基于模糊集合理论的主观信任管理模型研究*

唐 文+, 陈 钟

(北京大学 计算机科学技术系,北京 100871)

Research of Subjective Trust Management Model Based on the Fuzzy Set Theory

TANG Wen+, CHEN Zhong

(Department of Computer Science and Technology, Peking University, Beijing 100871, China)

+Corresponding author: Phn: 86-10-62765807, E-mail: tangwen@infosec.pku.edu.cn

http://infosec.pku.edu.cn

Received 2003-01-18; Accepted 2003-03-20

Tang W, Chen Z. Research of subjective trust management model based on the fuzzy set theory. *Journal of Software*, 2003,14(8):1401~1408.

http://www.jos.org.cn/1000-9825/14/1401.htm

Abstract: Trust management model is fundamental for information security in open networks. The fuzzy nature of subjective trust is considered, and the fuzzy set theory has been used to model the issues of trust management. The formalized valuation of subjective trust is given, the definition of trust class and the evaluation of trust are discussed, derivation rules of trust relationships are presented and a subjective trust management model is provided. The formal model proposed in this paper provides a new valuable way for studying trust management in open networks.

Key words: trust management; subjective trust; trust vector; trust class; trust derivation

摘 要: 在开放网络环境中,信任管理模型是信息安全的重要前提与基础.考察了主观信任的模糊性,运用模糊集合理论对信任管理问题进行了建模,给出了信任类型的定义机制和信任的评价机制,定义了主体信任的形式化表示,并提出了信任关系的推导规则,构造了一个完整的主观信任管理模型,为开放网络环境中的信任管理研究提供了一个有价值的新思路.

关键词: 信任管理;主观信任;信任向量;信任类型;信任推导

中图法分类号: TP301 **文献标识码**: A

现有的安全技术,无论是密码算法和协议,还是更高层次的安全模型和策略,都隐含地与信任相关,或者预先假定了某种信任前提,或者目的是为了获得或创建某种信任关系.所以,信任管理作为网络安全技术的重要前提与基础,正日益成为网络安全研究的焦点.

1996 年,M.Blaze 等人首先提出了信任管理的概念[1],并在此基础上发展出了相应的信任管理系统 PolicyMaker[1]和 KeyNote[2].文献[3]将信任分为直接信任和推荐信任,以对实体完成任务的期望为基础,根据肯定经验和否定经验计算出实体能够完成任务的概率,以此概率作为实体信任度的度量,并给出了信任推导和综合的规则和相应的信任度计算方法.但该模型的不足之处在于,简单地用概率模型对主观信任进行建模,实际上

* 第一作者简介: 唐文(1974－),男,湖南永州人,博士生,主要研究领域为网络与信息安全.

是将信任的主观性和不确定性等同于随机性;在对多个推荐信任进行综合时,简单地采用了取均值的方法,因而无法反映信任关系的真实情况.

此外,A.Jøsang 提出了基于主观逻辑(subjective logic)[4]的信任模型[5,6],引入证据空间(evidence space)和观念空间(opinion space)的概念来描述和度量信任关系,以描述二项事件后验概率的 Beta 分布函数为基础,给出了一个由观察到的肯定事件数和否定事件数来确定的概率确定性密度函数,并以此为基础计算实体产生每个事件的概率的可信度.A.Jøsang 还定义了一组可用于信任度计算的逻辑算子.Jøsang 模型实际上也认为信任的主观性和不确定性与随机性是等同的.但主观信任作为一种认知现象,其主观性和不确定性主要表现为模糊性,而对主观信任进行形式化研究的主要困难也在于如何对这种模糊性进行建模.文献[7]比较全面地介绍了目前国际上信任管理研究的现状.

目前,信任研究中所讨论的信任实际上包括两种相互关联的信任关系:一种是对客体(如标识、证书等)的信任,为了区别起见,本文称其为相信关系.相信关系是基于证据的,所以可以精确地描述、推理和验证.另一种信任是主体之间的信任,本文称其为主观信任,或简称信任.主体是指由人或由人和客体的混合体所构成的个体或群体.主观信任(或简称信任)是一种人类的认知现象,是对主体的特定特征或行为的特定级别的主观判断,而这种判断是独立于对主体特征和行为监控的.主观信任是相信关系的重要前提和基础,它本质上是基于信念的,具有很大的主观性、模糊性,无法精确地加以描述和验证.文献[3~6]对主体间的非理性的信任关系进行了有益的探索,但这些研究仍然采用的是精确的数学模型,因而无法处理主观信任本身所具有的模糊性.

1 信任管理研究的内容

为了着重于本文的研究内容,我们假设通过采用相应的安全技术,信任管理模型中主体的身份鉴别、信任信息的完整性和机密性都已得到了保障.

对主体信任进行建模的目的是为了形式化地研究在开放网络中人们是如何对其他主体的信任度进行定义、评价和推导的.所以信任管理研究的内容应当包括信任的定量描述机制、信任类型的定义机制、信任的评价机制、信任关系的形式化表示及推导机制.

2 主体信任的定量描述

对主观信任进行研究,远比对客体之间的相信关系进行研究要复杂得多.主体间的信任由于涉及到对其他主体的主观认识,具有模糊性,因而无法用常规的精确逻辑来描述和处理.所以,在信任研究中需要寻求一种既能反映主体信任的模糊性,又具有直观、简洁语义的定量描述机制.

L.A.Zadeh 首先提出了模糊理论[8].模糊理论将数学研究的对象扩大到质与量统一的对象和具有模糊性的概念.所以,本文将模糊集合理论引入到信任管理研究中,以解决对具有模糊性的主观信任进行建模的问题.

设 $X=\{x_0,x_1,\ldots,x_n\}$为信任管理所研究的问题域,其中 $x_i(i=1,2,\ldots,n)$表示开放网络环境中的主体.

定义 1. 设论域为非空集合 X,x 为 X 中的元素,对于任意的 $x\in X$ 给定了如下映射:

$$X\to[0,1],x\mapsto \mu_A(x)\in[0,1],$$

则称如下由序偶组成的集合 $A=\{(x|\mu_A(x))\},\forall x\in X$ 为 X 上的模糊子集合(简称模糊集合).称$\mu_A(x)$为 x 对 A 的隶属函数(也可表示为 $A(x)$).对某个具体的 x 而言,称$\mu_A(x)$为 x 对 A 的隶属度.

X 上的一切模糊集的集合记为$\mathcal{F}(X)$.

用多个模糊子集合 $T_j\in\mathcal{F}(X)(j=1,2,\ldots,M)$定义具有不同信任度的主体集合(简称信任集合).即用离散的标度 $\{1,2,\ldots,M\}$来描述主体信任的高低.同时,采用自然语言对 T_j 命名,可以赋予其直观、实际的意义.如当 $M=6$ 时,可以定义 T_j 的意义如下:

- T_6:表示“完全信任”子集合;
- T_5:表示“非常信任”子集合;
- T_4:表示“很信任”子集合;

- T_3:表示“一般信任”子集合;
- T_2:表示“有点信任”子集合;
- T_1:表示“不信任”子集合.

在实际环境中,主体对某个 T_j 集合的隶属关系不能简单地用“真”或“假”来描述,而判断主体也往往无法明确地判断某个主体究竟是属于哪一个信任集合 T_j 的,也即各信任集合之间并不是非此即彼的排他关系.因此,用主体对各 T_j 的隶属度所构成的向量来描述主体的信任度更符合主体信任的实际情况.所以,x_0 对 x_i 的信任可以用信任向量 $V=\{v_0,v_1,\ldots,v_M\}$ 来表示,其中 v_j 表示 x_i 对 T_j 的隶属度.

信任向量或 x_i 对各 T_j 的隶属度可以通过两种途径获得,一种方法是采用模糊综合评判的方法,对信任关系的构成因素进行评价和综合,计算出 x_i 的信任向量;另一种方法则是通过对其他主体所提供的关于 x_i 的信任信息进行分析,推导出 x_i 的信任向量.

3 信任类型和信任的综合评判

3.1 信任类型

在开放网络中,特定的信任关系不是在任何情况下都成立的.所以在研究具体的信任关系时,需要定义信任关系所隶属的信任类型.文献[3]根据对认证协议进行信任研究的需要定义了 6 种信任类型.然而在实际中,仅仅定义有限的几种信任类型无法适应复杂多样的应用环境的需要的.所以在信任管理中,应当提出一种通用的信任类型定义机制,而所定义的信任类型的具体内容则可以由具体应用来决定.

在实际生活中,人们所考虑和处理的复杂概念,都可以分解为多个复杂度较低的次一级的概念,而这些次一级的概念又可以进一步分解为更简单的概念.这种分解过程可以持续下去,直到所讨论的概念已经足够简单,不需要再分解为止.最简单的概念称为属性.可以认为概念是由特定信息形成的组合,也即通过采用适当的算子、连接、规则或其他方法对原子的基本概念或属性进行聚合而建立起的关系模型.最低层所包含的属性能够由简单到复杂地逐步地聚合,直到构造出体系顶端的复杂概念.所以,概念可以采用树状的多级概念体系来描述.信任类型本质上也是一种主体的主观概念,因此信任类型的定义也可以采用与概念体系相似的树状结构来描述.这种信任类型的树状定义框架称为概念树.

概念树是由多个结点构成的集合,$CT=\{rn,mn_1,mn_2,\ldots,ln_1,ln_2,\ldots\}$,其中

- rn 为根结点,表示特定的信任类型,$rn=\{n,s,\lambda\}$,其中 n 为概念树的名字,即所定义的信任类型的名字;$s=\{1,2,\ldots,M\}$ 为对概念树的构成因素进行评价时所采用的评价尺度集,与主体信任度的标度相对应,它也分为 M 级;λ 为一个判定阈值,用于判断信任类型之间的差异.
- $mn_i=\{n,p,w_i\}$ 为中间结点,表示构成该信任类型的子因素,其中 n 为结点的名称;p 为当前结点的父结点;w_i 为结点的权重,并满足对具有相同父结点的所有子结点的权重 w_i 有 $\Sigma w_i=1$.
- $ln_j=\{n,p,w_j,F_j\}$ 为叶子结点,表示构成特定信任类型的最基本的因素(属性),其中 n 为结点的名称;p 为当前结点的父结点的名称;w_j 为结点的权重,对具有相同父结点的所有子结点也满足 $\Sigma w_j=1$;F_j 为特征函数,描述构成信任类型的最基本的属性的特征.

在现实中,具体属性的特征函数 F_j 可能会千差万别.但对于主体来说,过分强调精确性不仅不必要,而且在很多情况下也不可能.所以只要叶子结点所定义的属性足够基本,属性的特征就都可以近似地用某个特征变量的一元函数来描述.如果更进一步地研究实际的属性评价过程,可以发现主体对某个属性的评价实际上是一个分段函数,即当属性的特征在不同的取值范围内时,就对该属性作不同的评价.而当属性的特征在同一范围内变化时,并不影响对该属性所作的评价.所以,本文定义特征函数 F_j 为

$$F_j(x,y)=f_k(x),\quad a_{k-1}<y<a_k,\quad k=1,2,\ldots,n,$$

其中,$y\in[a_0,a_n]$ 为描述属性特征差异的特征变量,$a_k(k=0,1,2,\ldots,n)$ 为 y 的 n 个取值范围的边界,$x\in s$ 为评价的尺度,$f_k(x)$ 为评价函数.当属性的特征 y 在第 i 个范围内时,对该属性的评价就为 $f_k(x)$.

由于主体对属性特征的认识往往也带有模糊性,所以 $f_k(x)$ 表示对属性作各种(n 种)评价的可能性(或具体属

性对各评价集合的隶属度).$f_k(x)$可能是非常复杂的函数.但与特征函数 F_j 相类似,在此也同样不必过分强调 $f_k(x)$的精确性.所以本文统一采用梯形函数来描述 $f_k(x)$,

$$f_k(x)=\begin{cases}0, & x\le b_{k1}\\ \dfrac{x-b_{k1}}{b_{k2}-b_{k1}}, & b_{k1}\le x<b_{k2}\\ 1, & b_{k2}\le x<b_{k3}\\ \dfrac{b_{k4}-x}{b_{k4}-b_{k3}}, & b_{k3}\le x<b_{k4}\\ 0, & x\ge b_{k4}\end{cases},$$

其中,$b_{k1},b_{k2},b_{k3},b_{k4}\in s$.$f_k(x)$具体描述了对特定主体的属性作 $x(x\in s)$级评价的可能性(或该属性对 x 级的评价的隶属度).

特征函数 F_j 共有 $5n+1$ 个参数,可表示为

$$F_j=(a_0,a_1,a_2,\ldots,a_n,\ldots,b_{k1},b_{k2},b_{k3},b_{k4},\ldots),\quad k=1,2,\ldots,n.$$

在实际中,经常需要判断两个信任类型是否相同,此时所要做的就是比较它们对应的概念树的拓扑结构和结点参数是否相同.人们在比较两个复杂概念的时候,往往采用的也是一种带有模糊性的比较方法,并不要求两个概念精确地一致.所以在比较两个信任类型的概念树时,只要两个概念树之间的差异不超过根结点所定义的阈值λ,就认为它们实际上描述的是相同的信任类型,记为 $c_1\cong c_2$.

3.2 信任的综合评判

在将信任类型定义为概念树之后,以概念树为框架对主体的信任知识进行评价和综合,可以评判出主体的信任度(信任向量).这种评价的过程就是信任的综合评判.由于在多数情况下,构成信任的子因素也具有模糊性,所以对这种模糊性因素作出的综合评判,也称为模糊综合评判.模糊综合评判的理论基础是模糊变换[9].

当所讨论的信任类型的概念树的高度为 1(即该类信任直接由其基本属性聚合而成)时,评价该类信任的过程就是一个简单模糊综合评判的过程.在对信任的综合评判中,有 4 个基本要素:

(1) 因素集 $E=\{e_1,e_2,\ldots,e_n\}$;

(2) 评价集 $D=\{d_1,d_2,\ldots,d_M\}$;

(3) 因素评判矩阵 $R=(r_{ij})_{n\times M}$;

(4) 各因素的权重分配 $W=\{w_1,w_2,\ldots,w_n\}$.

因素集 E 包含的是构成信任类型的所有属性,即概念树的所有叶子结点.评价集 D 描述的是对特定主体的属性所作的不同等级的评价,评价的等级必为 M 级(与信任集合的等级相对应).从属性到评价的模糊关系 R 表示对各个因素 e_i 作各种评价的可能性.例如,r_{ij} 就表示对 e_i 作出 d_j 评价的可能性.在评判过程中,只要根据主体的具体情况确定属性的特征变量 y 的取值,就可以根据属性的特征函数 F 计算出对属性作各种评价的可能性,从而构造出因素评判矩阵 R.W 是一个权重分配,它表示各因素在评价中的相对重要性.对概念树来说,各个因素/属性的权重就是其所对应(叶子)结点的权重.评价的结果就是信任向量 $V=\{v_0,v_1,\ldots,v_M\}$.

按照模糊变换的原理,信任的简单模糊综合评判就是进行如下的模糊变换:

$$(v_0,v_1,\ldots,v_M)=(w_1,w_2,\ldots,w_n)\circ(r_{ij})_{n\times M},$$

其中"$\circ$"表示模糊变换,$v_j=\bigvee_{i=1}^{n}(w_i\wedge r_{ij})(j=1,2,\ldots,M)$,$\vee$和$\wedge$为 Zadeh 算子,分别表示 max 和 min 运算.

对于复杂的信任类型(多级概念树)来说,信任的综合评判所要考虑的因素很多,需要采用多层次综合评判对主体信任进行评价.由于概念树按照信任类型的内在结构将构成信任的子因素分类组成了多级结构,并指定了它们之间的权重分配,所以概念树就构成了信任的多层次综合评判的依据.在对根结点或中间结点进行综合评判时,可以将因素集 E 中的元素看成是低一层次的子因素或子结点,将因素评判矩阵 R 看成是对低一层的子因素进行简单综合评判所获得的评判向量的综合.而低一层次的简单综合评判,也可以是更低层次因素的综合.从概念树的叶子结点到根结点反复进行综合评判,最终可以评判出主体的信任向量 V.

只要概念树明确定义了信任类型的构成框架,信任的综合评判就可以根据该信任类型的概念树对主体的信任知识进行评价和度量,得到所评价的主体的信任度的描述.

4 信任关系的形式化表示

对每一种类型的信任来说都存在两种信任方式:直接信任和推荐(间接)信任.文献[3]提出了一种比较直观的信任表示方法.本文以此为基础,定义了直接信任和推荐信任的形式化表示.

直接信任:

$$P\ trusts\ {}^{\omega}_{c}\ Q\ value\ V. \tag{1}$$

式(1)表示主体 P(通过综合评判或信任推导)认为,就 c 类信任而言,主体 Q 的信任度(信任向量)为 V.c 为特定的信任类型.ω为直接信任向量 V 的合成权重.定义是ω因为 P 可能通过多种途径(综合评判或信任推导)得到了多个相同类型的关于 Q 的信任关系.但主体间的多重信任关系不利于形成一致的信任观点.所以 P 需要对这些信任关系进行综合,形成关于 Q 的单一的信任关系.但在信任关系的合成中,各信任关系的相对重要性一般来说是不同的.适当地定义合成权重ω的大小,可以在信任关系的合成中,反映出各信任关系的相对重要性.

推荐信任需要采取限制更严格的描述方式.

推荐信任:

$$P\ trusts\ {}^{\omega}_{c}.rec\ {}^{n}_{rc}\ Q\ \text{when}.path\ S_p\ \text{when}.target\ S_t\ value\ V. \tag{2}$$

式(2)表示主体 P 将以推荐信任度 V 接受主体 Q 提供的关于其他主体的 c 类的直接信任或推荐信任.与直接信任类似,ω为推荐信任向量 V 的合成权重,c 为特定的信任类型.n 为推荐的层数限制,当进行推荐的迭代(对推荐的推荐)时,n 限定了推荐的最大迭代次数.$S_t \subset X$,限定 P 只接受 Q 提供的关于 S_t 中主体的信任关系;S_p 中的元素的是主体的有序列表$(x_i,x_j,x_k,\ldots)$,每个列表描述一条合法的推荐路径.此外,rc 描述了推荐的内容类型或简称推荐类型.

定义 rc 是因为推荐信任实际上会随着所推荐的内容的不同而有所区别.当推荐的内容(直接信任或推荐信任)不同时,推荐信任所研究的推荐主体的能力也是不同的.同时,它们的信任向量的依据也不相同.所以,根据推荐内容的不同,或根据所讨论的推荐主体的能力的不同,推荐信任可以分为两类:

- 直接推荐(rd):表示推荐信任描述的是推荐主体对 c 类直接信任的判断能力,其推荐的内容为直接信任.与信任类型 c 相似,rd 也采用概念树来定义.在信任关系的推导中,这种推荐信任的后继信任关系必然是(同信任类型的)直接信任,所以有推荐层数 n=1.
- 推荐的推荐(rr):这种推荐信任描述的是推荐主体对 c 类推荐信任的判断能力,其推荐的内容为推荐信任.rr 也采用概念树结构来定义.在信任关系的推导中,这种推荐信任的后继信任关系必然是(相同信任类型的)推荐信任,所以推荐层数 n>1.

对于推荐信任来说,主体首先关心的是推荐主体在多大程度上有能力进行这种推荐,所以在对推荐信任进行综合评判时,应当以 rc 的概念树为基础对推荐主体进行评价.

5 信任关系的形式化推导

5.1 信任向量的运算

目前,在有关的模糊数学文献中,多数都采用 Zadeh 算子∧和∨作为模糊算子来进行分析和讨论.但这对算子的缺点是比较粗糙,丢失的信息太多.对此,人们相继提出了多种新的广义模糊算子[10].本文选择 Einstein 算子作为模糊算子[10].

定义 2. 设模糊集合 $A,B\in\mathcal{F}(X)$,则 Einstein 算子 $\overset{\bullet}{\varepsilon}$ 和 $\overset{+}{\varepsilon}$ 的定义如下

$$(A\cap B)(x)=A(x)\overset{\bullet}{\varepsilon}B(x)=\frac{A(x)B(x)}{1-(1-A(x))(1-B(x))},\ (A\cup B)(x)=A(x)\overset{+}{\varepsilon}B(x)=\frac{A(x)+B(x)}{1+A(x)B(x)},$$

其中 $A(x)$和 $B(x)$分别表示 $x\in X$ 对模糊集合 A,B 的隶属度.

在信任的形式化推导过程中,需要对信任向量进行运算.本文定义了两种信任向量的运算:连接(join)和合并(union).

定义 3. 设 $V_1=\{v_1^1,v_2^1,...,v_M^1\}$,$V_2=\{v_1^2,v_2^2,...,v_M^2\}$为信任向量,则 V_1 与 V_2 的连接与合并运算的定义如下:

(1) 连接: $V=V_1\odot V_2\Leftrightarrow V=\{v_0,v_1,\ldots,v_M\}=\{v_1^1\overset{\bullet}{\varepsilon}v_1^2,v_2^1\overset{\bullet}{\varepsilon}v_2^2,...,v_M^1\overset{\bullet}{\varepsilon}v_M^2\}$.

(2) 合并: $V=V_1\oplus V_2\Leftrightarrow V=\{v_0,v_1,\ldots,v_M\}=\{v_1^1\overset{+}{\varepsilon}v_1^2,v_2^1\overset{+}{\varepsilon}v_2^2,...,v_M^1\overset{+}{\varepsilon}v_M^2\}$.

其中,$\overset{\bullet}{\varepsilon}$ 和 $\overset{+}{\varepsilon}$ 为 Einstein 算子.

5.2 信任关系的推导规则

与信任向量的连接和合并运算相对应,信任关系(直接信任和推荐信任)之间也存在推演(deduction)和合意(consensus)两种推导规则.

推演规则定义的是信任通过推荐沿信任链传递的机制.对于相同类型的信任关系来说,当有推荐发生时,推演规则可以将推荐信任及其推荐的内容(另一信任关系)连接起来,构成一个新的信任关系.

推演规则. 设 $x_i,x_j,x_k\in X$,在 x_i 与 x_j 之间存在推荐信任关系 TP_1,而在 x_j 与 x_k 之间存在信任关系 TP_2,TP_2 是直接信任或推荐信任.那么就可以定义推演规则:

对 TP_2 为推荐信任的情形,有

TP_1: x_i *trusts* $\overset{\omega_1}{c_1}$ *.rec* $\overset{n_1}{rc_1}$ x_j when.*path* S_{p1} when.*target* S_{t1} *value* V_1

$\wedge TP_2$: x_j *trusts* $\overset{\omega_2}{c_2}$ *.rec* $\overset{n_2}{rc_2}$ x_k when.*path* S_{p2} when.*target* S_{t2} *value* V_2

$\wedge c_1\cong c_2$

$\wedge n_1>n_2\geq 1$

$\wedge(((rc_1,rc_2 \text{ is } rr)\wedge(rc_1\cong rc_2))\vee((rc_1 \text{ is } rr)\wedge(rc_2 \text{ is } rd)))$

$\wedge(\exists p\in S_{p2},(x_j,p)\in S_{p1})$

$\Rightarrow TP$: x_i *trusts* $\overset{\omega_1}{c_1}$ *.rec* $\overset{\min(n_1-1,n_2)}{rc}$ x_k when.*path* $(\{p|\forall(x_j,p)\in S_{p1}\}\cap S_{p2})$ when.*target* $(S_{t1}\cap S_{t2})$ *value* $(V_1\odot V_2)$

其中,若 rc_1,rc_2 都为推荐的推荐(*rr*),则 *rc* 也为 *rr*;若 rc_1 为推荐的推荐(*rr*),rc_2 为直接推荐(*rd*),则 *rc* 为 *rd*.

对 TP_2 为直接信任的情形,有

TP_1: x_i *trusts* $\overset{\omega_1}{c_1}$ *.rec* $\overset{n_1}{rc_1}$ x_j when.*path* S_{p1} when.*target* S_{t1} *value* V_1

$\wedge TP_2$: x_j *trusts* $\overset{\omega_2}{c_2}$ x_k *value* V_2

$\wedge c_1\cong c_2$

$\wedge n_1=1$

$\wedge rc_1$ is *rd*

$\wedge x_k\in S_{t1}$

$\wedge(x_j)\in S_{p1}$

$\Rightarrow TP$: x_i *trusts* $\overset{\omega_1}{c_1}$ x_k *value* $(V_1\odot V_2)$

合意规则定义的是对主体间的多重信任关系进行综合的方法.当两个主体之间存在多重信任关系时,运用合意规则可以将各信任关系综合起来,构成一个新的信任关系.

合意规则. 设 $x_i,x_j\in X,x_i$ 与 x_j 之间存在 m 个(直接或推荐)信任关系 $TP_1,TP_2,\ldots,TP_m$,那么就可以定义合意规则:

对 $TP_1,TP_2,\ldots,TP_m$ 为推荐信任的情形,有

TP_1: x_i *trusts* $\overset{\omega_1}{c_1}$ *.rec* $\overset{n_1}{rc_1}$ x_j when.*path* S_{p1} when.*target* S_{t1} *value* V_1

$\wedge TP_2$: x_i *trusts* $\overset{\omega_2}{c_2}$ *.rec* $\overset{n_2}{rc_2}$ x_j when.*path* S_{p2} when.*target* S_{t2} *value* V_2

$\wedge\ldots$

$\wedge TP_m$: x_i $trusts$ $\overset{\omega_m}{c_m}$ .rec $\overset{n_m}{rc_m}$ x_j when.$path$ S_{pm} when.$target$ S_{tm} $value$ V_m

$\wedge c_1 \cong c_2 \cong \ldots \cong c_m$

$\wedge rc_1 \cong rc_2 \cong \ldots \cong rc_m$

$\Rightarrow TP$: x_i $trusts$ $\overset{\omega=f(\omega_1,\omega_2,\ldots,\omega_m)}{c}$ .rec $\overset{n=\max\{n_1,n_2,\ldots,n_m\}}{rc}$ x_j when.$path$ $(S_{p1} \cup S_{p2} \cup \ldots \cup S_{pm})$

when.$target$ $(S_{t1} \cup S_{t2} \cup \ldots \cup S_{tm})$ $value$ $(\omega'_1 V_1 \oplus \omega'_2 V_2 \oplus \ldots \oplus \omega'_m V_m)$

其中,新的合成权重 $f(\omega_1,\omega_2,\ldots,\omega_m)$可以为均值函数:

$$f(\omega_1,\omega_2,\ldots,\omega_m)=\frac{1}{m}\sum_{k=1}^{m}\omega_k .$$

如果合成权重$\omega_1,\omega_2,\ldots,\omega_m$的最大值为$\omega_l$,则 TP 的信任类型 c 和推荐类型 rc 取 $c=c_l$,$rc=rc_l$(与 TP_l 相同).信任向量的合并权重 $\omega'_k=\omega_k \Big/ \sum_{l=1}^{m}\omega_l$ (k=1,2,…,m)体现了各信任向量的相对重要性.

对 $TP_1,TP_2,\ldots,TP_m$ 为直接信任的情形,有

TP_1: x_i $trusts$ $\overset{\omega_1}{c_1}$ x_j $value$ V_1

$\wedge TP_2$: x_i $trusts$ $\overset{\omega_2}{c_2}$ x_j $value$ V_2

$\wedge \ldots$

$\wedge TP_m$: x_i $trusts$ $\overset{\omega_m}{c_m}$ x_j $value$ V_m

$\wedge c_1 \cong c_2 \cong \ldots \cong c_m$

$\Rightarrow TP$: x_i $trusts$ $\overset{\omega=f(\omega_1,\omega_2,\ldots,\omega_m)}{c}$ x_j $value$ $(\omega'_1 V_1 \oplus \omega'_2 V_2 \oplus \ldots \oplus \omega'_m V_m)$

其中,$f(\omega_1,\omega_2,...,\omega_m)$及 ω'_k (k=1,2,…,m)的定义同上.设合成权重最大的直接信任为 TP_l,则合意后的信任的类型与 TP_l 相同,$c=c_l$.

6 结 语

与文献[4,5]提出的信任管理模型相比,本文的信任管理模型对主观信任的模糊性进行了研究,认为对主观信任进行建模的主要困难在于信任具有模糊性,而模糊性并不等同于随机性,不能用精确的数学(概率)模型来描述.因此,本文引入模糊集合论中隶属度的概念来描述信任的模糊性,并定义了信任向量作为信任的度量机制.此外,本文还指出需要有一种通用的类型定义机制来描述实际中复杂多样的信任类型,提出了运用概念树来描述和定义信任类型的方法,并在此基础上提出了借助于信任的综合评判来获得信任向量的方法,解决了 Beth 模型和 Jøsang 模型中都未能很好解决的初始信任如何获得的问题.此外,在本文提出的信任推导规则中,考虑了信任关系的合成权重,使得信任关系的合成更符合实际情况,避免了 Beth 模型的不足.本文所提出的信任管理模型可以作为一种直观而有效的评价、分析和推导工具,为开放网络环境中的主体信任决策提供有效支持.

References:

[1] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management. In: Dale J, Dinolt G, eds. Proceedings of the 17th Symposium on Security and Privacy. Oakland: IEEE Computer Society Press, 1996. 164~173.

[2] Blaze M, Feigenbaum J, Keromytis AD. Keynote: Trust management for public-key infrastructures. In: Christianson B, Crispo B, William S, *et al*., eds. Cambridge 1998 Security Protocols International Workshop. Berlin: Springer-Verglag, 1999. 59~63.

[3] Beth T, Borcherding M, Klein B. Valuation of trust in open networks. In: Gollmann D, ed. Proceedings of the European Symposium on Research in Security (ESORICS). Brighton: Springer-Verlag, 1994. 3~18.

[4] Jøsang A. A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001,9(3):279~311.

[5] Jøsang A, Knapskog SJ. A metric for trusted systems. In: Global IT Security. Wien: Austrian Computer Society, 1998. 541~549.

[6] Jøsang A. Trust-Based decision making for electronic transactions. In: Proceedings of the 4th Nordic Workshop on Secure Computer Systems (NORDSEC'99). 1999. http://security.dstc.edu.au/staff/ajosang/paper.html.

[7] Xu F, Lü J. Research and development of trust management in Web security. Journal of Software, 2002,11(13):2057~2064 (in Chinese with English abstract).

[8] Zadeh LA. The Concept of a Linguistic Variable and Its Application to Approximate Reasoning. Beijing: Science Press, 1982. 23~33 (in Chinese).

[9] Zhu JY. Non-Classical Mathematics for Intelligent Systems. Wuhan: Huazhong University Press, 2001. 146~157 (in Chinese).

[10] Wang PZ, Li HX. Fuzzy System Theory and Fuzzy Computer. Beijing: Science Press, 1996. 219~243 (in Chinese).

附中文参考文献:

[7] 徐锋,吕建.Web 安全中的信任管理研究与进展.软件学报,2002,11(13):2057~2064.

[8] L.A.扎德著,陈国权译.模糊集合、语言变量及模糊逻辑.北京:科学出版社,1982.23~33.

[9] 朱剑英.智能系统非经典数学方法.武汉:华中科技大学出版社,2001.146~157.

[10] 汪培庄,李洪兴.模糊系统理论与模糊计算机.北京:科学出版社,1996.219~243.

2003 全国软件与应用学术会议(NASAC 2003)

征 文 通 知

由中国计算机学会软件工程专业委员会主办,上海交通大学计算机系承办,北京大学、北京航空航天大学、复旦大学、国防科技大学协办的 2003 全国软件与应用学术会议将于 2003 年 11 月 14~16 日在上海召开。届时将进行软件工程等方面的技术与应用交流,会议将出版正式论文集,并将优秀论文推荐到核心学术刊物(EI 检索源)发表。欢迎大家踊跃投稿。

一、征文范围(包括但不限于)

需求工程、软件过程、质量保障、软件工具与环境、软件工程实践、软件工程教育、操作系统、中间件、软件复用、软件语言、应用软件。

二、论文要求

1．论文未曾在其他杂志、会议上发表或录用。

2．论文长度：每篇限定在 6 页(A4)内。

3．请以 PDF 或者 PS 格式提交论文。有关文章的版心、字号、题目、各级标题、格式及参考文献格式与《软件学报》相同，具体模板请参阅如下网址 http://www.jos.org.cn 中的“相关网站”一栏

三、重要日期

文稿截止日期:2003 年 8 月 15 日

论文录用通知日期:2003 年 9 月 20 日

四、联系方式

200030 上海交通大学计算机系 李明禄

E-mail: li-ml@cs.sjtu.edu.cn

关于会议更详细内容请访问:http://www.cs.sjtu.edu.cn/nasac2003/