一种基于行为证明的主观动态可信模型建立方法

施光源 张建标
(北京工业大学计算机学院 北京 100124)

摘 要 在分布式环境中如何在实体之间建立信任关系一直是信息安全领域研究的热点问题,远程证明为解决该问题提供了一种新的研究方向。远程证明是可信计算中非常重要的特性,利用可信远程证明方法能够在实体之间建立起信任关系。但是,二进制等静态远程证明方法对于计算平台的可信性证明存在明显不足,在建立信任关系时不能够提供充分的证据。主要研究基于行为证明方法在实体之间如何建立可信关系的问题。因此,利用基于行为的远程证明方法对计算机平台可信性进行证明,该方法能够为建立信任关系提供更加准确的经验结果。在证明过程中存在一些不确定因素,这些不确定因素将影响信任关系的建立以及评估。利用主观逻辑对信任关系进行了度量,建立了TMBA动态可信模型,该模型能够在基于行为证明所获得的经验的基础上,通过考虑过去经验以及现有经验分析信任关系的动态性,并且将信任关系中的信任度用主观逻辑的观点来表示。最后给出根据TMBA对信任观点进行计算的方法。

关键词 可信计算,远程证明,信任关系,可信模型
中图法分类号 TP393 **文献标识码** A

Modeling the Subjective Dynamic Trust with Behavior-based Attestation

SHI Guang-yuan ZHANG Jian-biao
(Collage of Computer and Science, Beijing University of Technology, Beijing 100124, China)

Abstract In a distributed computing environment how to establish a trust relationship between entities has been a hot issues for information security, and remote attestation provides a new research direction for solving the issues. Remote attestation is an important feature of trusted computing, and entities can establish trust relationship by using the remote attestation. However, some static remote attestation methods such as binary based attestation are obviously inadequate to attest the trustworthiness of computing platform. They don't provide sufficient evidence in establishing trust relationship. Therefore, this paper used behavior-based attestation method to prove the trustworthiness of computing platform. This method can provide more accurate empirical results for establishing trust relationship. In additional, there are some uncertainties in behavior-based attestation, and these uncertainties will affect the establishment and evaluation of trust relationship. This paper used subjective logic to measure the trust relationship and build the dynamic trust model TMBA. This model can analyse dynamics of trust relationship by considering the past and present empirical results which are collected from behavior-based attestation, and represent the trust degree with the trust point in subjective logic. Finally, the method for calculation of the trust point was given.

Keywords Trusted computing, Remote attestation, Trust relationship, Trust model

1 介绍

远程证明(Remote Attestation)[1]在可信计算中作为一个重要的特性首先被引入,最开始的远程证明技术用来证明远程平台配置具备可信性。一个可信平台设备通过报告它的完整性状态,例如TPM芯片中的PCR值,来证明它的状态。这个特性能够使一个质询方对远程平台的完整性状态具备某种信心。TCG的规范中介绍了一种分层完整性度量的机制,即从硬件到应用程序分别进行度量,并且利用TPM提供的基本证明功能向质询方认证远程平台。在一个典型的证明场景中,包括一个证明的请求方和一个证明方,证明方通过提供证据信息来向请求方表明其具备请求方所期望的属性。根据可信计算所提供的基本证明服务已经有多种远程证明机制被提出。然而,对于远程证明的研究仍然不够充分,而且很多的挑战需要被攻克。第一个挑战就是现有的远程证明方法与TCG的所要求的目标之间还有很大的差距。在TCG的规范[1]中,可信被定义为"the expectation that a device will behave in a particular manner for a specific purpose"。其中,"expectation"表示一种预期,"behave in a particular manner"是指行为按照某种特定的方式进行,而"specific purpose"指

到稿日期:2011-04-26 返修日期:2011-08-28 本文受国家高技术研究与发展计划(863计划)(2009AA012437),国家重点基础研究发展计划(973计划)(2007CB311100),中国博士后科学基金(20100480173)资助。
施光源 博士生,主要研究方向为可信计算、信息安全;张建标 教授,主要研究方向为可信计算、信息安全。

具体的任务或者目标，换句话说，为了能够证明远程平台或者程序是可信的，远程平台需要证明这些目标行为可预期。如果主体在完成具体的任务时是以可预期的特定的行为方式进行，那么就认为它是可信的。TCG 用实体行为的预期性来定义可信，这一定义的优点是抓住了实体的行为特征，符合哲学上实践是检验真理的唯一标准的基本原则。然而，现有的远程证明方法大多数只是检验远程平台或者程序的配置或者完整性状态。这些方法不能够满足 TCG 关于可信的定义。第二个问题是大多数现有的证明机制没有特别考虑如何有效且高效地证明在一个动态的环境中正在运行的程序。Haldar 等提出了语义远程证明的概念[9]。李小勇等提出了基于行为证明的概念[7,8]。这些方法开始朝着验证远程平台行为的方向开展研究。但是，这些方法仍然处于初级水平。Haldar 没有说明如何实际地验证软件系统的行为。李小勇只是处理了静态策略，并且仅仅验证了系统行为记录。由此可见，现有的证明方法还无法满足 TCG 所给出的可信定义。首先，大多数证明方法只关注平台配置或者平台状态完整性等证明信息，这些证明信息与可信性所要求的内容不符，而且这些证明信息没有反映出所需要的动态信息。另外，现有证明方法对于程序在运行时的可信性研究不够充分，导致这种情况出现的原因是运行态程序状态变化多，行为不容易获取等，对其证明是一项比较有挑战的工作。对运行态的程序可信性进行研究是十分必要的。首先，针对于平台配置信息或者完整性进行证明的方法存在 time-of-check 到 time-of-use 的漏洞，容易造成检验状态与使用状态不一致的结果，最后导致证明结果不可信。其次，通过对运行态程序进行度量，能够对程序的行为进行分析，利用行为作为证明信息更加符合可信性的证明的要求。由于基于行为的证明方法既能够从动态性方面对可信性判定提供支持，同时，也更符合关于可信性的定义，在认识到软件的动态行为可以作为可信性判定的重要标准后，研究者将更多关注基于行为的可信证明研究工作。

本文主要研究基于行为证明方法在实体之间如何建立可信关系的问题。在给出了基于行为证明方法的同时，也会引入一些模糊不清的概念，比如对于可信性以及与可信性相关的行为的定义需要明确，这些模糊的概念不利于对证明方法进行分析，更阻碍了进行深层次的理论研究。另外，对于如何利用基于行为证明的方法进行可信性评估，如何考虑不确定性都需要采用一种更加合理有效的方法进行分析阐述。我们提出了基于行为证明的可信模型(Trust Model based on Behavior Attestation, TMBA)，TMBA 模型的建立旨在减少在行为证明中的模糊概念。另外，该模型中考虑了不确定性因素，这有助于更好地度量与推理实体间的信任关系。本文第 2 节对现有主要证明方法进行分析研究，介绍了现有的主要远程证明技术的研究内容；另外，给出了主观逻辑中观点以及观点映射的内容，这些内容将用于我们建立的 TMBA 模型；第 3 节建立 TMBA 模型，并且对模型中所使用的变量进行了详细定义；第 4 节给出根据 TMBA 模型对实体间的信任关系进行度量和推理的方法；最后对全文工作作出总结说明。

2 相关工作

2.1 证明相关工作

随着可信计算技术的迅速发展，可信证明技术也不断进步，从早期的 TCG 所提出的远程证明(Remote Attestation)[1]的概念开始，对于可信证明的研究就成为了可信计算领域中的研究热点。TCG 的证明方法[1]中将系统启动时所进行度量的度量值和相关日志作为可信证据提交给证明方。但是，TCG 所提供的证据主要是它在进行可信启动时所度量的信息，这种度量只进行到了 bootstrap loader，并且这些证据中包含了很多证明方的内部信息，例如平台的配置信息(软/硬件的版本，操纵系统类型等)，这就造成了目标平台信息的泄露，攻击方可以利用这些信息发动破坏攻击。Sailer 等人[2]发展了 TCG 的方法，提出了一种完整性度量架构 IMA (Integrity Measurement Architecture)。IMA 作为对于 TCG 证明机制的一种实现，将度量范围扩展到操作系统以及应用层，并且它能够在可执行程序加载时对其进行完整性度量，向远端证明完整性。但是该方法缺乏验证程序执行情况的能力，对于运行过程中程序的行为不能够进行度量。上述证明方法中都存在对于平台隐私泄露的问题，并且由于系统平台更新等问题使得完整性发生改变，从而引起更新升级不便的问题。为了解决上述问题，Ahmad-Reza Sadeghi 等人对计算机安全属性展开研究[3-6]。基于安全属性的证明方式是采集系统的配置信息，然后对这些信息进行度量，把系统的配置信息映射为与系统安全相关的安全属性。质询方通过验证证明方是否具有这些安全属性来判断其是否可信。该方法主要是利用安全属性证书的方式进行验证，在一定程度上解决了隐私保护的问题，保护平台的配置信息不被泄露，并且通过安全证书的方法比较直观，容易理解，但是安全属性证书需要随着计算平台状态的变化而变化，例如更新证书，撤销证书等，对于证书的维护比较麻烦，并且证明的粒度比较粗，对于系统运行时的状态没有考虑。上述这些证明方法主要是对系统配置信息等静态内容进行验证，对于系统动态信息的验证研究不足，对由漏洞或者发生攻击所导致的系统可信状态的变化无法进行有效的验证。因此，李晓勇等人提出了基于系统行为的证明方法[7,8,20]，该方法对与平台状态可信相关的系统行为加以记录，并检查这些系统行为的发生结果是否与安全策略预期冲突。V. Haldar 等人[9]通过对程序语义进行研究提出了基于语义的证明方法 SRA(Semantic Remote Attestation)，SRA 方法主要是对具体应用程序的语义进行度量，然后与安全策略进行比较来判断程序是否符合预期。该方法所提供的证据粒度更细，同时是在运行状态下的程序度量，具有一定的实时性，但是该方法是利用 Java 虚拟机进行程序分析的，因此使用范围具有一定的局限性。近年来，可信证明研究范围逐步从计算平台扩展到了应用软件，Lucas Davi 等[10]利用度量和证明方法来防范面向返回值的程序工具，利用污点跟踪和动态跟踪技术来发现 ROP 攻击，该文中描述了动态发现 ROP 的架构和方法，并且将传统 IMA 的完整性度量结果和动态度量结果一起作为远程证明的内容。Liang Gu 等在文献[11]中通过对目标平台及所有依赖对象进行度量，然后分析程序的执行是否正确，进而完成证明工作。

通过对现有证明方法进行分析后可以发现，单纯的静态证明方法对于复杂环境下的软件系统不再适用，它缺乏对于软件动态性可信证明的能力。而软件行为既能够从动态性方面对可信性判定提供支持，同时，也更符合关于可信性的定义，在认识到软件的动态行为可以作为可信性判定的重要标

准后，研究者将更多关注基于行为的可信证明研究工作。在可信证明中，证明质询方(Chagllenger，CH)需要证明方(Attester，AT)向其提供在对 AT 进行度量的过程中所获得的证据信息，CH 通过对证据信息进行分析来判断 AT 是否可信。由于 CH 与 AT 之间存在 time-of-check 到 time-of-use 的间隔，在度量后 AT 很可能由于更新等原因发生变化，这时的度量结果还能否作为证明的依据，CH 不能确定在多大程度上相信 AT 的证明报告，这就导致了证明过程中存在一定的不确定性，而且对于当前 AT 的行为进行证明可能是一种临时状态。为了使证明更具完备性，还需要考虑 AT 过去的行为。另外，CH 对证明结果信任的基础是相信对 AT 行为进行度量和验证的过程是可信的，这种信任存在一定的主观性，如果 CH 对这些操作过程不信任，那么 CH 对证明结果也将不信任，这些情况将使得对可信性的证明变得更加不确定。CH 能够在多大程度上相信 AT 具备可信性，大多数基于行为证明的研究工作大都集中在行为获取以及行为验证的机制方面，缺乏对基于行为证明的理论模型的研究，这将阻碍可信证明的研究。首先，重要概念模糊不清，特别是在可信证明过程中的可信性概念以及可信行为概念；其次，没有考虑可信证明过程中的不确定因素。针对这些问题，在进行可信性证明的过程中，应该考虑主观性和不确定性因素，因此，我们利用主观逻辑理论建立基于行为证明的可信模型，该模型提供了一种在引入主观性和不确定性的情况下，推理 CH 对 AT 具备可信性信任程度的方法。

2.2 主观逻辑

主观逻辑理论[12]是 Jøsang 在基于证据理论的基础上提出的。主观逻辑在对不确定性以及信任的度量和评估方面都建立了坚实的理论基础。主观逻辑中引入证据空间(Evidence Space)和观点空间(Opinion Space)来描述和度量信任关系。在主观逻辑中，观点(Opinion)表示对实体及其行为的主观信任程度，实体之间的信任通过观点表达。观点可以理解为将不确定的可能性作为辅助因素加以考虑的信任度量方法。主观逻辑中证据空间由一系列实体产生的可观测到的事件组成，实体所产生的事件分为肯定事件(Positive Event)、否定事件(Negative Event)以及不确定事件(Uncertain Event)，对这些事件的记录依靠对实体的观测和判断。在主观逻辑中，可信被表示为信任观点 $\omega=(b,d,u)$，b 表示信任，d 表示不信任，u 表示不确定，$b,d,u\in[0,1]$，且 $b+d+u=1$。用 pos,neg,unc 表示实体 A 对实体 B 关于 B 具备行为 x 的肯定经验数、否定经验数以及不确定经验数。A 相信 B 具备行为 x 的观点用 ${}^{A}\omega_x{}^{B}$ 表示。其中，${}^{A}b_x{}^{B}$ 表示 A 对 B 具备 x 的信任程度，${}^{A}d_x{}^{B}$ 表示 A 对 B 具备 x 的不信任程度，${}^{A}u_x{}^{B}$ 表示 A 对 B 具备 x 的不确定程度。证据映射函数为：

$${}^{A}\omega_x{}^{B}=({}^{A}b_x{}^{B},{}^{A}d_x{}^{B},{}^{A}u_x{}^{B})$$

其中，

$${}^{A}b_x{}^{B}={}^{A}pos_x{}^{B}/({}^{A}pos_x{}^{B}+{}^{A}neg_x{}^{B}+{}^{A}unc_x{}^{B})$$

$${}^{A}d_x{}^{B}={}^{A}neg_x{}^{B}/({}^{A}pos_x{}^{B}+{}^{A}neg_x{}^{B}+{}^{A}unc_x{}^{B})$$

$${}^{A}u_x{}^{B}={}^{A}unc_x{}^{B}/({}^{A}pos_x{}^{B}+{}^{A}neg_x{}^{B}+{}^{A}unc_x{}^{B})$$

为了能够对观点进行计算，主观逻辑中还引入了对于信任观点进行操作的算子，主要包括 *Conjunction*、*Consensus* 以及 *Discounting*。

Conjunction 操作：定义两个观点 ${}^{A}\omega_x{}^{B}$ 和 ${}^{A}\omega_y{}^{B}$，分别代表 A 相信 B 具备行为 x 和 y，${}^{A}\omega_{x,y}{}^{B}$ 表示观点 ${}^{A}\omega_x{}^{B}$ 和观点 ${}^{A}\omega_y{}^{B}$ 的合取操作，表示 A 相信 B 具备行为 x,y，计算方法如下：

$${}^{A}\omega_{x,y}{}^{B}={}^{A}\omega_x{}^{B}\times{}^{A}\omega_y{}^{B}$$

其中，

$${}^{A}b_{x,y}{}^{B}={}^{A}b_x{}^{B}\cdot{}^{A}b_y{}^{B}$$

$${}^{A}d_{x,y}{}^{B}={}^{A}d_x{}^{B}+{}^{A}d_y{}^{B}-{}^{A}d_x{}^{B}\cdot{}^{A}d_y{}^{B}$$

$${}^{A}u_{x,y}{}^{B}={}^{A}b_x{}^{B}\cdot{}^{A}u_y{}^{B}+{}^{A}u_x{}^{B}\cdot{}^{A}b_y{}^{B}+{}^{A}u_x{}^{B}\cdot{}^{A}u_y{}^{B}$$

Consensus 操作：如果 A 关于 B 具备行为 x 观点 ${}^{A}\omega_x{}^{B}$，C 也有对于 B 具备行为 x 的观点 ${}^{C}\omega_x{}^{B}$，那么通过 *Consensus* 操作能够得到 A 与 C 对于 B 具备行为 x 的观点 ${}^{A,C}\omega_x{}^{B}$，计算方法如下：

$${}^{A,C}\omega_x{}^{B}={}^{A}\omega_x{}^{B}\oplus{}^{C}\omega_x{}^{B}$$

其中，

$${}^{A,C}b_x{}^{B}=({}^{A}b_x{}^{B}\cdot{}^{C}u_x{}^{B}+{}^{C}b_x{}^{B}\cdot{}^{A}u_x{}^{B})/K$$

$${}^{A,C}d_x{}^{B}=({}^{A}d_x{}^{B}\cdot{}^{C}u_x{}^{B}+{}^{C}d_x{}^{B}\cdot{}^{A}u_x{}^{B})/K$$

$${}^{A,C}u_x{}^{B}=({}^{A}u_x{}^{B}\cdot{}^{C}u_x{}^{B})/K$$

其中，$K={}^{A}u_x{}^{B}+{}^{C}u_x{}^{B}-{}^{A}u_x{}^{B}\cdot{}^{C}u_x{}^{B}$。

Discounting 操作：如果 A 对 B 的观点为 ${}^{A}\omega^{B}=({}^{A}b^{B},{}^{A}d^{B},{}^{A}u^{B})$，$B$ 对行为 C 的观点为 ${}^{B}\omega^{C}=({}^{B}b^{C},{}^{B}d^{C},{}^{B}u^{C})$，那么 A 对于 C 的观点为 ${}^{A}\omega^{C}$ 根据 B 的观点以及 A 对 B 的观点计算得出。计算方法如下：

$${}^{A}\omega^{C}={}^{A}\omega^{B}\otimes{}^{B}\omega^{C}$$

其中，

$${}^{AB}b^{C}={}^{A}b^{B}\cdot{}^{B}\omega^{C}$$

$${}^{AB}d^{C}={}^{A}b^{B}\cdot{}^{B}d^{C}$$

$${}^{AB}u^{C}={}^{A}d^{B}+{}^{A}u^{B}+{}^{A}b^{B}\cdot{}^{B}u^{C}$$

3 基于行为证明的可信模型 TMBA

在建立可信模型之前，首先需要明确可信的定义。在信息安全领域对于可信定义的研究非常广泛[13,15-19]。我们从可信的行为定义出发，在文献[13]关于可信性描述的基础上，给出如下的可信定义。

定义 1 可信是一种心理状态，包括预期和信任。其中，预期是指 trustor 期望或者希望来自于 trustee 的某种特定行为；信任是指 trustor 依据 trustee 的能力和信誉相信所期望的行为会发生。用一阶逻辑表示为：

$$trust(TR,TE,x)\equiv madeby(x,TE)\supset believe(TR,x)$$

其中，TR 表示 trustor，TE 表示 trustee，x 表示 trustee 的行为，逻辑表达式的含义是 trustorTR 相信 trusteeTE 关于 trustee 的行为 x。该定义从实体行为的角度进行可信的定义，不但符合 TCG 中关于可信的定义，而且从行为角度定义可信也符合实践是检验真理标准的基本原则。根据定义 1 可以得出，可信是一种期望与信任的关系，如果 trustor 所期望的事件就是 trustor 具备行为 x 得到验证，那么 trustor 就认为 trustee 是可信的，这个简单的可信验证过程的描述也就是对可信证明的非形式化的描述。由此可见，可信证明过程中应该包括 3 个部分：实体—trustor 和 trustee，实体行为—trustee 的行为 x，以及对于实体行为的操作—度量、验证等操作。在定义 1 中将 trustor 是否相信 trustee 具备 trustor 所期望的 trustee 行为 x 作为可信的判断，因此需要对 trustee 是否具备所期望行为 x 进行度量，并且需要对度量结果进行验证。因此，下面将可信模型定义为一个三元组。

定义 2 可信模型 $TMBA=(EN,EB,OP)$，其中 EN 表示的实体集合；EB 表示实体的行为集合；OP 表示针对于实体可信性进行证明的操作集合。

3.1 TMBA 中的实体 EN

在可信模型 TMBA 中，将实体集合定义为 $EN=(CH,AT)$，其中，在 EN 中包括证明过程中的质询方(Chagllenger，CH)，CH 是对实体是否具备可信性提出质询的一方，也就是提出证明请求的一方。另外，EN 中还包括证明方(Attester，AT)，AT 是证明过程中需要被证明的一方。

3.2 TMBA 中的实体行为 EB

实体集合中的证明方是作为可信证明的主要对象，在证明方中包含了不同的组件 $C=\{c_1,c_2,\cdots,c_n\}$，组件 $c_i\in C$ 在完成既定任务时所进行的一系列与系统安全相关的操作认为是组件的行为，那么，实体行为由其所包含的所有组件的行为组成。

定义 3 实体行为 EB 是指实体中的组件 C 为了完成既定任务而在系统中所进行的可以观测的操作集合。“可观测”是指实体的行为能够被监控以及获取，在本文中所定义的可观测行为是以组件生成的外部可观测的事件形式表示的。

由于定义 1 可知，判断实体是否可信需要对实体的行为具备一定的预期，对于可信性的证明就是要验证实体的行为是否符合这种预期。根据定义 3 将行为分为两类，一类为实体的预期行为 Exb，一类为通过对实体的观测得到的实际行为 Enb。$M\in EN$ 表示一个证明方，C 表示组成 M 的不同组件的有限集合，$C=\{c_1,c_2,\cdots,c_n\}$，Exb 表示 C 应该具备的符合策略定义的期望行为的有限集合，$Exb=\{exb_1,exb_2,\cdots,exb_n\}$。$Enb$ 表示通过对 C 进行监控后所获得的实施行为的有限集合，$Enb=\{enb_1,enb_2,\cdots,enb_n\}$。因此，判定实体 M 是否具备可信性的定义描述如下。

定义 4 实体 M 可信是指 M 存在行为集合 $EB=(Exb,Enb)$，当实体 M 中任意组件 c_i 的实际行为 $enb_i\in Enb$ 与其预期行为 $exb_i\in Exb$ 相符合，就认为实体 M 具备可信性。

基于行为证明的可信模型 TMBA 可以认为是对一种实体间的信任关系进行验证，具体来说，这种信任关系是 CH 相信 AT 具备可信性。下面定义可信关系。

定义 5 实体间的可信关系定义为 TR，其中 $TR=(A,B,C,Y,T,F,pos,neg,unc)$，其中各变量定义如下。

一个实体 A 相信实体 B 的组件 C 在一个给定的时间 T 具备可信性 Y，根据给定的经验 pos，neg，unc，以及根据 F 计算得到的观点，实体 A 和实体 B 属于 EN；C 属于一个有限集合 C，C 是实体 B 的所有的组件。T 是获取可信关系 TR 中经验 pos，neg，unc 的时间。F 是证据映射操作，将证据映射为观点。pos，neg，unc 分别代表与可信关系相关的肯定经验、否定经验以及不确定经验的总数。

3.3 实体行为操作管理 OP

在可信证明以及信任管理的过程中，主要包括证据收集、信任观点评估、信任观点比较 3 个操作过程。通过可信证明中对于可信证据的操作来建立信任关系 TR，再利用信任管理对 TR 进行评估和比较。

证据收集是 CH 通过对 AT 进行可信证明后记录 AT 的证明结果的过程。在 TMBA 模型中，证据收集过程包括对 AT 行为进行度量和验证的过程，并且对证明结果进行分析统计，将其作为主观逻辑中使用的经验用于评估分析可信观点。下面给出证据收集操作相关定义。

定义 6 行为度量 Behavior Measurement(BM)是对实体 B 的组件 C 进行观测，进而得到实际行为 $Enb=(enb_1,enb_2,\cdots,enb_n)$，$BM:C\leftarrow Enb$，其中←表示对 C 度量后将 Enb 与 C 关联。

定义 7 行为验证 Behavior Verification(BV)是实体 B 中组件 C 的实际行为 Enb 与期望行为 $Exb=(exb_1,exb_2,\cdots,exb_n)$ 进行比较，形式化表示为：

$$Enb\otimes Exb=\{enb_1\otimes exb_1,enb_2\otimes exb_2,\cdots,enb_n\otimes exb_n\}$$

式中，⊗表示两种行为的比较关系。

BV 是一个偏函数，它将实际行为与预期行为的比较 $(Enb\otimes Exb)$ 映射为一个布尔值，若实际行为与预期行为相符合，则结果为 true，否则为 false。我们形式化表示验证过程为：

$$BV:Enb\otimes Exb\rightarrow\{\text{true}|\text{false}\}。$$

另外，比较关系⊗可以认为是一种行为的验证过程，举例说明，如果一个组件 c 发生访问某个机密文件 f(例如，该文件包含密钥)的行为 Enb，那么就会触发这种验证发生，将实际行为 Enb 与策略定义的期望行为 Exb 进行比较，这种期望行为 Exb 是由安全策略所定义的，假如策略定义的期望行为 Exb 是组件 c 没有访问 access 文件 f 的权限，这时 Enb 与 Exb 不符，那么就将比较的结果记录为 $false$。关于行为的验证不是本文的重点，由于篇幅有限不再详述。

在对证明方进行可信证明时，主要是验证证明方中组件行为是否符合策略定义的预期行为。我们利用安全策略来定义实体的预期行为，系统的安全策略是管理系统中主体/客体的规则集合，它规定了主体的行为，比如安全策略规定了何种主体能够访问何种客体，很多系统中都采用 MAC 机制[14]来对主体的实际行为进行监控，并且与策略定义的预期行为进行比较。我们利用证明方的状态变化来描述可信性是否破坏。由于证明方的状态变化是由各种与安全相关的行为导致的，因此证明方的状态直接与行为相关。假设证明方开始处于可信状态，如果在运行过程中所有行为都符合预期，那么这种状态就没有被破坏，如果发生了行为不符合预期行为，那么证明方就处于不可信状态，从而记录为不可信事件[7]。我们假设证明方的状态只与其所运行的操作系统状态有关，并且所有的行为都发生在软件系统中，没有发生破坏硬件的恶意行为。

定义 8 证明方的状态集合 $Z=(\Sigma,R,M,F)$，其中，$\Sigma\subseteq S\times O\times A$ 为当前的主体对于客体的访问控制权限集合，$S=\{s_1,s_2,\cdots,s_n\}$ 表示系统中主体集合；$O=\{o_1,o_2,\cdots,o_n\}$ 表示系统中客体集合；$A=\{r,w,e\}$ 表示访问属性集合，$r\rightarrow read\text{-}only$ 表示只读操作，$w\rightarrow write$ 表示写操作，$e\rightarrow execute$ 表示执行操作；$R=\{get,release,create,delete\}$ 为请求操作集合，get 表示获取访问权限，$release$ 表示释放访问权限，$create$ 创建主体/客体，$delete$ 表示删除主体/客体；M 为 i 行 j 列的访问控制矩阵，$F=\{BM,BV\}$ 表示行为操作函数集合。证明主体状态 $z=(b,r,m,f)\subseteq Z=(\Sigma,R,M,F)$，其中，$b\subseteq\Sigma$，$r\subseteq R$，$m\subseteq M$，$m_{ij}\subseteq A$ 表示主体 s_i 对客体 o_j 有访问权限，$f\subseteq F$。

当有实体的行为发生时，会导致证明方的状态发生变化，到达一个新状态 z'，如果这些行为符合预期的可信行为，那么

状态 z' 保持可信状态；如果发生了与预期不相符的不可信行为，那么 z' 的可信状态将被破坏。下面对行为进行描述。

创建行为 *create*：当一个主体准备创建一个客体时，如果创建客者不在证明主体集合中，*create* 添加新的主体 s 和客体 o 到证明主体集合 S 和证明客体集合 O 中。新的证明主体集合和证明客体集合表示为 S' 和 O'。另外，主体 s 被加入到 M 中，并且修改 $M(E')$ 为新的访问控制矩阵，形式化表示为：

$$create(s,o,a)=(O',S',A,E')$$

$$\forall s\in S,\forall o\in O,\forall a\in A,S'=S\cup\{s\},O'=O\cup\{o\}$$

$$E'(o,a)=E(o,a)\cup\{s\}$$

获取行为 *get*：当主体准备获取对于客体的访问权限时，需要对证明主/客体集合进行更新。与 *create* 操作类似，形式化表示如下：

$$get(s,o,a)=(O',S',A,E')$$

删除行为 *delete*：当主/客体结束任务后将导致主体或者客体从证明主体或者证明客体集合中被移除，形式化表示如下：

$$delete(s,o,a)=(O',S',A,E')$$

$$S'=S\Theta\{s\}\overset{def}{=}\begin{cases}S, & |E^{-1}(\{s\})|\geqslant 2\\ S-\{s\}, & \text{otherwise}\end{cases}$$

$$O'=O\Theta\{o\}\overset{def}{=}\begin{cases}O, & \sum_{i=1}^{n}|E(o,a_i)|\geqslant 2\\ O-\{o\}, & \text{otherwise}\end{cases}$$

$$E'(o,a)=E(o,a)-\{s\}$$

为了获得最新的证明主体集合，主体从证明主体集合中被移除 $S\Theta\{s\}$。然而，当主体访问多个客体的时候，主体不能被移除，通过验证 E 进行转置。类似地，在移除客体之前，也需要验证客体是否被多个主体访问。另外，M 中通过移除 s 的 (o,a) 进行更新。

释放行为 *release*：与 *delete* 行为类似，*release* 有条件的从 M 中移除证明主体和证明客体。

$$release(s,o,r)=(O',S',R,A')$$

delete 是由证明主体或者动态客体任务结束后系统调用引起的，而 *release* 是由主体自己引起的。

在可信模型中，主体对于客体的访问操作能够引起信息流发生改变，需要按照安全策略的要求进行。请求操作行为对主体/客体进行添加和删除，会导致证明方的状态发生改变。同时，这种状态的改变会对证明主/客体集合产生影响。证明方的行为如果满足下面的条件，那么认为行为没有破坏证明方的可信状态。

$$create(s,o,a)\rightarrow o\in O'\wedge s\in S'\wedge s\in E'(o,a)$$

$$get(s,o,a)\rightarrow o\in O'\wedge s\in S'\wedge s\in E'(o,a)$$

$$revoke(s,o,a)\rightarrow S'=S\Theta\{s\}\wedge O'=O\Theta\{o\}\wedge E'(o,a)=E(o,a)-\{s\}$$

$$release(s,o,a)\rightarrow S'=S\Theta\{s\}\wedge O'=O\Theta\{o\}\wedge E'(o,a)=E(o,a)-\{s\}$$

根据上述定义的请求操作行为，如果所有上述的条件都满足，证明方请求操作行为是可信的，也就是说证明方的状态变化 $z\rightarrow z'$ 是可信的，可信状态没有发生变化。如果在证明过程中发现证明方存在破坏可信状态的不可信行为，那么就将这种行为作为一种经验记录下来，作为一种评估的依据。

不确定性问题：对于实体行为的度量过程 BM 与验证过程 BV 存在主观信任问题。CH 对于 AT 的信任是建立在对 BM 和 BV 信任的基础上，如果 CH 对 BM 和/或 BV 不信任，那 CH 对于 AT 的可信性也将产生质疑。由于存在很多不确定因素，因此导致 CH 对于 AT 的可信性判断也存在不确定性。在利用主观逻辑对信任关系进行度量和评估前，需要获取用于信任关系评估的证据，然后再将证据映射为主观逻辑中的信任观点。利用基于行为的证明方法来获取证据时，需要根据定义的期望行为与实际监控所得到的行为进行比较，如果符合定义 4 的要求，那么作为肯定事件经验记录，若发生破坏可信状态的行为则将作为一种否定事件经验记录。对 BM 和 BV 的信任、不信任以及不确定经验分别用 b,d,u 表示，其中，$b(BM)=1,d(BM)=1,u(BM)=1$ 分别表示对 BM 有关于信任、不信任以及不确定的经验，$b(BM)=0,d(BM)=0,u(BM)=0$ 分别表示对 BM 没有关于信任、不信任以及不确定的经验，对于 BV 的经验表示类似。CH 根据基于行为的证明方法来记录 AT 是否满足可信性的 pos，neg，unc 事件的经验结果，将这些经验结果作为主观逻辑中对于信任关系 TR 进行评估的证据。CH 在记录经验结果时包括如下情况。

当实体 AT 满足可信性所定义的标准时，(1) 如果 BM，BV 的经验不可用或者获取不到，那么记录 $pos(AT)$ 事件经验；(2) 如果 BM 和 BV 经验可用，那么无论 BM，BV 的经验结果如何，都没有影响 AT 的经验结果，证据收集时记录为 $pos(AT)$ 事件经验，相应增加对于 BM，BV 的信任事件经验 $pos(BM)$，$pos(BV)$；当实体 AT 不满足可信性时，(1) 如果 $b(BM)=1,b(BV)=1$，那么依据对于 BM，BV 过程信任的经验，能够分析出 AT 不具备可信性，因而将记录 AT 的否定经验 $neg(AT)$；(2) 如果 $b(BM)=1,d(BV)=1$，那么 CH 根据 $d(BV)=1$ 的经验推断发生 $neg(AT)$ 事件的原因可能是由于 AT 更新引起变化导致的，那么需要记录 $neg(AT)$，$neg(BV)$ 事件；(3) 如果 $b(BM)=1,u(BV)=1$，那么 CH 不能够确定导致 $neg(AT)$ 的事件是不是因为 BV，因此记录 $neg(AT)$，$unc(BV)$ 事件。类似地，当 $d(BM)=1$ 或者 $u(BM)=1$ 时，BV 在分别具备 3 种信任经验结果 $b(BV)=1,d(BV)=1$，以及 $u(BV)=1$ 的情况下，可以分别得到 neg，unc 事件经验。

CH 对于 AT 的信任不但要依据过去的事件经验结果，还需要根据当前经验做出决定。因为关于 AT 可信性的过去经验反映了 AT 的较稳定的长期状态，AT 根据当前经验判断为可信很可能是一种临时状态表现，更进一步，当前经验反映了 AT 此时此刻的状态，过去经验可以作为参考，可是过去经验代表过去发生的事件，当前经验反映了现在的实体状态，由此可见当前经验的权重要高于过去经验。但是，单凭临时状态判断 AT 是否可信在一定程度上不是十分充分，还需要结合 AT 的过去经验。因此，CH 在对 AT 进行信任推理时，还要结合当前经验以及过去经验来综合判断。

信任观点评估是将收集到的证据映射为观点的过程。在可信关系中 TR，A 对于 B 的组件 c_i 具备可信性 Y 的证据表示为 $\{{}^{A}pos^{B,tr(c_i,Y)},{}^{A}neg^{B,tr(c_i,Y)},{}^{A}unc^{B,tr(c_i,Y)}\}$，通过映射函数 M 将证据映射为在 $\Delta\in T$ 时刻的信任观点为：

$${}^{A}\omega_{\Delta}^{B,tr(c_i,Y)}=\{{}^{A}b_{\Delta}^{B,tr(c_i,Y)},{}^{A}neg_{\Delta}^{B,tr(c_i,Y)},{}^{A}unc_{\Delta}^{B,tr(c_i,Y)}\}$$

用 $\{{}^{A}pos^{BM,bm(c_i,Y)},{}^{A}neg^{BM,bm(c_i,Y)},{}^{A}unc^{BM,bm(c_i,Y)}\}$ 表示 A 对于 B 中的组件 c_i 具备可信性 Y 的行为度量 BM 的证据，利用观点映射函数 M 计算出 A 对于 BM 在 $\Delta\in T$ 时刻的信任

观点：

$$^{A}\omega_{\Delta}^{BM,bm(c_i,Y)}=\{^{A}b_{\Delta}^{BM,bm(c_i,Y)},{}^{A}neg_{\Delta}^{BM,bm(c_i,Y)},{}^{A}unc_{\Delta}^{BM,bm(c_i,Y)}\}$$

用$\{^{A}pos^{BV,bv(c_i,Y)},{}^{A}neg^{BV,bv(c_i,Y)},{}^{A}unc^{BV,bv(c_i,Y)}\}$表示 A 对于 B 中的组件 c_i 具备可信性 Y 的行为验证 BV 的证据，利用观点映射函数 M 计算出 A 对于 BV 在 $\Delta\in T$ 时刻的信任观点，即$^{A}\omega_{\Delta}^{BV,bv(c_i,Y)}=\{^{A}b_{\Delta}^{BV,bv(c_i,Y)},{}^{A}neg_{\Delta}^{BV,bv(c_i,Y)},{}^{A}unc_{\Delta}^{BV,bv(c_i,Y)}\}$。因此 A 对于实体 B 的组件 c_i 在时刻 Δ 具备可信性 Y 的观点表示为：

$$^{A}\omega_{\Delta}^{B,c_i,Y}={}^{A}\omega_{\Delta}^{B,tr(c_i,Y)}\times{}^{A}\omega_{\Delta}^{BM,bm(c_i,Y)}\times{}^{A}\omega_{\Delta}^{BV,bv(c_i,Y)}\tag{1}$$

通过实体的历史行为进行可信证明后获取的证据，其可信性会随着时间的流逝而不断衰减，这样就会引起信任观点产生衰退，这种信任随时间的衰退体现了可信的动态性特点。我们用 Π_{λ}^{k} 表示衰退操作函数，利用该函数来计算由 ω_{old} 随着时间的变化而得到的 ω_{new}，形式化表示为：

$$\omega_{new}=\Pi_{\lambda}^{k}[\omega_{old}]\tag{2}$$

$$b_{new}=b_{old}[e^{-(k,\lambda)}]$$

$$d_{new}=d_{old}[e^{-(k,\lambda)}]$$

$$u_{new}=u_{old}+[(b_{old}+d_{old})-(b_{new}+d_{new})]$$

式中，k 是衰减率，它用来调节衰减的快慢，$k\in(0,1]$。λ 表示请求服务的时刻 Δ 与最近信任观点更新的时间 Δ' 的差与固定时间的比值，$\Delta-\Delta'\geqslant 0$。这个固定值可以以一年 365 天为基数，也可以根据实际变化进行调整。如果 $\lambda=0$ 表示 ω_{new} 与 ω_{old} 相同，为了便于计算，我们假设 $\lambda=\Delta-\Delta'/365$ 的最大值为 2，即请求服务的时间与观点最后更新的时间间隔最大为两年。因此，在信任观点式(1)中引入表示可信动态性式(2)后得到动态信任观点计算式(3)：

$$^{A}\omega_{\Delta}^{B,c_i,Y}=\prod_{\lambda}^{k}[{}^{A}\omega_{\Delta}^{B,tr(c_i,Y)}]\times{}^{A}\prod_{\lambda}^{k}[{}^{A}\omega_{\Delta}^{BM,bm(c_i,Y)}]\times\prod_{\lambda}^{k}[{}^{A}\omega_{\Delta}^{BV,bv(c_i,Y)}]\tag{3}$$

(1)独立信任：实体 A 在对于实体 B 的组件 c_i 进行独立可信性评估时，不但要考虑当前时刻 Λ 的经验，同时也要考虑 A 对于 B 在时刻 $\Lambda-t$ 的过去经验，因此将 A 对 B 的独立信任观点$^{A_d}\omega^{B,c_i,Y}$表示为：

$$^{A\_d}\omega^{B,c_i,Y}={}^{A}\omega_{\Lambda}^{B,c_i,Y}\times{}^{A}\omega_{\Lambda-t}^{B,c_i,Y}\tag{4}$$

其中，

$$^{A}\omega_{\Lambda-t}^{B,c_i,Y}=\prod_{\lambda}^{k}[{}^{A}\omega_{\Lambda-t}^{B,tr(c_i,Y)}]\tag{5}$$

$$^{A}\omega_{\Lambda}^{B,c_i,Y}=\prod_{\lambda=0}^{k}[{}^{A}\omega_{\Lambda}^{B,tr(c_i,Y)}]\times\prod_{\lambda}^{k}[{}^{A}\omega_{\Lambda-t}^{BM,bm(c_i,Y)}]\times\prod_{\lambda}^{k}[{}^{A}\omega_{\Lambda-t}^{BV,bv(c_i,Y)}]\tag{6}$$

在式(4)中，实体 A 的信任观点由 Λ 时刻和 $\Lambda-t$ 时刻的观点通过 conjunction 操作计算得出。假设当前 Λ 时刻的观点为(1,0,0)时，那么实体 A 的独立观点将根据过去的经验$^{A}\omega_{\Lambda-t}^{B,c_i,Y}$计算；如果当过去的观点不可用时默认其具备(1,0,0)的信任观点，那么实体 A 的独立观点将只由当前时刻 Λ 的观点$^{A}\omega_{\Lambda}^{B,c_i,Y}$决定。式(5)是将时间 $\Lambda-t$ 带入式(3)后得出的结果，但是，由于在 $\Lambda-t$ 时，对于 BM，BV 的观点$^{A}\omega_{\Lambda-t}^{BM,bm(c_i,Y)}$，$^{A}\omega_{\Lambda-t}^{BV,bv(c_i,Y)}$是通过在 $\Lambda-t$ 时刻之前的经验结果计算得出的，由于时间比较久远，可能存在 BM，BV 过程改变或者方法更新等，使得这些经验结果失效，因此在式(5)中舍弃 BM，BV 的观点。在式(6)中，由于$^{A}\omega_{\Lambda}^{B,tr(c_i,Y)}$是在服务请求时刻 Λ 的观点，因此没有时间衰减 $\lambda=0$。对于 BM，BV 的信任观点是由过去的经验获取的，如果过去的经验不可用，那么默认它们的观点都是(1,0,0)，那么使得$^{A}\omega_{\Lambda}^{B,c_i,Y}=\prod_{\lambda=0}^{k}[{}^{A}\omega_{\Lambda}^{B,tr(c_i,Y)}]$

(2)推荐信任：除了实体 A 的独立信任外，根据那些对于实体 B 了解的其他实体，向实体 A 所推荐的观点计算出来 B 的推荐信任观点$^{A_r}\omega^{B,c_i,Y}$表示为：

$$^{A\_r}\omega^{B,c_i,Y}=(E_{R_1}\otimes\prod_{\lambda}^{k}[^{R_1}\omega_{\Lambda-t}^{B,tr(c_i,Y)}])\oplus\cdots\oplus(E_{R_n}\otimes\prod_{\lambda}^{k}[^{R_n}\omega_{\Lambda-t}^{B,tr(c_i,Y)}])\tag{7}$$

式中，推荐信任由不同的推荐者 $R=\{R_1,R_1,\cdots,R_n\}$ 对于实体 B 的信任观点$\prod_{\lambda}^{k}[^{R_m}\omega_{\Lambda-t}^{B,tr(c_i,Y)}]$通过 consensus 计算获得，表示不同的推荐者对于实体 B 的观点，并且为了体现实体 A 对于不同推荐者的信任程度，引入了重要性因子 $E_R=(w,1-w,0)$，其中 w 表示不同观点的权重。

(3)综合信任：综合信任是将实体 A 对于实体 B 的组件 c_i 的独立信任与推荐信任经过 consensus 计算所得出的信任观点$^{A_z}\omega^{B,c_i,Y}$，表示为：

$$^{A\_z}\omega^{B,c_i,Y}={}^{A\_d}\omega^{B,c_i,Y}\oplus{}^{A\_r}\omega^{B,c_i,Y}\tag{8}$$

式中，对于独立信任$^{A_d}\omega^{B,c_i,Y}$与推荐信任$^{A_r}\omega^{B,c_i,Y}$分别通过式(4)和式(7)计算得出。进一步，要计算这个实体 B 的信任观点，需要将 B 中所有需要进行证明的组件 C 的综合信任进行计算。

$$^{A\_z}\omega^{B,Y}=(E_{c1}\otimes\prod_{\lambda}^{k}[^{A\_z}\omega^{B,c_1Y}])\oplus\cdots\oplus(E_{cn}\otimes\Pi_{\lambda}^{k}[^{A\_z}\omega^{B,c_n,Y}])\tag{9}$$

式中，$c_i\in C$ 表示实体 B 中进行证明的组件，E_{ci} 表示 A 认为不同组件对于整个实体 B 可信性的重要程度，它与对应组件的综合信任观点进行 consensus 操作。

信任观点比较是将两个信任观点 ω_1 与 ω_2 进行对比，定义观点比较操作$\geqslant_{\omega}$，如果 $b_1>b_2$，$d_1<d_2$，并且 $u_1<u_2$ 或者 $u_1>u_2$，那么 $\omega_1\geqslant_{\omega}\omega_2$，即观点 ω_1 比设定的门限观点 ω_2 大。

4 可信性评估

通过 TMBA 模型能够对 CH 与 AT 之间的信任关系进行评估。首先需要在 AT 与 CH 之间建立信任关系，利用基于行为的证明方法对 AT 中组件的可信性进行证明，获取组件的实际行为，将这些行为与安全策略所定义的预期行为进行比较，最终将验证结果发送给 CH。CH 通过证明结果来判断 AT 的组件是否具备可信性。在 CH 与 AT 之间具备了这种信任关系后，还需要对这种关系进行评估。因为在整个证明过程中包括对组件的度量和验证过程，这些步骤都对信任关系产生了影响，使得信任关系变得不确定。CH 对于 AT 的独立信任观点可以利用式(4)进行计算，在计算独立信任观点时考虑了过去经验，因此，也需要引入时间衰减的因素。除了 CH 对于 AT 的独立信任外，如果存在对于 AT 的推荐信任时，在评估信任关系时也需要考虑，因此可以利用式(7)计算推荐信任，最后综合信任可以通过式(9)计算获得。

我们以具备 C/S 架构的生产型信息系统为例，使用 TMBA 模型度量客户端与服务器之间的信任关系，度量的结果可以作为访问控制的依据。在生产型信息系统中，攻击者为了能够从服务器中获取机密信息，以前的方法是对服务器发动攻击，可是服务器由于具有更好的防火墙、更加敏锐的入侵检测系统，因此能够被很好地保护，因而很难被破坏，所以攻

击者开始将矛头指向对安全性不太重视的客户端，攻击者会修改客户端的程序，从而间接地获取机密信息。在本系统中，服务器用来提供所需要的服务，但是这种服务是有条件的，要求只有可信度比较高的客户端才能使用，也就是说服务器必须在一定程度上信任该客户端才能向其提供服务。客户端能够向服务器证明其运行的程序 P 的行为是可信的。我们假设服务器 A 已经有了客户端 X 的过去经验并且记录了所有的经验结果。同时，服务器 A 能够从与 X 有过交互的服务器 B,C 中获得关于 X 的推荐经验，由于 A 与 B,C 对等，因此 A 对于 B,C 的推荐意见的权重相同。服务器 A 允许 X 获取服务的条件是综合信任观点要大于门限观点(0.7,0.3,0)。服务器 A 对于 X 的评估是在 2011 年的 3 月 10 日，服务器 A，B,C 记录的关于客户端 X 的经验结果如表 1 所列。

表 1　经验结果记录

编号	参与实体	信任观点 ω	经验结果	经验类型	请求时间	当前时间
001	A,X,P	[1,0,0]	1,0,0	tr	2011.3.10	2011.3.10
002	A,X,P	[0.813, 0.125,0.062]	13,2,1	tr	2011.1.10	2011.3.10
003	A,BM,P	[0.769,0, 0.231]	10,0,3	bm	2011.1.10	2011.3.10
004	A,BV,P	[0.833, 0,167,0]	10,2,0	bv	2011.1.10	2011.3.10
005	B,X,P	[0.087, 0.783,0.13]	2,18,3	tr	2011.2.6	2011.3.10
006	C,X,P	[0.11, 0.852,0.038]	3,23,1	tr	2011.1.31	2011.3.10

根据表 1 中的信任观点值分别计算独立信任观点，推荐信任观点以及综合信任观点。其中，衰减率 k 取 1，并且实体 A 对于实体 B,C 的意见具有同等的重视程度，因此权重因子为 0.5。

在计算综合信任观点时，根据式(8)需要分别计算独立信任观点以及推信任观点。独立信任观点${}^{A_d}\omega^{B,c_i,Y}$根据式(4)需要分别计算请求发生时的观点${}^{A}\omega_{\Lambda}^{B,c_i,Y}$，以及根据过去的经验计算的过去信任观点${}^{A}\omega_{\Lambda-t}^{B,c_i,Y}$。其中，根据式(5)计算 A 对于实体 X 的组件 P 在请求前 59 天时间的信任观点是${}^{A}\omega_{\Lambda-59}^{X,P,Y}=(0.691,0.106,0.203)$，接下来需要根据式(6)计算请求证明发生时的信任观点，同时需要考虑现有经验记录以及度量和验证过程的经验记录，因此${}^{A}\omega_{\Lambda}^{X,P,Y}=(0.463,0.142,0.395)$，最后计算独立信任观点${}^{A_d}\omega^{X,P,Y}=(0.32,0.233,0.447)$。在计算推荐信任观点时，根据实体 B 在证明请求前 32 天的经验记录计算实体 B 的独立信任观点${}^{B}\omega_{\Lambda-32}^{X,P,Y}=(0.08,0.717,0.203)$，同理，根据实体 C 在证明请求前 38 天的经验记录计算实体 C 的独立信任观点${}^{C}\omega_{\Lambda-38}^{X,P,Y}=(0.099,0.768,0.133)$，$A$ 对于 B,C 的意见重视程度相同，因此，经过计算权重因子后的信任观点分别为实体 B 的直接信任观点是${}^{B}\omega_{\Lambda-32}^{X,P,Y}=(0.04,0.359,0.601)$以及实体 C 的观点为${}^{C}\omega_{\Lambda-38}^{X,P,Y}=(0.049,0.384,0.567)$，$A$ 再根据 B,C 的独立信任观点经过 consensus 计算后得到推荐信任观点${}^{A_r}\omega^{X,P,Y}=(0.063,0.525,0.412)$，最后计算综合信任观点${}^{A_z}\omega^{X,P,Y}=(0.237,0.49,0.273)$。

服务器 A 允许 X 使用其服务的门限值为(0.7,0.3,0.0)，根据信任观点的计算方法所得到的综合信任观点为(0.237,0.49,0.273)小于门限值，因此服务器 A 拒绝提供服务。

结束语　可信远程证明是建立实体之间信任关系的重要方法，它以可信计算技术为基础，为可信性由单独的计算环境扩展到分布式计算环境提供了保障。通过对可信性的定义进行研究分析，进一步明确可信性的证明过程是一个检验实际行为与预期行为是否相符的过程，这种基于行为的证明方法更加符合对于可信性的定义。TCG 所提出的二进制证明方法以及以后出现的一些静态证明方法与可信性的目标存在一定差距，不能够为可信性证明提供充足证据。因此，本文结合现阶段比较前沿的基于行为的证明方法对可信性进行证明，将证明结果作为一种主观逻辑理论中的经验结果进行记录，用于计算信任观点。另外，对于证明过程中存在的不确定因素进行分析，建立了 TMBA 可信模型，并且考虑了可信性的动态特性，最后综合这些因素分别计算了独立信任观点，推荐信任观点以及综合信任观点。

参 考 文 献

[1] Trusted Computing Group. TCG Specification Architecture Overview[S]. reversion 1. 2007

[2] Sailer R, Zhang X, Jaeger T, et al. Design and implementation of a TCG-based integrigty measurement architecture[C]// Proceedings of the 13th USENIX Security Symposium. San Diego, CA, USA, August 2004

[3] Korthaus R, Sadeghi A-R, Stüble C, et al. A practical property-based bootstrap architecture[C]// the Proceedings of the 2009 ACM workshop on Scalable trusted computing. Chicago, Illinois, USA, ACM Press, 2009: 29-38

[4] Sadeghi A-R, Stüble C. Property-based attestation for computing platforms: Caring about properties, not mechanisms[C]// the 2004 New Security Paradigms Workshop. Virginia Beach, VA, USA, ACM SIGSAC, ACM Press, Sept. 2004

[5] Kühn U, Selhorst M, Stüble C. Realizing Property-based Attestation and Sealing with Commonly Available Hard- and Software[C]// Proceedings of the 2007 ACM workshop on Scalable trusted computing. New York, NY, USA, 2007

[6] Chen L, Landfermann R, Löhr H, et al. A protocol for property-based attestation[C]// STC'06: Proceedings of the first ACM workshop on Scalable trusted computing. New York, NY, USA, ACM Press, 2006: 7-16

[7] 李晓勇，左晓栋，沈昌祥. 基于系统行为的计算平台可信证明[J]. 电子学报，2007，6(7)：1235-1239

[8] Li Xiao-yong, Shen Chang-xiang, Zuo Xiao-dong. An efficient attestation for trustworthiness of computing platform[C]// Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06). 2006

[9] Haldar V, Chandra D, Franz M. Semantic remote attestation: a virtual machine directed approach to trusted computing[C]// the Third virtual Machine Research and Technology Symposium (VM'04). USENIX, 2004

[10] Davi L, Sadeghi A-R, Winandy M. Dynamic integrity measurement and attestation: towards defense against return-oriented programming attacks[C]// the Proceedings of the 2009 ACM workshop on Scalable trusted computing. Chicago, Illinois, USA, ACM Press, 2009: 49-54

[11] Gu Liang, Ding Xu-hua, et al. Remote attestation on program execution[C]// the Proceedings of the 3rd ACM workshop on Scalable trusted computing. Alexandria, Virginia, USA, ACM

Press,2008:11-20
[12] Jøsang A. A logic for uncertain probabilities[J]. International Journal of Uncertainty, Fuzziness and Knowledge-based Systems,2001,9(3)
[13] Huang Jing-wei, Nicol D. A Formal-Semanti- cs-Based Calculus of Trust[J]. Internet Computing, IEEE,2010,14(5):38-46
[14] Loscocco P, Smalley S. Integrating flexible support for security policies into the Linux operating system[R]. U. S. National Security Agency(NSA). Feb. 2001
[15] Wang H M, Tang Y B, Yin G, et al. Trustworthiness of Internet-based software[J]. Science in China Series F: Information Sciences,2006,49(6):759-773
[16] TCG Specication Architecture Overview[S]. TCG, April 2004: 11-12
[17] Nguyen E A T, Weiss J, Watson J, et al. Toward an approach to measuring software trust[C]// IEEE Symposium on Security and Privacy. 1991:198-218
[18] Avizienis A, Laprie J C, Randell B, et al. Basic concepts and taxonomy of dependable and secure computing[J]. IEEE Trans. on Dependable and Secure Computing,2004,1(1):11-33
[19] Mundie C, de Vries P, Haynes P, et al. Trustworthy computing [R]. Microsoft White Paper. 2002. http://download. microsoft. com/download/a/f/2/af22fd56-7f19-47aa-8167-4b1d73c d3c57/twc_mundie. doc
[20] 李小勇,桂小林,等. 基于行为监控的自适应动态信任度测模型[J]. 计算机学报,2009(4):664-674

(上接第 22 页)

同基于关键字的服务发现相比,引入语义本体后,本体概念间的等价和继承关系可以使相关的实体在输入输出匹配时进行互相匹配。另外可以设定不同的匹配阈值,以用户的选择来缩放服务选择的范围。由此看来,本算法增加了可能匹配服务的范围,使得服务的查全率也有所提高。

下面是通过构造的 100 组实验数据而得出的查全率和查准率的对比图。其中,图 4 是本文算法和弹性匹配算法的查准率对比图,图 5 是本文算法和弹性匹配算法的查全率对比图。

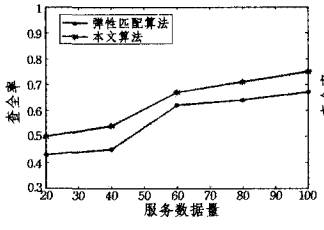

图 4 查准率对比图

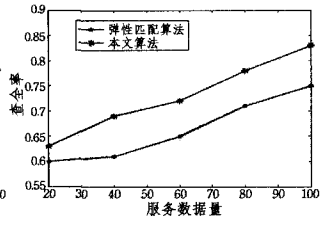

图 5 查全率对比图

结束语 通过分析现有的服务发现方法,找出在具体应用到普适计算中的位置服务方面的不足之处,然后提出一种新的服务匹配算法。本算法从性能上提高了查准率,并且考虑了用户的喜好度和服务质量,更加人性化。但是在服务发现的安全性和隐私性以及完善匹配算法上,没有做进一步的研究,加上构建一个具体的 LBS 系统,也是接下来工作的重要方面。

参 考 文 献

[1] Weiser M. The computer for the twenty-first century[J]. Scientific American,1991,265(3):94-104
[2] 徐光祐,史元春,谢伟凯. 普适计算[J]. 计算机学报,2003,26(9):1042-1050
[3] Kaasinen E. User needs for location-aware mobile services[J]. Per Ubiquit Comput,2003(7):70-79
[4] 周晓,沈振宇,陈鸣. 服务发现机制的比较与分析[J]. 计算机工程与科学,2003,25(2):56-60
[5] Yoon Y-B, Youn H-Y. A New Service Discovery Scheme Adapting to User Behavior for Ubiquitous Computing[M]. Berlin Heidelberg: Springer-Verlag,2005:19-28
[6] Kim M C, Kim S J. A Scenario-based User-oriented Integrated Architecture for Supporting Interoperability Among Heterogeneous Home Network Middlewares[M]. Berlin Heidelberg: Springer-Verlag,2006:669-678
[7] d'Amorim M, Ferrazn C. A Design for Jtrader, an Internet Trading Service[M]. Berlin Heidelberg: Springer-Verlag,2001: 159-166
[8] Oprescu J, Rousseau F, Duda A. Push Driven Service Composition in Personal Communication Environments[Z]. International Federation for Information Processing(IFIP). 2003:505-510
[9] Lee S-H, Jang K-S, Shin D-R. Agent-based Discovery Middleware Supporting Interoperability in Ubiquitous Environments [M]. Berlin Heidelberg: Springer-Verlag,2007:141-149
[10] Hasselmeyer P. On Service Discovery Process Types[M]. Berlin Heidelberg: Springer-Verlag,2005:144-156
[11] Arnold K, O'Sullivan B, Scheifler R W, et al. The Jini specification[S]. Addison-Wesley,1999
[12] The Jini device architecture specification[S]. Sun Microsystem, 1999
[13] Universal Plug and Play (UpnP) [EB/OL]. http://www. upnp. org
[14] Miller B A, Pascoe R A. Salutation Service Discovery in Pervasive Computing Environments[R]. IBM Pervasive Computing White Paper. February 2000
[15] Guttman E, Perkins C E, Veizades J, et al. Sevice Location Protocol[R]. Version 2, IETF, RFC 2680. June 1999
[16] Paolucci M, Kawamura T, Payne T R, et al. Semantic Matching of Service Capabilities[C]//Proceedings of 1st International Semantic Web Conference (ISWC2002). Berlin: Springer-Verlag, 2002:333-34
[17] 林清滢,彭文灵. 基于 OWL-S 的 Web 服务匹配方法及其实现[J]. 微计算机应用,2006,27(4):496-498
[18] Li Lei, Horrocks I. A software framework for matchmaking based on semantic Web Technology[C]// Proceedings of the Twelfth Inernational World Wide Web Conference (WWW 2003). Budapest: ACM Press,2003:31-339
[19] 吕庆聪,周集良,杨帆,等. 普适计算服务匹配技术研究[J]. 计算机科学,2009,36(11):182-185
[20] Mokhtar S B. EASY: Efficient semantic service discovery in pervasive computing environments with QoS and context support [J]. J Syst Soft-ware,2007,10:9-11