doi:10.3969/j.issn.1000-436x.2012.11.006

普适计算中一种上下文感知的自适应可信模型

王江涛[1,2]，陈志刚[1]，邓晓衡[1]
（1. 中南大学 信息科学与工程学院，湖南 长沙 410083；2. 长沙大学 计算机系，湖南 长沙 410003）

摘 要：针对普适计算环境中涌现出的行为可信问题，提出了一种适合于普适计算网络环境的上下文感知的自适应可信模型 CASATM，该可信模型能够自适应地对不同的服务提供不同层次的安全保障，能有效地对时间、地点、服务内容等上下文感知。同时提出了一种简单高效的风险评估模型来完成对一些完全陌生客体的可信度初始化。仿真实验表明该可信模型能有效地感知上下文并抵抗恶意客体的周期性欺骗行为。

关键词：普适计算；可信模型；上下文感知；自适应
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2012)11-0041-08

Context-aware and self-adaptive trust model for pervasive computing

WANG Jiang-tao[1,2], CHEN Zhi-gang[1], DENG Xiao-heng[1]
(1. School of Information Science and Engineering, Central South University, Changsha 410083 ,China;
2. Department of Computer Science, Changsha University, Changsha 410003 ,China)

Abstract: To cope with the behaviour trust problems emerging at ve environments, a context-aware and self-adaptive trust model(CASATM) for pervasive environments was proposed, the trust model provided security protection based on service content adaptively at various level, nd be sensitive to contexts such as time, location and service content. A simple and efficient risk evaluation model was presented to initialize trust value to unknown entities which was a common phenomenon in pervasive environments. Simulation results testify to the contexts awareness of this model, as well as resistance of periodically cheating behaviour from malicious entity.

Key words: pervasive computing; trust model; context-aware; self-adaptive

1 引言

随着便携式可移动设备与低能耗无线通信技术的发展，普适计算技术也得以日益成熟。普适计算倡导将计算与通信能力嵌入到日常生活的物理环境中，使其对用户透明。广义的来讲普适计算包括以下 4 个方面：1)移动计算；2)无线通信；3)嵌入式计算；4)上下文感知传感器网络。其计算环境主要由 PDA、蜂窝手机、智能手机、便携式笔记本、传感器等大量无线计算设备组成。从现在的情况来看这些无线设备无处不在，无线通信技术也逐渐成熟，使得 Weiser 的普适计算构想日益接近现实。

普适计算网络环境是一个混合网络，其中包括了一些提供复杂计算能力的智能空间，由各种无线移动设备组成的 ADHOC 网络、无线传感器网络以及普通的网络。普适计算的网络环境具有动态和不

收稿日期：2011-01-14；修回日期：2011-06-25
基金项目：国家自然科学基金资助项目（60873082, 60903058）；湖南省科技计划基金资助项目（2012FJ4122）；长沙市科技计划基金资助项目（K1109012-71-2）
Foundation Items: The National Natural Science Foundation of China (60873082, 60903058); The Science and Technology Program of Hunan Province(2012FJ4122); The Science and Technology Program of Changsha City (K1109012-71-2)

可预知的特点，网络拓扑变化较快，交互可能发生在熟知的实体之间也可能发生在完全陌生的实体之间，普适计算倡导以人为中心，因此如同人类社会网络存在的安全与可信问题一样，普适计算技术的发展也必然伴随着安全与可信问题，然而传统的安全技术 PKI，CA 等静态信任机制已经不能适应这种动态变化环境的需求，如果缺乏有效的安全可信机制保障，普适计算将难以真正实现，因此，如何设计有效的动态信任机制来适应普适计算中的各种动态变化环境已经逐渐成为一个研究热点，也是本文的主要研究内容。

近年来，国内外众多研究者针对如何解决各种网络中涌现出的各种不良及恶意行为进行了深入研究，提出了众多的可信模型来对有不良或者恶意行为的实体进行惩罚，对行为良好的实体进行奖励，从而达到扬善惩恶以及激励实体间进行合作的作用。然而这些可信模型主要是针对一些传统的网络如 P2P 网络、无线传感器网络等，而对普适计算环境网络的特点并没有加以考虑。普适计算环境网络有以下 3 个主要的特点。

1) 交互时实体的行为模式会随着交互上下文环境的改变而变化，在这里的上下文环境指的是时间、地点、服务内容等。例如对于服务内容上下文，某些恶意实体可能会采取一种周期性的欺骗行为，周期性地在某些低级别服务上表现良好挣取足够的可信度后转而在某些高级别的重要服务上通过恶意行为获得私利。同时实体的行为模式在不同的时间、地点会表现不同。而传统的可信模型没有考虑到这些上下文信息，因此也无法解决这些问题。

2) 普适计算网络环境的动态性是其重要特征，即网络拓扑经常改变，经常需要跟陌生的实体进行交互，因此在相应的可信模型中需要考虑交互风险评估，这点在传统的可信模型中并没有涉及。

3) 网络中实体的计算、存储能力普遍不强，一些复杂的可信模型并不适用。一般而言在普适计算中可信模型是应用在设备的服务发现机制中，是服务发现机制的核心组成部分，服务发现机制的作用是在普适计算网络环境中找到并选择能够安全有效地提供某种特定服务的设备。可信、安全是普适计算的服务发现过程中必须要考虑的重要因素。许多用户愿意向其他用户提供一些服务，前提是提供这些服务不会对自身产生安全威胁，因此需要一个基于可信模型的能够确保安全的服务发现模型。与此同时，这些设备大多缺乏足够的计算和通信能力，因此传统的基于加密的安全机制在普适计算环境下不是很实际。很多嵌入式和移动设备倾向于忽略安全、可信与用户隐私，原因就是附加的复杂协议会大幅降低设备的性能。因此设计一个适合普适计算网络环境并能提供基本安全保护的轻量级可信安全机制是实现普适计算的迫切需要。

综上所述适合普适计算环境的可信模型需要具有以下几个特征。

1) 上下文感知能力。考虑普适计算环境网络动态变化的本质特点，该可信模型应该能够对时间、地点、交互内容等上下文具有感知能力。

2) 自适应性。该可信模型应该能对同一设备的不同服务具有自适应能力，对不同的服务根据其特点提供不同水平的安全保护。

3) 风险评估能力。在普适计算的网络环境中，拓扑变化很快，经常需要同一个没有任何信息的用户或设备交互，同时也无法从邻居节点得到该设备的任何信息，因此需要一个简单高效的风险评估模型来对该设备进行可信度初始化。

4) 独立性。该可信模型应该不需任何公用设施或者集中式设备而独立工作，同时该模型运行时尽量对用户透明，才适合普适计算的网络环境。

5) 低代价。该可信模型应该是一个低代价的模型，即该模型应该是一个轻量级的模型，可信模型的实现不会占用系统过多的资源，不会带来过多的计算和通信消耗，同时能耗低。

针对普适计算环境网络的这几个特点，本文设计了一种简单高效的上下文感知的自适应可信模型（CASATM），该模型能对时间、地点、服务内容等上下文有效感知，并且能对初次交互的陌生实体通过风险评估机制进行快速的可信度初始化。通过仿真实验分析，该可信模型能有效地感知上下文并抵抗恶意客体的周期性欺骗行为。

2 相关研究

近年来，国内外许多学者对分布式网络计算环境下的可信模型进行了研究，提出了大量可信模型，本文首先对可信模型中借鉴的 2 个可信模型 PTM 和 TSSD 进行了介绍，介绍了这 2 个模型的优缺点以及对本文的借鉴意义，然后介绍了一些其他主要可信模型。

2.1 PTM

PTM[1,2]是欧洲 IST FP6 支持的 UBISEC(安全的普适计算)研究子项目。它定义了基于普适环境域间的动态可信模型，主要采用改进的证据理论(D-S theory)方法进行建模，信任度的评估采用概率加权平均的方法。PTM 中 2 个实体间的信任关系表示为 $R(A, B)=a$，$a\in[0, 1]$。$R(A, B)=a|G(a+? R(A, B)\geq a)\wedge G(a-.? R(A, B)<a)$，信任度随着时间和行为上下文的变化而增减($a+$表示正行为，$a-$表示负行为)。该模型使用下式计算更新后的信任度值 $R(A,C)_{\text{new}}$。

$$V_{\text{a}}=\left(1-\frac{A_{\text{N}}}{Total_{\text{a}}}\right)W_{\text{a}}^{m}$$

$$R(A,C)_{\text{new}}=\begin{cases}V_{\text{a}}b+R(A,C)_{\text{old}}(1-b),V_{\text{a}}>0\\0,\text{其他}\end{cases}\qquad(1)$$

其中，V_{a} 为当次交互评价，$Total_{\text{a}}$ 为双方交互总次数，A_{N} 为双方交互负行为的次数，W_{a} 为交互权重，正行为时为 1，负行为时为 0.5，m 为当前的安全水平因子（体现了模型的地点感知能力），b 体现历史权重。

PTM 是较早研究普适环境下动态信任关系的模型，其有以下主要优点。

1) 信任推导和进化的规则体现了一种严格的惩罚性。从计算式可知，信任是得到困难、失去容易的值，因为 $R(A,C)_{\text{new}}$ 随着正行为的增加缓慢增长，但随着负行为的增加会迅速降低。

2) PTM 的可信模型也很好地体现了信任度随着时间和行为上下文的变化而增减的动态性。

3) 是一个具体实现和应用的动态可信模型。

4) 没有复杂的迭代计算，适合普适环境下能源节约的应用需求，具有较好的计算收敛性和可扩展性。

但 PTM 模型也存在如下明显的不足。

1) 不能处理由于部分信息和新未知实体所引起的不确定性问题，没有详细的风险分析及建模风险和信任之间的关系。

2) 算术平均获得间接信任度，没有考虑到信任的模糊性、主观性和不确定性。

基于以上分析，本文借鉴了其能够部分体现上下文感知能力的可信度计算公式，并对其进行改进，提出了新的可信度计算模型，使其能有效对时间、地点、交互内容等上下文进行感知。

2.2 TSSD

Sheikh I Ahamed 等于 2008 年在《Computer Communication》期刊上提出了 A trust-based secure service discovery (TSSD) model for pervasive computing[3]模型。该文中的可信模型有以下主要特点。

1) 该模型对设备的可信度进行细分，对同一设备的不同服务维护不同的可信度，这样可以提高可信模型的精确度，同时也意味着该模型要维护的信息量较大。

2) 基于服务的安全保障：给不同的服务提供不同的安全保障，即安全不是基于设备的而是基于具体服务的，一个设备中的所有服务根据安全需要划分为不同级别，提高了可信模型的自适应能力。

3) 针对陌生实体的交互情况，引入了风险评估模型，不过文中的风险评估模型过于简单，并没有详述。

该模型的主要不足如下。

1) 可信度的计算过于简单，仅仅根据服务时间来确定。

2) 不具有上下文感知能力，因此不适合普适计算环境。

3) 可信度的维护代价较大。

4) 在以下的场景中该可信模型具有不合理性。如果主体对于客体在某个服务上的可信度评价低于某个阈值，该客体将永远没有机会通过自身的努力来获得主体的该服务。

基于以上的分析，本文借鉴了其可信模型中基于服务的安全保障思想，对同一个设备中的所有服务根据安全需要划分为不同级别来提高可信模型的自适应能力，同时为了改进上面指出的该模型的不足之处，本文对同一设备只维护一个可信度综合值，即可信度不细分，来降低模型实施代价。

2.3 近期内其他的一些可信模型

2.3.1 FTM

2010 年，Sheikh I Ahamed 等在《Journal of Systems and Software》上的《Design, analysis, and deployment of omnipresent Formal Trust Model (FTM) with trust bootstrapping for pervasive environments》[4]一文中提出了 FTM 模型，在该文中提出一个普适计算网络环境下通用的、上下文关联的基于信誉的通用信任模型，文中提出一个多跳推荐协议和一个灵活的行为模型来处理交互，该文的另一个贡献是提出了一个信任初始化模型，该信任初

始化模型根据具体的安全需要将服务和物理条件上下文划分为不同的安全级别，同时该文提出了解决恶意推荐的有效方法。

Sheikh I Ahamed 等的团队在可信模型研究方面已经累积了多年的经验，提出了大量的模型，其核心思想是对不同的服务提供不同的安全保护，利用信任来让普适计算网络环境下的各种设备自主合作。在其信任模型中充分考虑信任的多样性和上下文相关性。

2.3.2 PTO

2008 年，Mohsen Taherian 等提出了 PTO 模型，其文章《PTO: a trust ontology for pervasive environments》[5]首次提出了可信模型要考虑普适计算环境中实体之间的语义关系，特别是实体间不同信任关系之间的语义关系。该文提出一种基于本体结构的信任计算模型，每个实体独立地计算其对其他实体的信任关系，并基于该信任关系来做出交互决策。该模型采纳了本体模型使得其可扩展性更高，比如提供了一种更好的途径来解决普适计算环境中上下文感知的问题。文中借鉴本体论的思想来对实体间的各种信任关系之间的关联性进行建模是一大亮点。

2.3.3 CBTM (cloud-based trust model)

He 等提出了一种普适环境下基于云模型(cloud model)的可信模型 CBTM[6]。该模型以云的形式，将实体之间信任关系描述和不确定性描述统一起来，并给出了信任云的传播和合并算法。信任云的定义是以一维正态云的形式描述的实体之间的信任关系，形式化表述为 $tc_{AB} = nc(Ex, En, He)$, $0 \le Ex \le 1, 0 \le En \le 1, 0 \le He \le 1$。其中，$Ex$ 是信任期望，表明了实体 A 对 B 的基本信任度，En 是信任熵，反映了信任关系的不确定性，而 He 是信任超熵，反映了信任熵的不确定性。

2.3.4 Dimitri's model (Bayesian dynamic trust model[7])

Bayesian 方法的特点是使用概率去表示所有形式的不确定性，学习或其他形式的推理都用概率规则来实现，Bayesian 学习的结果表示为随机变量的概率分布，它可以解释为对不同可能性的信任程度。

Dimitri 基于 Bayesian 网络模型提出了一种使用 Kalman 信息过滤方法的动态随机估计模型，支持一个系统的动态进化过程，而且无论有无新的上下文被检测到，模型都会自动进化，这个恰当的数学工具非常适合于动态可信模型的需求。

2.3.5 Claudiu's model (reinforcement learning model)

Claudiu[8]等提出了一种 P2P 环境下基于机器学习中强化学习[9]方法的动态可信模型。信任度的取值范围也是采用集合[0, 1]。与其他 P2P 可信模型显著不同的是，它引入近期信任、长期信任、惩罚因子和推荐信任 4 个参数来反映节点信任度。提出了用机器学习中强化学习的方法计算信任度，并用惩罚因子对学习因子进行了明确定义，所以，该模型是一个自适应的系统。对新发生的交互行为有足够的敏感性，提高了可信模型的动态适应能力。通过惩罚机制，可以有效减少不诚实节点，特别是合伙欺骗节点提供的虚假反馈。

3 基于可信模型的服务发现机制

本文提出的一种上下文感知的自适应可信模型 CASATM，其主要是应用在普适计算环境中设备的服务发现机制中，是该机制的核心组成。服务发现机制主要由 3 部分组成，分别是服务发现模块、可信评估模块和风险评估模块。3 个模块的功能逻辑关系如图 1 所示。

服务发现模块用于接收（或发送）服务申请，在接收到服务申请后调用可信评估模块来验证该申请者的可信度是否满足要求，如果没有该申请者的可信度信息，同时也无法通过邻居来获取其推荐可信度，则调用风险评估模块来对陌生实体进行可信度的初始化。

每个设备将自己所拥有的所有服务根据其安全需求设定一个安全因子（其范围为[0,1]，例如可以划分为 0.1，0.2，0.3，…，0.9，比如天气查询服务的安全因子为 0.1，解压缩服务为 0.3，Internet 连接服务为 0.7，地址簿服务为 0.9），如某个设备的某个服务的安全因子为 0.5，则意味着该设备对该服务申请者的可信度评估必须要不小于 0.5，该次服务申请才会被接受。不同的服务拥有不同的安全因子，该服务安全因子体现了该服务在安全方面的重要性，服务安全因子的设定由用户自定义，用户可以根据自身的需要、偏好及历史经验来对服务池里的每一个服务进行安全因子设定。

本模型设定一个通信加密的阈值 R，即某次服务交互的安全因子如果大于 R，则该次交互的通信需要加密。

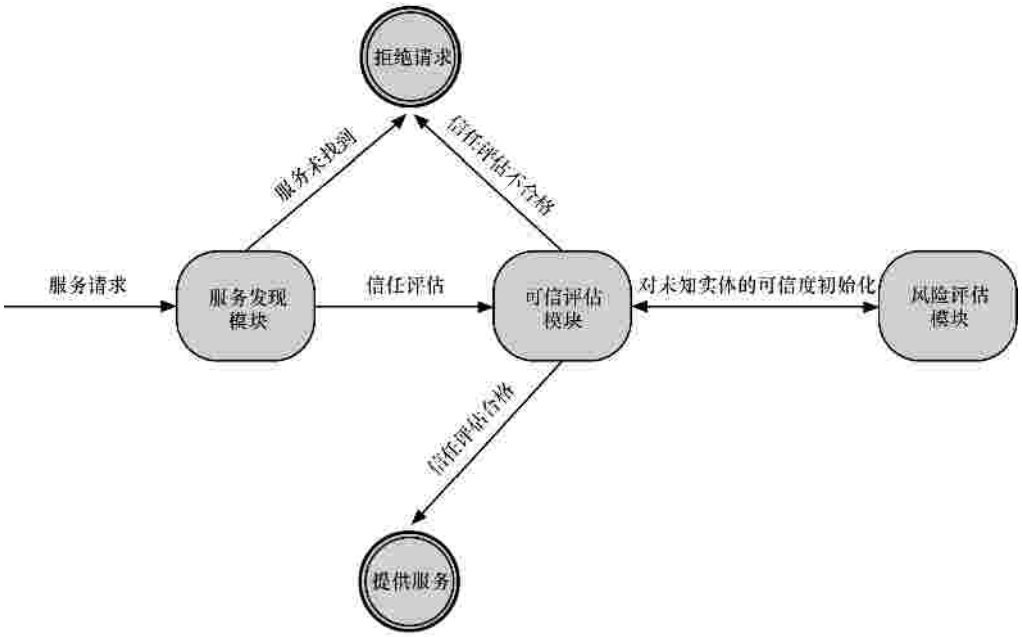

图 1　3 个模块的逻辑关系

设定一个用户介入阈值 U，即某次服务交互的安全因子如果大于 U，则即使服务申请者通过了可信评估，那么该次交互也必须要提交给用户来显示以得到用户的允许，这个阈值 U 的作用主要用于保护某些安全性要求特别高的服务。

安全因子、通信加密阈值、用户介入阈值的引入可以简单有效地提高服务发现模型的灵活性和自适应性，即不同的服务享受不同水平的安全保护。

3.1　服务发现模块

该模块的主要功能是向邻近的设备发送服务请求和接收服务申请响应以及从别的设备接收服务请求和对该请求进行回应。在本文中假设网络中邻近的设备组成一个簇，整个普适计算网络由多个不同的簇组成，服务发现遵从就近原则，即每个设备倾向于首先选择向簇内设备请求服务，如果找不到才会向其他相对较近的簇申请服务。

服务发现模块使用一个 match all 的技术来发现邻近设备的所有潜在服务，当需要请求某一项服务时，该模块则可以通过多播的方式向某些设备提出服务申请，也可以通过广播的方式在簇内进行服务请求广播，接收到一个或多个服务响应后，在进行服务选择时则调用相应的可信评估模块来选择可信度最高的服务提供设备进行实际交互（为了保障 QoS 和容错，将次优服务匹配设备的信息保存起来做备份之用）。

3.2　可信评估模块

该模块的主要功能包括 2 个，1) 负责对服务申请者的可信度进行评估来决定是否接受某个设备提出的服务申请；2) 负责对多个服务提供者的可信度进行评估来决定最终选择哪个设备进行实际申请。该可信评估模块对用户而言是透明的，即用户只需要初始时对自身设备的不同服务设置不同的安全因子，之后该可信评估模型能自动根据设置而运作，除了涉及个别安全水平高的服务需要用户及时介入外，其他情况无需用户介入。

该模块负责维护对所有实体的可信度评估（与 TSSD 中可信模型不同，本模型的可信度评估是基于设备而非服务的，即评估者对每个实体只有一个总可信度评估而不区分服务，主要目的是这样可以降低可信模型的复杂度，减小实施代价），对可信度进行初始化设置以及根据交互的情况进行可信度动态更新。在无法对一个陌生实体进行可信度评估的时候，该模块会从邻居设备中征集推荐可信度评估进行推荐可信度计算，在无法从邻居节点得到陌生实体的推荐可信度的时候该模块会调用风险评估模块来对该陌生实体进行可信度初始化。

3.3　风险评估模块

普适计算环境的一个重要特点是网络拓扑变化很快，用户经常需要同陌生的设备交互，而且有时无法从邻居设备得到相关信息来计算该陌生对象的推荐可信度，这个时候本模型使用风险评估模

块来对陌生设备的可信度进行初始化，其主要思想是：评估者由于没有陌生实体的任何信息，所以只能靠主观的判断来指定一个可信度的初始值，判断的依据主要来源于其对最近一段时间内所有实体交互行为的主观整体判断。即如果近段时间内网络大环境好，大多数用户行为良好，则对陌生客体赋一个较高的初始可信度，否则的话，赋一个较低的初始可信度。

本模型通过修改可信度计算式（见第4节）中的时间衰减因子（即加大近期交互的权重）来计算所有与主体有交互历史的客体的近期平均可信度，用该近期平均可信度来对陌生实体赋初值。

4 上下文感知的自适应可信模型

4.1 可信度的定义

本模型将可信度定义为主体通过对客体的过往交互历史或推荐信息而得到的对该客体本质的认识的信任指标。可信度反映了主体对客体行为的一个客观期望，同时也蕴含着风险。

4.2 可信度的性质

可信度拥有以下3个性质。

1) 自反性。即每个设备或用户对自己完全信任。

2) 共同信任。如果一个用户 x 拥有多个设备 $(s_1,s_2,\cdots,s_n)$，则这些设备之间也完全信任。即

$$\forall s_1,s_2(o(x,s_1)\ \mathrm{I}\ o(x,s_2))\Rightarrow t\ (s_1,s_2,1) \tag{2}$$

3) 不完全传递性。如果 A 信任 B，B 信任 C，那么 A 也信任 C，但是这3个信任的信任值不同，即

$$\begin{aligned} &t\ (\mathrm{A,B},1)\ \mathrm{I}\ t\ (\mathrm{B,C},1)\Rightarrow t\ (\mathrm{A,C},x)\\ &t\ (\mathrm{A,B},x)\ \mathrm{I}\ t\ (\mathrm{B,C},y)\Rightarrow t\ (\mathrm{A,C},z)\\ &z=y\ (x,y)\\ &0<x,y,z<1 \end{aligned} \tag{3}$$

4.3 可信度的初始化

对于初次交互的陌生客体，本模型支持2种方式的可信度初始化。

第一种方式是本模型提出的通过风险评估模块来完成对完全陌生实体的可信度初始化，基本原理在3.3节中已阐述，具体实现见4.4节中对可信度计算式的描述，其主要思想是通过本文提出的可信度计算式(5)来对近期的网络大环境进行评估，然后根据评估结果来给陌生实体的可信度进行初始化。

第二种是传统的方式即通过向簇内邻居节点征集推荐可信度，其计算式为

$$R_{ac}=\frac{\sum_{i=1}^{n}R_{ai}R_{ic}}{\sum_{i=1}^{n}R_{ai}} \tag{4}$$

其中，i 为与实体 a 和 b 都有交互历史的推荐第三方，该计算式是一个推荐可信度加权平均公式，能较客观地反映客体的可信度。

4.4 可信度的计算

本模型对于可信度的动态进化借鉴了 PTM 模型，引入了时间窗口、时间衰减因子、安全敏感因子、服务安全因子来体现模型对时间、地点、交互内容等上下文的感知能力。

主体对客体的每次交互行为进行评价分为2类：正行为和负行为，正行为则适当提高其可信度，负行为则降低其可信度（具体如何评价正负行为，不同的应用背景有不同的标准，这里不详述）。

主体对每个客体维护一个长度为 n 的交互历史，划分为 n 个时间窗口，对每个时间窗口进行编号 0,1,2,⋯,n-1，根据交互的时间次序依次编号，即对最近的交互编号为 0，其次为 1,2,⋯。每完成一次新的交互后，交互信息依次后移。

在每个时间窗口内保存当次交互的一些信息，如交互权重、安全敏感因子、服务安全因子等。

本模型的可信度更新式为

$$R=\frac{\sum_{i=1}^{n-1}g^{tw_i}sw_i^{1-m_i}aw_i}{\sum_{i=1}^{n-1}g^{tw_i}sw_i^{1-m_i}} \tag{5}$$

其中，R 为对某客体的可信度评价，aw 为该次交互的交互权重，正行为为 1，负行为为 0。m 为安全敏感因子（范围为[0,1],1 为最敏感，0 为最不敏感，该安全敏感因子用来体现模型对地点上下文的敏感，即主体处于不同的环境时其对安全的敏感性是不同的，比如处于自己的办公室则对安全的敏感性相对小些，处于公共场所则对安全的敏感性大些）。g 为时间衰减因子。tw 为该次交互的时间窗口编号，体现时间上下文敏感。SW 为服务安全因子，体现交互内容上下文敏感性。

该可信度计算式(5)在本模型中同样应用于风险评估模型，只需将时间衰减因子 g 减小，即加大近期交互的权重，就可评估出对该客体近期内交互情况的可信度，然后对所有交互客体取近期内的平

均可信度即可得到近期风险评估值 T，预估出近期内网络的大环境，然后把该近期风险评估值 T 作为陌生实体的初始可信度。

5　可信模型分析

5.1　场景分析

下面提出 2 个在大多数可信模型中常见的场景来分析本可信模型的特点。

场景 1：在大多数可信模型中均存在恶意欺骗行为，即怀有恶意的客体 B 可以周期性地采取通过在不重要服务领域的少数几次正行为的交互来骗取主体 A 足够高的可信度后，转而在一些很重要的服务领域来对主体造成伤害。而本模型比较好地解决了这个问题，本文提出的可信模型是一个自适应的模型，能对同一设备不同服务提供不同层次的安全保护，模型中引入的服务安全因子体现了系统对不同服务安全保护的重视程度，在可信度计算式中的 sw_i 参数即体现了不同的服务交互在交互历史中具有不同的权重。因此即使客体 B 要继续采取上述策略来进行恶意欺骗行为，也要付出更大的代价，根据本文的可信度计算模型，客体 B 在不重要的服务领域通过正行为来增加可信度的速度是很缓慢的，因为这些不重要服务的权重较低，即使在这些服务领域进行正行为也只能稍稍的增加整体可信度，而客体 B 在重要的服务领域的实施负行为则其可信度会迅速降低，因此本方案能有效地解决这个问题，通过后面的实验分析也可看出。

场景 2：在 TSSD 模型中由于对同一设备服务维护不同的可信度，因此如果主体 A 对客体 B 在某个服务领域的可信度评估小于某一阈值，则该客体 B 将永远无法向主体 A 申请该服务，其服务申请将直接被拒绝。而在本模型中由于对同一设备的所有服务只维护一个统一的可信度，因此即使客体在某个服务领域的行为暂时表现不好，该客体也可以通过在其他的服务领域中通过自身的努力来逐步提高自身的可信度，从而可能在未来重新获得申请该服务的资格。

5.2　可信模型复杂性分析

本方案中可信模型不依赖于任何公用设施或集中式设备，具有良好的独立性，可信度计算式的复杂度为 $O(n)$，不需要迭代计算，相对简单高效，并且能够有效地对时间、地点、交互内容等上下文感知，适合普适计算的网络环境，对同一设备只维护一个整体的可信度，减小了模型的实施代价。

5.3　实验分析

5.3.1　可信模型的服务内容上下文感知能力分析（即恶意欺骗场景分析）

在大多数可信模型中均存在某些客体恶意欺骗的行为，即某些客体可以周期性地在一些不重要的服务领域通过少数几次正行为交互累积高的可信度后，马上在重要的服务领域对主体采取恶意行为，这个恶意欺骗的问题大多数可信模型均无法解决。本模型在可信度计算式中引入了服务安全因子，可以较好地解决这个问题，同时也体现了本可信模型具有服务内容上下文感知能力，即在本模型的可信度计算式中客体通过在不重要服务领域的正行为来累积可信度的过程很缓慢，而在重要服务领域进行负行为时其可信度下降很快。使得那些周期性恶意欺骗的客体付出更大的代价。

下面通过实验来具体分析，本文中可信模型的可信度计算式借鉴了前面提及的经典可信模型 PTM。在 PTM 模型中，无法解决上面提及的恶意欺骗行为，而本文的可信模型通过在可信度计算式中引入服务安全因子可以有效解决这个问题。

实验假设条件如下：CASATM 和 PTM 中代表时间上下文的时间折旧系数 g 和 b 均为 0.5，代表地点上下文的参数 m 均为 0。初始时在 2 个模型中主体 A 和客体 B 在服务安全因子 sw=0.5 的服务领域进行了一正一负 2 次交互，然后客体 B 周期性地采取在 sw=0.2 的不重要服务领域进行连续 3 次正行为来累积可信度，又在 sw=0.9 的重要服务领域进行一次恶意行为来欺骗主体。在 2 种可信模型中主体 A 对客体 B 的可信度评估如图 2 所示。

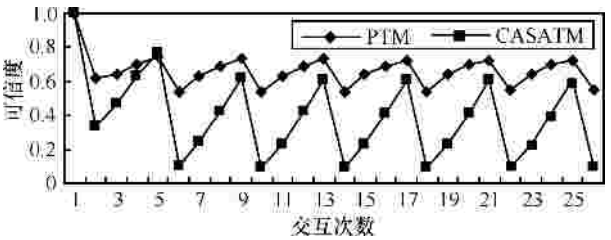

图 2　可信模型的抗恶意欺骗能力分析

由图 2 可知，对于那些采取周期性欺骗行为的恶意客体，本可信模型 CASATM 具有较好的抵抗能力，在本模型中恶意欺骗客体通过在不重要服务领域的正行为累积可信度的速度相对较缓慢，而该

恶意欺骗客体进行负行为时其可信度会迅速下降，从图 2 中可以看出在本模型中恶意欺骗客体的可信度始终处于相对较低的水平，因此本模型具有较好的抗恶意欺骗能力。

5.3.2 CASATM 可信模型的地点上下文感知能力分析

本模型通过可信度计算式中的安全敏感因子 m 来体现模型的地点上下文感知能力，即实体处于不同的环境下其安全敏感因子是不同的，假设初始时主体 A 和客体 B 双方在 sw=0.2，g =0.5，m=0.5 的参数条件下进行了一正一负 2 次交互，在此基础上假设交互双方在 2 个不同的场景下分别进行了五负五正共 10 次交互，2 个场景唯一的区别是主体 A 的安全敏感因子不同（即双方交互地点不同），分别为 m=0.2 和 m=0.9。双方交互过程中主体 A 对客体 B 的可信度评估的变化情况如图 3 所示。

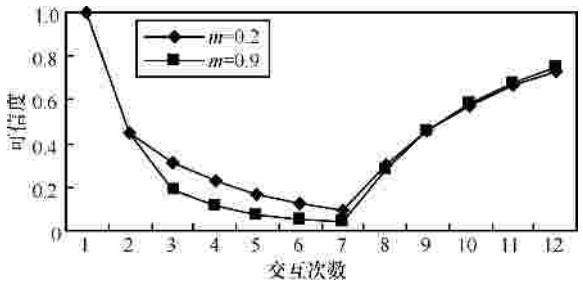

图 3 CASATM 可信模型的地点上下文感知能力分析

由图 3 可以看出，在 m=0.9 时相对 m=0.2，本可信模型中主体 A 对于客体 B 的行为更为敏感，其可信度的变化曲线更为陡峭，即可信度随着客体的负行为下降得更快，随着客体的正行为上升得更快。实验结果验证了本文提出的 CASATM 可信模型具有地点上下文感知能力。

5.3.3 CASATM 可信模型的服务上下文感知能力分析

本模型通过可信度计算式中的服务安全因子 SW 来体现模型的服务上下文感知能力，即交互双方在不同重要程度的服务领域进行交互时，其行为对可信度的评估会产生不同的影响。

实验假设条件如下：CASATM 和 PTM 中代表时间上下文的时间折旧系数 g 和 b 均为 0.5，代表地点上下文的参数 m 均为 0。假设初始时主体 A 和客体 B 双方在 sw=0.5 的参数条件下进行了一正一负 2 次交互，在此基础上假设交互双方在表 1 中的参数条件下进行了 10 次交互。

表 1 10 次交互中的实验参数设置

服务安全因子（SW）	正负行为（+，-）
0.3	+
0.2	-
0.8	+
0.9	-
0.3	+
0.5	-
0.9	+
0.8	-
0.7	+
0.8	-

在 CASATM 模型和 PTM 模型中双方交互过程中主体 A 对客体 B 的可信度评估的变化情况如图 4 所示。

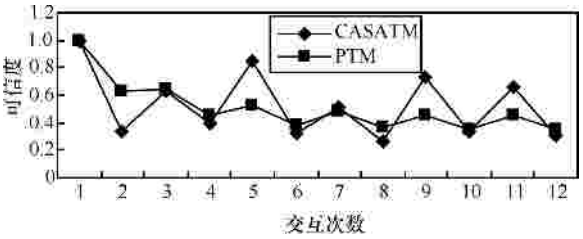

图 4 CASATM 可信模型的服务上下文感知能力分析

由图 4 可以看出，相对 PTM 模型，本可信模型对交互的服务内容更为敏感，反映在图中即为本模型的可信度曲线上下波动更大。实验结果验证了本文提出的 CASATM 可信模型具有服务上下文感知能力。

6 结束语

针对普适计算环境中涌现出的行为可信问题，本文提出了一种适合于普适计算网络环境的上下文感知自适应可信模型 CASATM，该可信模型能够自适应地对不同的服务提供不同层次的安全保障，能有效地对时间、地点、服务内容等上下文感知，提出了一种简单高效的风险评估模型来完成对一些完全陌生客体的可信度初始化。通过仿真实验分析该可信模型能有效地抵抗恶意节点的周期性欺骗行为。

参考文献：

[1] ALMENAREZ F, MARIN A, DIAZ D, *et al*. Developing a model for trust management in pervasive devices[A]. Bob Werner, ed. Proc of the 3rd IEEE Int'l Workshop on Pervasive Computing and Communication Security (PerSec 2006)[C]. Washington, USA, 2006. 267-272.

（下转第 56 页）

[6] 丁超, 杨立君, 吴蒙. IoT/CPS 的安全体系结构及关键技术[J]中兴通信技术, 2011,17(1):11-16.
DING C, YANG L J, WU M. Security architecture and key technologies for IoT/CPS[J]. ZTE Technology Journal, 2011, 17(1):11-16.

[7] TOMMILA T, VENTA O, KOSKINEN K. Next GenerationIndustrial Automation-Needs and Opportunities, AutomationTechnology Review[R]. 2001.34-41.

[8] LOGEAISG. Internet of Things in the Context of Manufacturing[R]. SAPResearch Report.

[9] KIM H B,YOO M,CHO K. Application of M2M technology to manufacturing systems[A]. Information and Communication Technology Convergence[C]. 2010. 519-520.

[10] 彭瑜.物联网技术的发展及其工业应用的方向[J].自动化仪表,2011,32(1):1-7.
PENG Y. Development of the Internet of things and its orientation in industrial applications[J]. Process Automation Instrumentation, 2011, 32(1):1-7.

[11] 王建强.物联网在感知矿山建设中的应用研究[J].中国安全生产科学技术,2012,8(5):178-183.
WANG J Q. Application of IOT in construction of sensor mine[J]. Journal of Safety Science and Technology, 2012, 8(5):178-183.

[12] 李楠, 刘敏, 严隽薇. 面向钢铁连铸设备维护维修的工业物联网框架[J]. 计算机集成制造系统,2011,17(2):413-418.
LI N, LIU M,YAN J W. Framework for industrial Internet of things oriented to steel continuous casting plant MRO[J]. Computer Integrated Manufacturing Systems, 2011, 17(2):413-418.

[13] 曾韬. 物联网在数字油田的应用[J] .电信科学,2010,26(4):25-32.
ZENG T. IoT's Application in the "Digital Oil Field" [J]. Telecommunications Science, 2010,26(4):25-32.

[14] 龚钢军, 孙毅, 蔡明明. 面向智能电网的物联网架构与应用方案研究[J]. 电力系统保护与控制,2011,39(20):52-58.
GONG G J, SUN Y, CAI M M. Research of network architecture and implementing scheme for the Internet of things towards the smart grid[J]. Power System Protection and Control, 2011,39(20):52-58.

作者简介：

杨金翠（1969-），女，山西侯马人，北京邮电大学博士生，主要研究方向为信息安全、物联网安全、软件工程等。

方滨兴（1960-），男，江西万年人，中国工程院院士，北京邮电大学校长、博士生导师，主要研究方向为网络安全、信息内容安全、并行处理、互联网技术等。

翟立东（1982-），男，山西祁县人，博士，中国科学院副研究员，主要研究方向为融合网络安全监测、网络攻防、数据挖掘、物联网控制安全等。

张方娇（1989-），女，山东新泰人，北京邮电大学硕士生，主要研究方向为物联网安全。

（上接第 48 页）

[2] ALMENAREZ F, MARIN A, CAMPO C, *et al.* TrustAC: trust-based access control for pervasive devices[A]. LNCS 450[C]. Berlin, Germany, 2005. 225-238.

[3] AHAMED S I, SHARMIN M. A trust-based secure service discovery (TSSD) model for pervasive computing[J]. Journal of Computer Communications, 2008,31(18):4281-4293.

[4] AHAMED S I, HAQUE M M. Design, analysis, and deployment of omnipresent formal trust model (FTM) with trust bootstrapping for pervasive environments[J]. Journal of Systems and Software, 2010, 83(2): 253-270.

[5] TAHERIAN M, JALILI R, ABOLHASSANI H, *et al.* PTO: a trust ontology for pervasive environments[A]. IEEE AINA-2008 International Conference[C]. Gino Wan, Okinawa, Japan, 2008.301-306.

[6] HE R, NIU J W, ZHANG G W. CBTM: a trust model with uncertainty quantification and reasoning for pervasive computing[A]. LNCS 3758[C]. Berlin, Germany, 2005. 541-552.

[7] MELAYE D, DEMAZEAU Y. Bayesian dynamic trust model[A]. LNCS 3690[C]. Berlin, Germany, 2005. 480-489.

[8] DUMA C, SHAHMEHRI N. Dynamic trust metrics for peer-to-peer system[A]. Proc of the 16th Int'l Workshop on Database and Expert Systems Applications (DEXA 2005)[C]. Washington, USA, 2005. 776-781.

[9] KAELBLING L P, LITTMAN M L, MOORE A W. Reinforcement learning: a survey[J]. Journal of Artificial Intelligence Research, 1996, 4:237-285.

作者简介：

王江涛（1977-），男，湖南郴州人，长沙大学讲师，主要研究方向为普适计算网络环境中的可信模型研究、上下文感知可信模型。

陈志刚（1964-），男，湖南益阳人，博士，中南大学教授、博士生导师，主要研究方向为网络计算与分布式处理。

邓晓衡（1974-），男，湖南衡阳人，博士，中南大学副教授，主要研究方向为流量管理、网络拥塞控制、网络优化、网格计算等。