ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.6, June 2007, pp.1510−1521
DOI: 10.1360/jos181510

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

大规模分布式环境下动态信任模型研究*

李小勇, 桂小林+

(西安交通大学 电子与信息工程学院,陕西 西安 710049)

Research on Dynamic Trust Model for Large Scale Distributed Environment

LI Xiao-Yong, GUI Xiao-Lin+

(Department of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

+ Corresponding author: Phn: +86-29-82667860 ext 805, E-mail: xlgui@mail.xjtu.edu.cn, http://grid.xjtu.edu.cn

Li XY, Gui XL. Research on dynamic trust model for large scale distributed environment. *Journal of Software*, 2007,18(6):1510−1521. http://www.jos.org.cn/1000-9825/18/1510.htm

Abstract: With the in-depth researches of large scale distributed systems, such as Grid computing, Ubiquitous computing, P2P computing, Ad hoc networks, etc, system is a dynamic and cooperative model made up of multi-software serving. Under these dynamic and uncertainty environments, trust mechanism based on CA (certificate authority) in a regular PKI (pubic key infrastructure) can't adapt to these requirements. Dynamic trust mechanism is a new and hot topic of security research for these new distributed applications. In this paper, firstly, the concepts, problems, and research approaches of dynamic trust relationship are summarized and presented. Secondly, several typical dynamic trust model systems including their mathematical methods are described in detail. And then, this paper presents the results of comparative evaluation of these models under a selection of scenarios. Finally, the current problems and the challenges of this field for future research are presented. The research work indicates that the dynamic nature of trust creates the biggest challenge in measuring trust and predicting trustworthiness. So the future work will focus on the theoretical research of dynamic trust relationships to present a solid theoretical foundation for the practical applications.

Key words: distributed system; information security; dynamic trust model; context

摘 要: 随着网格计算、普适计算、P2P 计算、Ad Hoc 等大规模的分布式应用系统的深入研究,系统表现为由多个软件服务组成的动态协作模型.在这种动态和不确定的环境下,PKI(pubic key infrastructure)中基于 CA(certificate authority)的静态信任机制不能适应这种需求,动态信任模型是新的研究热点.分析了动态信任关系的相关概念、主要问题和研究方法;选取新的、典型的动态信任模型及其使用的数学方法进行评述,并进行了各种算法的比较性总结;分析了目前研究中的问题,并展望了其未来的发展方向.研究表明,动态性是信任关系量化与预测的最大挑战.今后的工作重点是对信任动态性的本质属性作进一步的理论研究,为实际应用提供坚实的理论基础.

关键词: 分布式系统;信息安全;动态信任模型;上下文
中图法分类号: TP393 文献标识码: A

* Supported by the National Natural Science Foundation of China under Grant No.60273085 (国家自然科学基金); the Program for New Century Excellent Talents in University of China under Grant No.NCET-05-0829 (新世纪优秀人才支持计划)

Received 2006-05-16; Accepted 2007-01-24

信任管理[1−8]的基本思想是承认系统中安全信息的不完整性,系统的安全决策需要依靠可信任第三方提供附加的安全信息.随着大规模的分布式系统,如网格计算、普适计算、P2P 计算、Ad Hoc 网络等应用的深入研究,应用系统表现为由多个软件服务组成的动态协作系统.系统形态正从面向封闭的、熟识用户群体和相对静态的形式向开放的、公共可访问的和动态协作的服务模式转变.另外,在开放的分布式环境中,没有中心化的管理权威可以依赖,不能获得某一主体的全部信息,或者根本就不认识主体,这样,请求者有可能对授权者作出破坏性行为,因而产生了动态信任管理问题,为解决分布式环境中新应用形式的安全问题提供了新思路.

从社会学角度看,信任关系是最复杂的社会关系之一,是一个很难度量的抽象的心理认知,当实体之间的信任关系不能明确定义的时候,它也是不稳定的,给它的管理和评估带来了困难[5].信任也是与上下文相关的一个动态过程,随着时间的变化,实体之间的行为上下文可能会动态地变化,并且具有时间滞后性的特点,也就是说,新的信任关系的评估依赖于时间和行为上下文.信任关系的建模试图结合现实世界中实体(Agent)之间的主观(subjective)信任关系进行评估和预测信息网络中的信任关系[6].

近几年,一些学者开展了各种分布式应用中动态信任管理方面的研究工作.他们使用各种不同的数学方法和工具建立动态信任关系的模型,并取得了一些新的进展.本文综述了动态信任模型方面的研究进展.本文第 1 节分析动态信任关系的相关概念和主要问题.第 2 节总结动态信任关系的建模方法和动态信任管理的主要任务.第 3 节选取新的、典型的动态信任模型,根据其使用的数学方法进行分类评述,并进行各种算法的比较.第 4 节分析当前工作存在的问题并展望新的研究契机.第 5 节是结束语.

1 理解动态信任关系

1.1 信 任

综合各种不同的文献,首先给出与信任相关的一些描述性定义.

定义 **1**. 信任就是相信对方,是一种建立在自身知识和经验基础上的判断,是一种实体与实体之间的主观行为.信任不同于人们对客观事物的“相信(believe)”,而是一种主观判断,所有的信任本质上都是主观的,信任本身并不是事实或者证据,而是关于所观察到的事实的知识.

定义 **2**. 信任度(trust degree)就是信任的定量表示,也可以称为信任程度、信任值、信任级别、可信度等.

定义 **3**. 直接信任度(direct trust degree)表示在给定的上下文中,一个实体根据直接接触行为的历史记录而得出的对另外一个实体的信任程度.

定义 **4**. 间接信任度(indirect trust degree),表示实体间通过第三者的间接推荐形成的信任度,也叫声誉(reputation)、推荐信任度、反馈信任度等.

定义 **5**. 总体信任度(overall trust degree)是直接信任度和间接信任度的加权平均.

有非常多的文献采用不同的方法研究信任关系和信任关系的建模,这些研究主要分为 4 个方向:(1) 基于策略和凭证的信任关系(credential-based trust);(2) 通用模型的研究(general models of trust);(3) 基于声誉的信任关系(reputation-based trust);(4) Web 和信息资源中的信任关系(trust in websites and information sources).

1.2 信任的动态性

信任的动态性是信任评估和可信赖性预测的最大挑战[5].信任的动态性是由信任关系中的实体的自然属性决定的.在现实世界中,动态性(变化)既可以由实体的内因(endogenous factors,例如实体的心理、性格、知识、能力、意愿等)引起,也可以由实体的外因(exogenous factors,例如实体表现出的行为、策略、协议等)引起,但一个主体的内因很难由其他主体来判断和量化(即使非常有经验的心理学家也很难做到),而外因可以直接观察到,尽管非常模糊和不确定,但是可以进行预测、量化和推理,也可以管理它们.在信任关系中,某一时刻采样到的外因特征值,我们认为它是一个相对静态和稳定的量,采样的时间粒度决定了推理的准确程度.外因是内因的外部表现形式,可以间接地根据外因去评估内因.所以,实体的动态性是可以量化的(尽管是一个模糊的量).这种关系用图 1[5]进行说明:

图 1 说明了内因和外因决定的实体信任关系动态性和模糊性的 6 个重要性质[5]:

(1) Implicitness in trust(不确定性),是指随着上下文和时间的变化,主体(trustor)不能清楚地判断客体(trustee)的动态变化,只能根据以前的交互历史决定的声誉进行评估;

(2) Asymmetry in trust(不对称性),也就是信任的主观性,*A* 信任 *B* 不能等价于 *B* 也信任 *A*;

(3) Transitivity in trust(传递性),*A* 信任 *B*,*B* 信任 *C*,那么,*A* 通过 *B* 的推荐也可以信任 *C*;

(4) Antonym in context(反意性),实体之间对一些上下文的理解是完全反意的,例如,商业中的"卖"和"买"之间的信任关系;

(5) Asynchrony in time(异步性),是指实体之间的对信任关系的评估结果具有时间异步性,解决问题的办法是对时间槽进行平均;

(6) Gravity in relationship(严格性),是指实体之间的信任评价严格按照需求和规则去评判,以降低风险.

Fig.1 Fuzziness and dynamism nature of trust

图 1 信任的动态性和模糊性

2 动态信任关系建模与管理

2.1 动态信任关系的建模

信任的动态性决定了信任是一个随时间变化而进化(evolve)的关系,*A* 对 *B* 过去信任并不意味着现在和将来 *A* 对 *B* 的继续信任,*B* 的一些行为或者其他一些相关信息将导致 *A* 对 *B* 的信任进行重新评估.动态信任关系模型要能够反映出这种动态进化性,也要有信任随时间和上下文变化而重新评估的功能,动态的信任关系一般需要建立以下数学模型:

(1) 信任度空间(trust degree space)

首先要定义信任度的取值范围,这个空间一般是一个模糊逻辑定义的集合.例如,可以定义信任值为[0,1]上的值,也可以是[–1,1];既可以是连续的量,也可以是离散的整数值.

(2) 信任值的获取(acquirement of trust value)

一般要考虑两种方式的信任值获取方式:直接(direct)方式和间接(indirect)方式.在 Direct 方式中,信任关系是通过主体对客体自然属性的判断而直接建立的.当对另一个实体完全没有了解时,信任度设置成默认值(例如 0.5 或者 0);在 Indirect 方式中,通过第三方的推荐(recommend)建立信任关系和获取推荐的信任值,推荐信任值的获取要根据建立的推荐信任度计算的数学模型进行计算.

(3) 信任度的评估或者进化(trust value evaluation or evolution)

根据时间和上下文的动态变化进行信任度的动态更新,在每次交互后,主体 *A* 更新信任信息结构表中对主体 *B* 的信任值,如果一个交互是满意的,微调高直接信任值;如果交互不满意,微降低直接信任值.但在有些模型中,对信任度进行评估时,即使没有发生交互,信任者关于某一被信任者的信任度会随着时间的流逝而改变.

2.2 动态信任管理的主要任务

Blaze[1]将信任管理定义为采用一种统一的方法描述和解释安全策略(security policy)、安全凭证(security credential)以及用于直接授权关键性安全操作的信任关系.信任管理系统的核心内容是,用于描述安全策略和安全凭证的安全策略描述语言以及用于对请求、安全凭证集和安全策略进行一致性证明验证的信任管理引擎.动态信任管理的主要任务包括以下几个方面[7]:

(1) 信任关系的初始化(initializing a trust relationship)

主体和客体信任关系的建立,需要经历两个阶段:主体的服务发现阶段以及客体的信任度赋值和评估.当一个客体需要某种服务时,能够提供某种服务的服务者可能有多个,客体需要选择一个合适的服务提供者,这需要根据服务者的声誉(reputation)等因素来选择[8].

(2) 观测(observation)

监控主体间所有交互的影响,产生证据是动态信任管理的关键任务之一,信任的评估和决策依据在很大程度上依赖于观察者.信任值的更新需要根据观测系统的观测结果进行动态更新.主要有两个任务:实体之间交互上下文的观测与存储和触发信任值的动态更新.当一个观测系统检测到某个实体的行为超出了许可或者实体的行为是一个攻击性行为时,则需要触发一个信任度的重新评估.

(3) 信任评估(evolving trust)

根据数学模型建立的运算规则,在时间和观测到的证据上下文的触发下动态地进行信任值的重新计算,是信任管理的核心工作.实体 *A* 和实体 *B* 交互后,*A* 需要更新信任信息结构表中对 *B* 的信任值.如果这个交互基于推荐者的交互,主体 *A* 不仅要更新它对实体 *B* 的信任值,而且也要评估对它提供推荐的主体的信任值,这样,信任评估可以部分解决信任模型中存在的恶意推荐问题.

2.3 动态信任本体论(**ontology**)

Ontology 是描述概念及概念之间关系的概念模型,通过概念之间的关系来描述概念的语义.作为一种有效表现概念层次结构和语义的模型,Ontology 被广泛地应用到计算机科学的众多领域.Lea[9]通过对 10 年来的信任模型的研究总结,提出了一个综合的动态信任 Ontology.Lea 对一些信任模型根据它们采用的输入因子进行了分类,并取这些模型中输入因子的并集,提出如图 2 所示的 Ontology 模型.信任的主体称为 Trustor,信任的客体称为 Trustee.首先,Trustor 和 Trustee 之间的信任关系评估决定于 Trustor 的主观行为(action),而这种 action 具有其相关的一些行为属性,如,risk,benefit,importance 等,Trustor 利用上下文信息和历史数据进行信任的动态评估;其次,信任关系也依赖于双方的 competence 和 confidence;第三,一些第三方的信息,如声誉、凭证、推荐信息,也可以影响到信任的评估.

Fig.2 Dynamic trust ontology model

图 2 动态信任 ontology 模型

3 典型模型及其评述

许多学者研究各种分布式应用中的动态的信任关系,并使用不同的数学方法和工具建立了信任关系的模型.本节将根据其采用数学方法的不同,选取一些新的、典型的模型进行介绍和评述.

3.1 PTM (pervasive trust management model based on D-S theory)

PTM[10−12]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的域间的动态信任模型,主要采用改进的证据理论(D-S theory)的方法进行建模,信任度的评估采用概率加权平均的方法.PTM 中两个实体间的信任关系表示为 $R(A,B)=\alpha,\alpha\in[0,1]$.

$$\exists R(A,B)=\alpha|G(\alpha^{+}\rightarrow R(A,B)\geq\alpha)\wedge G(\alpha^{-}\rightarrow R(A,B)<\alpha).$$

信任度随着时间和行为上下文的变化而增减(α^{+}表示 positive actions,α^{-}表示 negative actions).

信任关系的初始化,通过 Direct 和 Indirect 两种方式.在 Direct 方式中,信任是通过主体对客体的直接判断而建立的,不需要 TTP,当对另一个实体完全没有了解时,信任度设置成默认值 0.5.在 Indirect 方式中,通过 Recommend 建立信任关系:(1) A 通过 B 的推荐建立对 C 的信任:$R(A,C)=R_B\cdot R(A,B)$;(2) 通过数字证书建立的信任 $R(A,C)=1$,因为传统 PKI(pubic key infrastructure)机制就是基于布尔逻辑,推荐的信任当然为 1.但当有 n 个 Recommender 时,要计算平均信任值

$$R(A,C)=\frac{1}{n}\sum_{i=1}^{n}R_{B_i}\cdot R(A,B_i).$$

信任度随着时间和行为上下文的变化而增减,使用如下模型计算更新后的信任度值 T_i:

$$T_i=\begin{cases}T_{i-1}+\omega\cdot V_{a_i}(1-T_{i-1}), & V_{a_i}>0\\ T_{i-1}(1-\omega+\omega\cdot V_{a_i}), & \text{Else}\end{cases},$$

其中,$V_{a_i}=W_{a_i}^{(m)}\cdot\frac{(\alpha^{+}-\alpha^{-})((\alpha^{+}-\alpha^{-})\cdot\delta)^{2m}}{(\alpha^{+}+\alpha^{-})((\alpha^{+}-\alpha^{-})\cdot\delta)^{2m}+1}$,$W_i$ 为某一次 action 的权重,δ为时间增量,常数 $m\geq1$ 为安全的级别(security level),严格因子(strictness factor)$\omega\in[0.25,0.75]$是一个手工配置的参数.

PTM 是较早研究普适环境下动态信任关系的模型,其主要优点是:

(1) 信任推导和进化的规则体现了一种严格的惩罚性.从计算公式可知,信任是得到困难、失去容易的值,因为 T_i 随着α^{+}的增加缓慢增长,但随着α^{-}的增加会迅速降低;(2) PTM 的信任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) 这是一个具体实现和应用的动态信任模型[12];(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 模型也存在明显的不足:

(1) 信任模型中使用固定信任域,不能适应不同应用背景下模型的不同需求;(2) 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;(3) 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.

3.2 Hassan's model (trust model based on vectors)

Hassan[13]等人提出了一种普适环境下基于向量机制的信任模型,P 对 Q 的信任度值 $t_{P,Q}\in[0,1]$.假设系统中共有 n 个实体 $Q_1,Q_2,\ldots,Q_n,Q_i$ 的信任度用向量定义为 $\vec{Q}_i=(t_{Q_iQ_1},t_{Q_iQ_2},\ldots,t_{Q_iQ_{i-1}},t_{Q_iQ_{i+1}},t_{Q_iQ_n})$.

当两个实体 Q_i,Q_k 之间初次交互时,$t_{Q_iQ_k}=null$.推荐的信任度定义为

$$PR_{Q_i,Q_j}=\begin{cases}\vec{C}_{Q_i,Q}\cdot\vec{C}_{Q,Q_j}/m, & S_{Q_i}\cap S_{Q_j}\neq\varnothing\\ 0, & S_{Q_i}\cap S_{Q_j}=\varnothing\end{cases},\ \text{其中,}\ \begin{matrix}\vec{C}_{Q_i,Q}=(t_{Q_i,Q_{k_1}},t_{Q_i,Q_{k_2}},\ldots,t_{Q_i,Q_{k_m}})\\ \vec{C}_{Q,Q_j}=(t_{Q_{k_1},Q_j},t_{Q_{k_2},Q_j},\ldots,t_{Q_{k_m},Q_j})\end{matrix}.$$

S_{Q_i} 为所有满足 $t_{Q_i,Q}\neq null$ 的实体集合,S_{Q_j} 为所有满足 $t_{Q_j,Q}\neq null$ 的实体集合,$m=|S_{Q_i}\cap S_{Q_j}|$.

随着时间和上下文的动态变化,综合历史记录等因素,根据下式计算信任度的更新值:

$$t_{Q_i,Q_j}=\frac{\omega_1(PR_{Q_i,Q_j})\left(\frac{CF_{Q_i,Q_j}+TF_{Q_i,Q_j}}{2}\right)+\omega_2(PI_{Q_i,Q_j})}{\sum_{i=1}^{2}\omega_i},$$

其中,CF 是信任因子,PI 是历史因子,TE 是时间因子[13],ω_1,ω_2 是平均算子.

Hassan 信任模型引入向量运算机制来描述信任关系,其主要优点是:

(1) 综合考虑自信任(confidence)、历史、时间等因子来反映信任关系动态性;(2) 该模型对于一些不确定性的因素进行了数学模型化,引入了信任因子、历史因子、时间因子等,这是它与其他模型相比最显著的特点;(3) 具有较好的动态适应能力,对恶意行为具有一定的敏感性和较强的抵御能力;(4) 模型尽管使用向量机制,但均为一些简单的算术运算,没有复杂的迭代计算,所以,模型具有较快的收敛速度和较好的可扩展性.

其不足主要是:(1) 不能解决实体之间为了相互之间的利益在推荐时进行欺骗的行为,它假设具有高信任度的推荐者不会提供不可靠的推荐信任;(2) 没有风险分析机制及建模风险和信任之间的关系;(3) 没有考虑服务者的声誉,推荐信任值的计算只相信邻居节点,这样,计算得到的信任度不能代表全局性.

3.3 George's model(trust model based on semiring)

George[14,15]等人提出了一种基于半环(semiring)代数理论[16]的信任模型.将信任问题定义为一个有向图 $G(V,E)$的路径问题,用节点代表实体,有向边代表信任关系,然后使用半环代数理论计算两个节点之间的信任值并进行信任评估.权重函数定义为 $l(i,j):V\times V\to S$, S 是观念空间(opinion space),表示为笛卡尔乘积 $S=[0.1]\times[0,1]$(如图 3 所示),trust(信任值)是一个估算值,confidence 是两个实体间经过多次交互后确立的准确和可靠的值,代表了信任的质量,在作请求实体是否可信判断时更为有用.

George's model 可以完成两个任务:(1) 可以完成一个实体对另一个实体 opinion space 的动态计算;(2) 求两个实体之间通信时的信任路径.半环代数理论可以用来求解有向图中的有向边和顶点值的聚合问题.半环的代数结构为$(S,\oplus,\otimes)$,S 是一个集合,$(\oplus,\otimes)$满足一系列操作属性的二元运算,在有向图中,$\otimes$操作可以用来求解一条路径上各个节点的推荐 opinion value 的聚合,$\oplus$操作可用来求两个实体之间多条路径上的 opinion 值的聚合.

利用半环求 opinion value:

$$(t_{ik},c_{ik})\otimes(t_{kj},c_{kj})\to\left(\frac{1}{\frac{1}{t_{ik}}+\frac{1}{t_{kj}}},c_{ik}c_{kj}\right),\ (t_{ij}^{p1},c_{ij}^{p1})\oplus(t_{ij}^{p2},c_{ij}^{p2})\to\left(\frac{c_{ij}^{p1}+c_{ij}^{p2}}{\frac{c_{ij}^{p1}}{t_{ij}^{p1}}+\frac{c_{ij}^{p2}}{t_{ij}^{p2}}},c_{ij}^{p1}+c_{ij}^{p2}\right),$$

其中,数对(t,c)为 opinion 的值.关于利用半环求信任路径问题,不是本文讨论的范畴,具体内容参见文献[14].

该模型的主要优点是:(1) 提出了一种新的信任关系建模方法——有向图的方法.借助于半环理论,可以计算请求实体的信任度的值,还可以计算得到一条实体之间最信任的路径,这对于两点之间进行可靠通信也是有用的;(2) 推荐信任度的计算使用多级的信任链的方式,能够较准确地反映全局的信任度.(3) 根据作者的模拟结果,在信任链的建立过程中能够较准确地区分诚实的实体和恶意的实体,说明模型具有较好的动态适应能力和较好的恶意行为检测能力.

有待完善之处是:(1) 没有明确讨论信任值的初始化问题,仅仅说明初始值由请求实体根据自己的标准给定,但请求实体一般会分配一个很高的 opinion(t,c),这样风险会很高;(2) 没有风险评估机制;(3) 对上下文基于时间的动态变化问题没有定义,也没有说明计算更新的时间间隔;(4) 信任链的方法建立聚合推荐信任度,信任链的跳数越多,计算的收敛速度越慢,可扩展性是该模型最大的挑战,所以 George 等人指出,该模型比较适合于小世界网络.

3.4 Sun's model (entropy-based trust model)

Sun[17,18]等人提出了一种基于熵(entropy)理论的信任模型,用 $T\{subject:agent,action\}$表示信任关系,$T\in[-1,1]$,用 $P\{subject:agent,action\}$表示 *agent* 从 *subject* 的观点来看可能对 *subject* 采取 *action* 的概率.基于熵

的信任值定义如下:

$$T\{subject:agent,actions\}=\begin{cases}1-H(p), & 0.5\le p\le 1\\ H(p)-1, & 0\le p\le 0.5\end{cases},$$

其中,$H(p)=-p\log_2(p)-(1-p)\log_2(1-p)$是熵函数,$p=P\{subject:agent,action\}$.推荐信任值的计算如下:

$$T_{ABC}=R_{AB}T_{BC} \tag{1}$$

或

$$T(A:C,action)=\omega_1(R_{AB}T_{BC})+\omega_2(R_{AD}T_{AD}) \tag{2}$$

其中,R_{AB} 表示推荐信任, $\omega_1=\dfrac{R_{AB}}{R_{AB}+R_{AD}},\omega_2=\dfrac{R_{AD}}{R_{AB}+R_{AD}}$,式(1)表示单路径推荐,式(2)表示多路径推荐(如图 4 所示).

信任度随着时间和行为上下文而变化,使用如下评估模型计算 *suject*:*A* 观察到 *agent*:*X* 执行 *action* 的概率:

$$P\{A:X,action\}=\frac{1+\sum\beta^{t_c-t_j}k_j}{2+\sum\beta^{t_c-t_j}N_j},$$

其中,t_j 为统计时间,$j=1,2,\ldots,I$,在时刻 t_j,*A* 统计到 *X* 执行 k_j 次 *action*,N_j 为要求执行 *action* 的次数,t_c 是当前时间,$0\le\beta\le1$ 是指遗忘因子(forgetting factor).

Sun's model 的主要优点是:(1) Sun 等人指出,信息理论中的熵具有表示信任关系不确定性的自然属性;(2) 使用该方法,推荐信任度的计算使用多级多路径的信任连的方式,能够较准确地反映全局的信任度;(3) 可以实现信任值的动态更新,模型具有较好的动态适应能力;(4) 可以进行可信路由的选择,也可以有效地检测和抵御恶意节点的攻击行为.

Sun's model 的不足之处是:(1) 在信任度动态更新的模型中,仅仅给出了一个示例,没有给出一个通用的数学模型;(2) 行为上下文的定义比较单一,也比较模糊,没有定义多 *action* 的情况;(3) 信任度评估模型缺少灵活的机制,如参数设置太单一;(4) 多级多层的信任链计算全局信任度,模型的具有较慢的计算收敛性,可扩展性是该模型的主要问题之一.

3.5 CBTM (a trust model cloud-based)

He[19]等人提出了一种普适环境下基于云模型(cloud model)[20]的信任模型 CBTM.该模型以云的形式,将实体之间信任关系的信任程度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

$$tc_{AB}=nc(Ex,En,He),0\le Ex\le1,0\le En\le1,0\le He\le1,$$

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.

实体间推荐信任度的计算.若实体间不信任,则 $Ex=0$;若实体间信任值不知道,则 $En=1,He=1$.假设有 *m* 个实体 $E_1,E_2,\ldots,E_m,E_i$ 对 E_{i+1} 的信任度为 $tc_i(Ex_i,En_i,He_i)$,那么,E_1 对于 E_m 的信任云 $tc(Ex,En,He)$通过下式来计算:

$$tc(Ex,En,He)=tc_1\otimes tc_2\otimes\cdots\otimes tc_m=\sum_{i=1}^{m}tc_i(Ex_i,En_i,He_i),$$

$$Ex=\prod_{i=1}^{m}Ex_i,En=\min\left(\sqrt{\sum_{i=1}^{m}En_i^2},1\right),He=\min\left(\sum_{i=1}^{m}He_i,1\right).$$

在开放网络环境中,众多实体间信任关系构成了一个信任网络,两个实体之间常存在多条信任路径.这样,在计算信任关系时,根据不同的信任路径就会得到多个信任云.这时,就需要将这些信任云合并成一个信任云.

$$tc(Ex,En,He)=tc_1\oplus tc_2\oplus\ldots\oplus tc_m=\prod_{i=1}^{m}nc_i(Ex_i,En_i,He_i),$$

$$Ex=\frac{1}{m}\prod_{i=1}^{m}Ex_i,En=\min\left(\frac{1}{m}\sum_{i=1}^{m}En_i,1\right),He=\min\left(\frac{1}{m}\sum_{i=1}^{m}He_i,1\right).$$

CBTM 首次提出的云信任模型是在开放网络环境中进行信任管理时的一种选择.其主要优点是:(1) 考虑了实体之间信任的不确定性,并以云的方式将信任程度和不确定程度结合起来,理论上更合理;(2) 推荐信任度采用多条信任链的方式进行聚合计算,能够得到较为准确的全局信任度;(3) 计算得到的信任链也是一条可信的路径,这对于两点之间进行可靠通信也是有用的.

其主要不足是:(1) 没有充分考虑普适环境下上下文的动态变化性,也没有引入时间粒度反映这种变化,模型还很粗糙;(2) 没有风险评估机制,也没有考虑协同欺骗和恶意节点的问题;(3) 没有初始信任值的计算方法;(4) 多条多级的信任链计算全局信任度,需要较多的时空开销,模型具有较慢的计算收敛性,影响了模型的可扩展性.

3.6 Dimitri's model (Bayesian dynamic trust model)

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,它可以解释为我们对不同可能性的信任程度.

Dimitri[21]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(如图 5 所示),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信任模型的需求.限于篇幅,详细原理此处不作介绍,请参见文献[21].

Fig.5 Kalman filter process for trust

图 5 Kalman 信任过滤过程

该模型的主要优点是:(1) Bayesian 推理的计算学习机制是将先验分布中的期望值与样木均值按各自的精度进行加权平均,精度越高者其权值越大.在先验分布为共扼分布的前提下,可以将后验信息作为新一轮计算的先验.用 Bayesian 定理与进一步得到的样本信息进行综合,多次重复这个过程后,上下文样本信息的影响越来越显著.所以,使用 Bayesian 方法建模信任的动态性有天然的优点;(2) 具有较好的动态适应能力,无论有无新的上下文被检测到,这个模型都会自动进化,这个恰当的数学工具非常适合于动态信任模型的需求.

该模型的不足之处是:(1) 没有具体定义影响信任动态性上下文信息,仅仅给出了一个简化的模型;(2) 没有说明信任值的初始化问题,如两个实体如何进行初次交互时信任如何建立;(3) 没有说明具体适用的环境;(4) 实现过滤器需要额外的时空开销,且运算比较复杂,在大规模的分布式环境下,可扩展性也是该模型的问题之一.

3.7 Song's model (trust model based on fuzzy-logic theory)

Song 等人[22]提出了一种网格环境下的实体之间基于模糊逻辑的动态信任模型(fuzzy-trust model),模型包括 3 个组成部分:信任的描述部分、信任关系的评估(模糊推理)部分和信任的进化(更新)部分.

在信任的描述部分定义了信任度的模糊逻辑表示方法.与前面介绍的大部分模型类似,信任值是一个集合[0,1]的元素,引入 3 个模糊的量来刻画网格中对某一实体(或者称为网格域)的信任关系:Γ 表示信任度(trust index),Φ表示任务成功率(job success rate),Δ表示入侵自我防御能力(intrusion defense capability).Γ由Φ和Δ根据一定的模糊推理规则确定:

$$\Gamma=fuzzy-inference(\Phi,\Delta).$$

模糊推理规则是根据网格中信任关系的需求提前定义的.

信任的进化(更新)部分给出了一个信任值Γ(即 t_{ij})动态更新的表达式:

$$t_{ij}^{new}=\alpha t_{ij}^{old}+(1-\alpha)s_{ij}\ .$$

权重因子$\alpha\in[0,1]$.对于安全级别要求较高的系统,取较小的α值;对安全级别要求较低的系统,α可以取较大的值.$s_{ij}=fuzzy-inference(\Phi,\Delta)$表示根据$\Phi$和$\Delta$的动态变化,由推理规则计算得到的信任值的增量.

在众多的基于网格的信任模型中,Song 的模型是比较典型的,主要优点是:(1) 不但使用模糊逻辑建立了信任的模糊推理规则,也研究了当网格环境动态变化时信任动态更新模块;(2) 将Φ(任务成功率)和Δ(入侵自我防御能力)作为输入因子引入信任的决策过程,符合网格计算中任务指派和自我保护的本质需求;(3) 在信任的更新部分,既考虑了动态信任值新的证据的产生,也考虑了历史因素,这符合动态信任关系的基本特点;(4) 模型具有较好的恶意实体的检测能力与抵御能力.

其不足之处是:(1) 对实体行为的时间变化性考虑较少,没有讨论模型随着时间的变化如何更新,所以,模型的动态适应能力值得商榷;(2) 模糊推理规则在系统建模上本身的发展问题,例如,建立较为复杂的推理过程需要较大的系统开销,影响了计算的收敛性和系统的可扩展性;(3) 没有考虑间接信任值的计算问题,所以,该模型计算得到的信任值是一种直接信任值,不能反映信任值的全局可信性,是模型需要继续完善的地方之一.

3.8 Claudiu's model (reinforcement learning model)

Claudiu 等人[23]提出了一种 P2P 环境下基于机器学习中强化学习[24]方法的动态信任模型.信任度的取值范围也是采用集合[0,1].与其他 P2P 信任模型显著不同的是,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,节点 a 对 b 基于连续时间戳的近期信任 $st_{n+1}(a,b)$定义为强化学习的模型:

$$st_{n+1}(a,b)=\begin{cases}st_n(a,b)+\alpha\times rt(a,x)(e_{n+1}(x,b)-st_n(a,b)), & \text{if } e_{n+1}(x,b)-st_n(a,b)\geq-\varepsilon\\ st_n(a,b)+\beta\times rt(a,x)(e_{n+1}(x,b)-st_n(a,b)), & \text{otherwise}\end{cases},$$

其中,$\alpha,\beta\in[0,1]$,$st_1(a,b),st_2(a,b),\ldots,st_{n-1}(a,b),st_n(a,b),st_{n+1}(a,b)$是基于连续时间帧 a 对 b 的信任评价,$rt(a,x)*e(x,b)$表示推荐信任,α和β分别为信任增加或者减少的学习因子.参数$\varepsilon>0$ 规定了交互满意度评价时误差容忍范围.如果交互的评价潜在地受噪音的影响,那么较高的学习因子会使信任评价产生较大的偏差.

长期信任定义为

$$lt_{n+1}(a,b)=\frac{w_s(n+1)}{n+1}\left[\frac{n}{w_s}lt_n(a,b)+rt(a,x_i)e_{n+1}(x_i,b)\right],$$

其中,$w_s(n)=n/\max(n,n_{\min})$反映了计算长期信任时,时间戳 n 的个数太小不能反映出长期的历史累积信任.

惩罚因子定义为

$$pt_n(a,b)=\frac{macc_n(a,b)}{c+macc_n(a,b)},$$

其中,$macc_n(a,b)$表示累积的交互失败的次数,正常数 c 控制着惩罚因子趋向于 1 的速度.

信任度聚合函数定义为

$$t_n(a,b)=\min(st_n(a,b),lt_n(a,b)).$$

惩罚因子集成于近期信任、长期信任之中,即 $lt_n(a,b)=lt_n(a,b)(1-pt(a,b))$和学习因子$\alpha=\alpha(1-pt(a,b))$.

该模型的主要优点是:(1) 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,通过反馈控制机制,动态调节计算节点的信任值的上述参数;(2) 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;(3) 对新发生的交互行为有足够的敏感性,提高了信任模型的动态适应能力;(4) 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.

该模型的不足之处是:(1) 只根据邻居节点的推荐计算推荐信任值,计算得到的是一种局部信任度,影响了信任评估的准确性;(2) 信任度取短期信任和长期信任中的最小值,虽然有利于安全性的提高,但这也限制了模

型的服务范围,许多节点的服务请求由于近期的一些误操作而会被拒绝,为了提高模型的适应能力,需要进一步改进.

3.9 各种模型的比较

表 1 是对本节介绍的算法的比较,指标 1~11 是根据 Lea[9]等人的信任本体论进行的各种输入因子的比较,指标 12~14 是模型所使用数学方法、应用环境和适用环境的比较.模型在计算推荐者信任值时,要么只询问少数的邻居计算局部信任值,要么通过信任链在整个系统中进行全局信任值计算.只询问少数实体计算得到的信任值不能反映信任值的准确性,在用信任链计算全局信任值时,收敛性是最大的挑战.因此,我们增加了指标 15(准确性:veracity)和指标 16(可扩展性:scalability).另外,一个好的信任模型能够在复杂的动态环境中继续提供稳定的服务,能够抵御恶意实体的攻击和预防协作欺骗行为的发生,所以增加了指标 17(健壮性:robustness)的比较.

Table 1 Comparison of representative work on dynamic trust model

表 1 典型动态信任模型的比较

	Model	PTM	Hassan	George	Sun	CBTM	Bayesian	Song	Claudiu
1	Dynamic evaluation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2	Context aware	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3	Risk evaluation	No	No	No	No	No	No	No	No
4	Reputation evaluation	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
5	Implementation	Yes	No	No	No	No	No	No	No
6	Strictness factor	Yes	No	No	No	No	No	No	Yes
7	Confidence aware	No	Yes	Yes	No	No	No	No	No
8	History awareness	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
9	Third party awareness	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
10	Action aware	Yes	No	No	Yes	No	No	Yes	Yes
11	Feedback-Protocol	Yes	No	Yes	No	No	No	Yes	No
12	App	Pervasive	Pervasive	Ad hoc	Ad hoc	Pervasive	unknown	Grid	P2P
13	Arith-Method	D-S	Vectors	Semiring	Entropy	Cloud-based	Bayesian	Fuzzy-logic	Machine learning
14	Decentralized	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
15	Veracity	Good	Better	Better	Low	Better	Good	Low	Low
16	Scalability	High	High	Lower	Low	Low	Low	Higher	Lower
17	Robustness	Good	Good	Lower	Better	Medium	Better	Lowest	Best

4 存在的问题及展望

4.1 当前研究存在的问题

动态信任模型目前的研究还处于起始阶段,存在一些明显的问题:

(1) 信任关系定义的混乱性.信任关系是最复杂的社会关系之一,也是一个非常主观化的心理认知,是一个实体的主观决定.对“信任”也还没有统一的定义,各种模型各自提出了信任的定义,甚至它们所使用的语言词汇也各不相同.虽然一些学者也努力提出一些所谓 universal definition,但都还没有被广泛接受.

(2) 信任模型的多样性.各种模型都是基于不同的应用背景提出来的,例如,分布式环境下的信任模型强调动态性和不确定性;而电子商务中的信任模型强调交互双方的互信.所以,不同的应用提出了不同的信任模型.

(3) 模型性能的评价困难.对于一个模型的性能优于其他模型的评价是一个非常困难的工作,在我们介绍的以上模型中,模型性能的评价大多采用模拟实验的办法进行功能的评价,而没有进行实际性能的评测.

(4) 模型的实现问题.在以上介绍的动态信任模型中,仅有 PTM 实现了一个原形模型,在访问控制和服务发现中进行了一些应用,其他模型都没有说明实现问题.

(5) 从表 1 可以看出,这些模型大多没有综合考虑各种可能的输入因子.例如,大多数模型没有风险机制,没有考虑服务者的声誉,不能很好地消除恶意推荐对信任评估的影响,没有解决初始信任值如何获得的问题等等.

4.2 展 望

结合第 4.1 节中提出的问题,我们认为在分布式环境下动态信任关系建模中,可以在以下几个方面做进一步的工作:

(1) 进一步研究信任关系,尤其是动态信任关系的相关性质、信任的表述和度量的合理性.这对信任关系的建模是非常重要的,也是信任关系建模的基础.

(2) 通用信任模型的研究.通过比较研究发现,在某些相似的应用系统中,信任关系具有相似性.将适用于某一具体系统信任模型扩展到某一类系统的信任模型,例如从 P2P 到分布式系统.

(3) 信任模型的评价问题.如何对众多的信任模型进行客观的性能评测也是一个值得研究的方向.Michael[25]等人设计了一个实验情景对一些信任模型的更新算法进行了比较研究;Karen 等人[25]介绍了一些信任模型测试的相关概念.

(4) 在以上介绍的各种动态信任模型中,仅有 PTM[10−12]实现了一个原形模型,其他模型还没有讨论实现的问题.再者,各种模型提出了复杂的数学推导和计算过程,这些模型在实现时,复杂度也是一个需要继续讨论的问题.

(5) 结合其他学科的知识,如机器学习、人工智能等,继续探索适合描述动态信任关系的新模型.

5 结束语

10 年来,信任、信任模型、信任管理系统的研究从 PKI 中集中式的信任关系到分布式的信任关系、从静态的信任模型到动态的信任模型、从比较单一的输入因子模型到多输入因子模型[9]、从证据理论模型到多种数学模型的提出,可以说,信任关系的研究是非常活跃的一个方向.通过本文可以看出,动态信任模型的研究工作还处于起始阶段,还需要研究工作者的继续努力.

References:

[1] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management. In: Proc. of the 1996 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society Press, 1996. 164−173. http://doi.ieeecomputersociety.org/10.1109/SECPRI.1996.502679

[2] Weeks S. Understanding trust management systems. In: Proc. of the 2001 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society Press, 2001. 94−105.

[3] Xu F, Lü J. Research and development of trust management in Web security. Journal of Software, 2002,13(11):2057−2064 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/13/2057.pdf

[4] Yuan SJ. The research on key technologies of trust management [Ph.D. Thesis]. Shanghai: Fudan University, 2004 (in Chinese with English abstract).

[5] Chang E, Thomson P, Dillon T, Hussain F. The fuzzy and dynamic nature of trust. LNCS 3592. Berlin: Springer-Verlag, 2005. 161−174.

[6] Koutrouli E, Tsalgatidou A. Reputation-Based trust systems for P2P applications:design issues and comparison framework. LNCS 4083, 2006. 152−161.

[7] Ruohomaa S, Kutvonen L. Trust management survey. LNCS 3477. Berlin: Springer-Verlag, 2005. 77−92.

[8] Song S, Hwang K, Zhou R, Kwok YK. Trusted P2P transactions with fuzzy reputation aggregation. IEEE Internet Computing, 2005, 9(6):24−34.

[9] Viljanen L. Towards an ontology of trust. LNCS 3592. Berlin: Springer-Verlag, 2005. 175−184.

[10] Almenarez F, Marin A, Diaz D, Sanchez J. Developing a model for trust management in pervasive devices. In: Bob Werner, ed. Proc. of the 3rd IEEE Int'l Workshop on Pervasive Computing and Communication Security (PerSec 2006). Washington: IEEE Computer Society Press, 2006. 267−272.

[11] Almenarez F, Marin A, Campo C, Garcia RC. PTM: A pervasive trust management model for dynamic open environments. In: Proc. of the 1st Workshop on Pervasive Security, Privacy and Trust. Boston, 2004. http://jerry.c-lab.de/ubisec/publications/PSPT04_PTM.pdf

[12] Almenarez F, Marin A, Campo C, Garcia RC. TrustAC: Trust-Based access control for pervasive devices. LNCS 450. Berlin: Springer-Verlag, 2005. 225−238.

[13] Jameel H, Hung LX, Kalim U, Asjjad A, Lee SY, Lee YK. A trust model for ubiquitous systems based on vectors of trust values. In: Proc. of the 7th IEEE Int'l Symp. on Multimedia. Washington: IEEE Computer Society Press, 2005. 674−679.

[14] Theodorakopoulos G, Baras JS. On trust models and trust evaluation metrics for ad-hoc networks. IEEE Journal on Selected Areas in Communications, 2006,24(2):318−328.

[15] Theodorakopoulos G. Distributed trust evaluation in ad-hoc networks [MS Thesis]. 2004. http://www.isr.umd.edu/~baras/publications/dissertations/2004/Theodorakopoulos_MS_2004-2.pdf

[16] Sun Y, Yu W, Han Z, Liu KJR. Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE Journal on Selected Areas in Communications, Selected Areas in Communications, 2006,249(2):305−319.

[17] Sun Y, Yu W, Han Z, Liu KJR. Trust modeling and evaluation in ad hoc networks. In: Proc. of the Global Telecommunications Conf., Globecom 2005. Washington: IEEE Computer Society Press, 2005. 1−10.

[18] He R, Niu JW, Zhang GW. CBTM: A trust model with uncertainty quantification and reasoning for pervasive computing. LNCS 3758. Berlin: Springer-Verlag, 2005. 541−552.

[19] Li DY, Meng HJ, Shi XM. Membership clouds and membership clouds generator. Journal of Computer Research and Development, 1995,32(6):15−20 (in Chinese with English abstract).

[20] Melaye D, Demazeau Y. Bayesian dynamic trust model. LNCS 3690. Berlin: Springer-Verlag, 2005. 480−489.

[21] Song SS, Hwang K. Fuzzy trust integration for security enforcement in grid computing. In: Proc. of the Int'l Symp. on Network and Parallel Computing (NPC 2004). LNCS 3222, Berlin: Springer-Verlag, 2005. 9−21.

[22] Duma C, Shahmehri N. Dynamic trust metrics for peer-to-peer system. In: Proc. of the 16th Int'l Workshop on Database and Expert Systems Applications (DEXA 2005). Washington: IEEE Computer Society Press, 2005. 776−781.

[23] Kaelbling LP, Littman ML, Moore AW. Reinforcement learning: A survey. Journal of Artificial Intelligence Research, 1996,4: 237−285.

[24] Kinateder M, Baschny E, Rothermel K. Towards a generic trust model—Comparison of various trust update algorithms. In: Proc. of the iTrust 2005. LNCS 3477, 2005. 177−192.

[25] Fullam KK, Sabater-Mir J, Barber KS. A design foundation for a trust-modeling experimental testbed. LNAI 3577. Berlin: Springer-Verlag, 2005. 95−109.

附中文参考文献:

[3] 徐锋,吕建.Web 安全中的信任管理研究与进展.软件学报,2002,13(11):2057−2064. http://www.jos.org.cn/1000-9825/13/2057.htm

[4] 袁时金.信任管理关键技术研究[博士学位论文].上海:复旦大学,2004.

[19] 李德毅,孟海军,史雪梅.隶属云和隶属云发生器.计算机研究与发展,1995,32(6):15−20.

李小勇(1975－),男,甘肃天水人,讲师,主要研究领域为网络安全,网络协议.

桂小林(1966－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为网格计算,网络安全,软件容错.