构模型，从理论上讲，需要完备的搜索，才能得到最优解。但是这样的计算复杂度是 NP，因此一般采用贪婪的算法。当然这样会导致陷入局部最优，并且最终远离全局最

优解。一个防止显然具备最优的方法，就是采用蒙特卡洛的方法，用许多随机数在贝叶斯网络中试一试，看看是否显然局部最优。

2.5 两种建模方法的对比

如果一个属性有 7 个状态，采用马尔科夫链对属性进行建模，其状态转移矩阵如下：

$$\begin{pmatrix} 0.4 & 0.6 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 \\ 0.2 & 0.5 & 0.3 & 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.1 & 0.7 & 0.2 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.2 & 0.2 & 0.6 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.3 & 0.6 & 0.1 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.3 & 0.2 & 0.5 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.0 & 0.9 & 0.1 \end{pmatrix}$$

矩阵的第 i 行第 j 列的数值表示该属性在第 i 个状态下转移到第 j 个状态的概率。用这种方法进行建模的话，状态之间的变化就受到了限制，只能在前一个状态，当前状态以及后一个状态进行转换。

采用贝叶斯网络对属性进行建模，其状态转移矩阵如下：

$$\begin{pmatrix} 0.3 & 0.6 & 0.0 & 0.0 & 0.1 & 0.0 & 0.0 \\ 0.1 & 0.2 & 0.3 & 0.4 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.3 & 0.1 & 0.1 & 0.3 & 0.2 & 0.0 \\ 0.0 & 0.4 & 0.0 & 0.3 & 0.3 & 0.0 & 0.0 \\ 0.1 & 0.2 & 0.1 & 0.3 & 0.1 & 0.2 & 0.0 \\ 0.3 & 0.1 & 0.0 & 0.1 & 0.3 & 0.2 & 0.0 \\ 0.2 & 0.0 & 0.4 & 0.1 & 0.0 & 0.0 & 0.3 \end{pmatrix}$$

属性在一个状态可以向任意的另一个状态进行转移，这种建模方法更加符合实际情况。

3 基于 R-UCON 的授权体系结构

3.1 R-UCON 架构模型

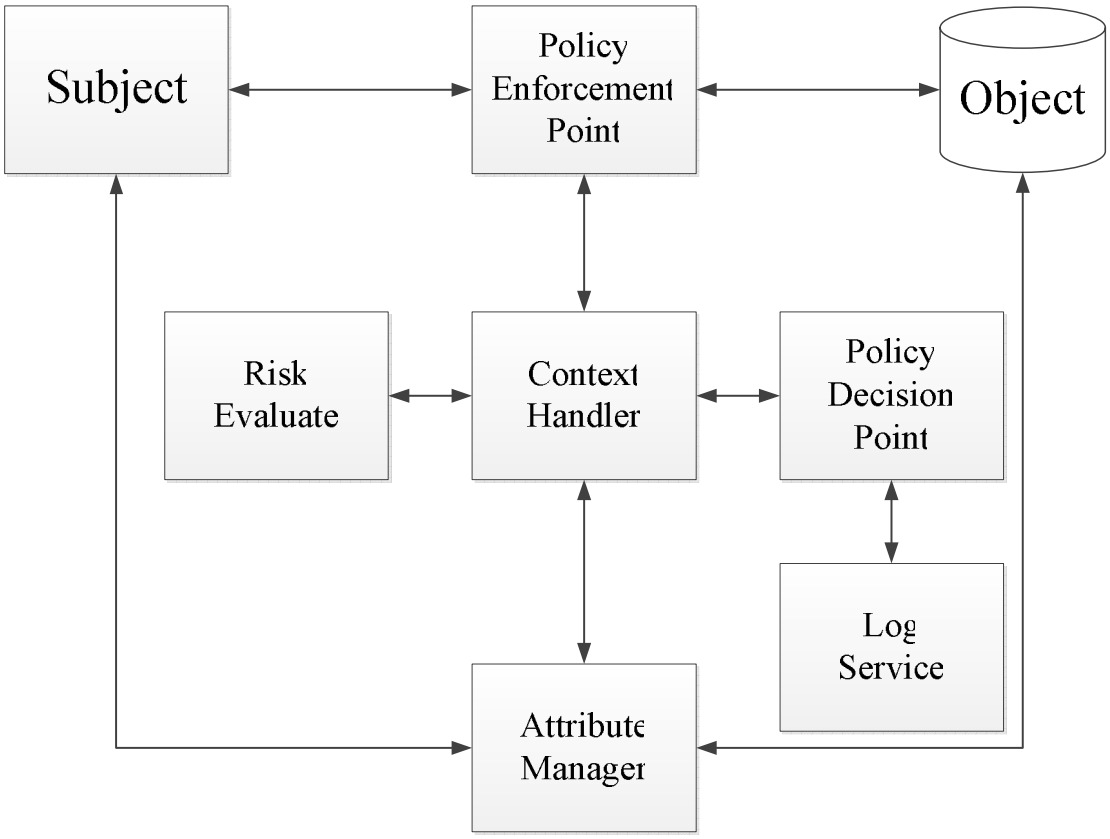

图 1 R-UCON 架构图

Fig. 1 The Architecture Of R-UCON

图 1 展示了 R-UCON 的架构，加入了风险控制模块。类似于大多数的授权系统，其主要组件是：

- PEP(Policy Enforcement Point)，这个模块的作用是接收主体发出的访问请求并将访问请求发给 PDP 模块，也可以配置和执行决策。任何的访问客体的请求，都会通过这个模块。这个模块的其他职责会在其他模块里面说明。
- CH(Context Handler)，这个模块用于存储和转发不同模块之间的通信消息，从工程实现的角度考虑，用于解除不同模块之间的耦合。
- PDP(Policy Decision Point)，这个模块的任务是计算策略并且返回授权结果。此模块是整个体系结构的核心部分，计算每个来自 PEP 的请求，在决策的过程中，PDP 会与 AM 交换数据，拿到主体和客体和环境的属性。如果策略通过，还会进行风险评估，最后将决策结果返回给 PEP。
- AM(Attribute Manager)，从主体，客体和环境中读取属性。由于 UCON 模型要不断的进行决策，因此必须周期性的从主体，客体或者环境中读取属性值，或是接受从主体或者客体推送来的属性值。
- RE(Risk Evaluate)，在决策过程中进行风险的评估，用来判断根据某个属性做出的决策是否有风险。
- LS(Log Service)，用来记录所有 PDP 做出的决策以及当时各个属性的属性值，便于

以后的分析统计。

3.2 授权流程

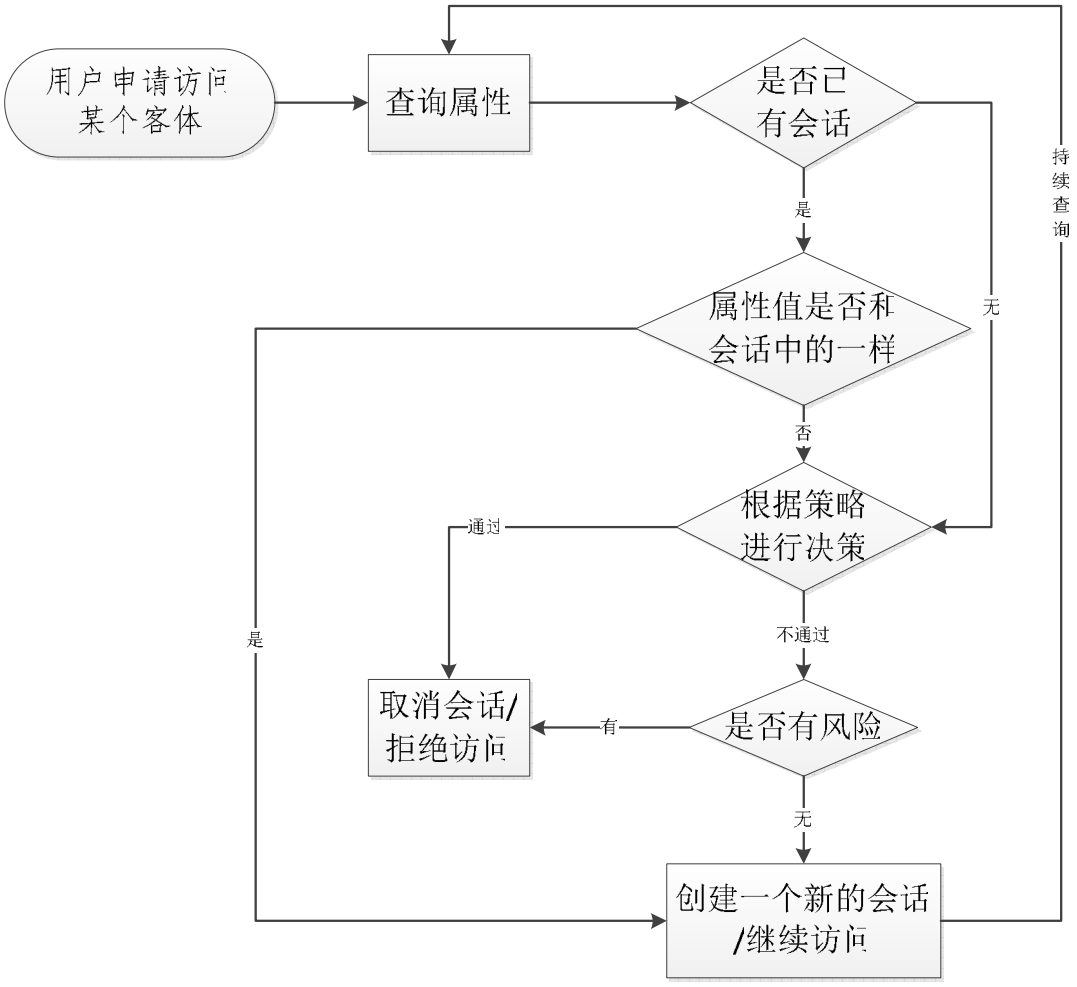

图 2 授权流程

Fig.2 The Flowchart Of Authorization

用户发出访问请求，PEP 接收到访问请求，并发送给 CH。然后 CH 向 AM 请求可能用到的属性，然后 CH 把访问请求以及收集到的属性值发送给 PDP。PDP 计算出是否违背策略，然后调用 RE 模块，进行风险评估，并把结果返回给 CH。

假设 PDP 允许了这次请求的执行，CH 把决策结果返回给 PEP，在返回之前，如果当前无访问会话，PEP 会让 SM 创建一个新的会话。

在整个会话访问期间，AM 每隔一段时间会从主体或者客体读取属性，PDP 模块也会重新进行决策，同时 PDP 会向 RE 发出请求，重新计算是否有风险，如果有风险，就关闭这次会话，并且结束访问，如果无风险，那就更新属性值，等待下一次决策。

4 结论

作为新一代的访问控制技术，使用控制中决策的持续性和属性可变的特性使其能够较好的适应高度动态的网络，但是在此环境下，因为属性值的不确定性，基于可变属性做出的决策往往有一定的风险。本文提出了使用贝叶斯网络对属性进行建模，贝叶斯网络是一个加权的有向图，是马尔科夫链的扩展，克服了马尔科夫链机械的线性的约束，可以更准确的描述

属性状态值之间的相关性。本文还给出了一个基于风险的授权体系框架，分析了框架中每个组件的作用，最后介绍了该框架的授权流程。

[参考文献] (References)

[1] Crampton J, Loizou G, O'Shea GA logic of access control[J]. The Computer Journal, 2001, 44(2): 137-149.
[2] Park J, Sandhu R. The UCON ABC usage control model[J]. ACM Transactions on Information and System Security (TISSEC), 2004, 7(1): 128-174.
[3] Krautsevich L, Lazouski A, Martinelli F, et al. Risk-aware usage decision making in highly dynamic systems[A]. Krautsevich L. Internet Monitoring and Protection (ICIMP), 2010 Fifth International Conference on[C]. Washington: IEEE, 2010. 29-34.
[4] 姚冬梅. 基于 UCON 的云计算访问控制模型研究[D]. 南京：南京大学，2012.
[5] 白赫. 基于 UCON 改进模型的授权管理体系研究[D]. 大连：大连理工大学，2010.
[6] 朱君礼. 基于 UCON 的云计算访问控制的研究与应用[D]. 北京：北京邮电大学,2012.