模糊自主信任建立策略的研究

张仕斌[①②]　何大可[①]　遠藤 誉[③]
[①](西南交通大学信息安全与国家计算网格实验室　成都　610031)
[②](成都信息工程学院网络工程系　成都　610225)
[③](帝京大学　日本东京都八王子市大塚 359 番地　192-0395)

摘　要　该文首先从分析开放式网络环境中有关信任的问题和主观信任的模糊性入手，以模糊理论为基础，引入隶属度来描述信任的模糊性，解决了模糊信任模型的建模问题；以图论为基础，将网络环境模型化为一个无向图 $G(V,E)$，定义了基于本地信息交互的信任评价规则；提出了基于开放式网络环境的模糊自主信任模型，具体研究了自主信任建立策略及建立完全可信网络的实现机制及条件；最后通过仿真实验讨论了网络拓扑结构对自主信任建立的影响，并以小世界网络模型(ϕ-model)为基础分析讨论了自主信任建立的速度问题，这为网络管理的研究提供了一个有价值的新思路。

关键词　自主信任建立，信任模型，信任向量，模糊集合理论，图论
中图分类号：TP393.08　　文献标识码：A　　文章编号：1009-5896(2006)08-1492-05

Research of Fuzzy Autonomous Trust Establishment Strategy

Zhang Shi-bin[①②]　He Da-ke[①]　Homare Endo[③]
[①](*Information Security and National Computing Grid Laboratory*, *Southwest Jiaotong University*, *Chengdu* 610031, *China*)
[②](*Department of Network Engineering*, *Chengdu University of Information Technology*, *Chengdu* 610225, *China*)
[③](*Teikyo University*, 359 *Otsuka Hachioji Tokyo* 192-0395, *Japan*)

Abstract　Firstly, this paper analyzes some questions of trust and the fuzziness of subjective trust, based on fuzzy set theory, the fuzziness of trust is described by membership function, and how to create the fuzzy trust model has been solved. Secondly, based on the graph theory, the network is modeled as an undirected graph $G(V,E)$, and the rule of trust evaluation is defined by the aid of local information interaction. Thirdly, the model of fuzzy autonomous trust establishment based on open network environment is proposed; trust establishment strategy, the mechanism and condition of establishing a fully trusted network are studied in this paper. Finally, the influence of network topology to autonomous trust establishment is discussed through simulation experiment, and the convergence rate of autonomous trust establishment based on the small-world model (ϕ-model) is analyzed in this paper, which enlightens a new way for network management.

Key words　Autonomous trust establishment, Trust model, Trust vector, Fuzzy set theory, Graph theory

1　引言

在网络世界中，主体之间的信任(简称为主观信任)是对主体的特定特征或行为的特定级别的主观判断，而这种主观判断是独立于对主体特征和行为监控的[1]。主观信任本质上是基于信念的[2]，具有很大的主观性、模糊性，无法精确地加以描述和验证。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[3–5]对主观信任进行了有益的探索，但均简单地用概率模型对主观信任进行建模，实际上将信任的主观性和不确定性等同于随机性。因此，这些信任模型[3–6]存在诸多不足之处，比如：使用经典的数学模型对主体的信任度进行度量，可能导致无法反映信任的真实情况；通常采用策略一致性验证方法进行安全度量和决策(安全度量的绝对化)，但该种方法过于精确，无法处理主观信任本身所具有的模糊性，因而不能很好地适应开放式网络环境中的模糊性(多变性、主观性和不确定性)等。此外，由于开放式网络环境边界的动态变化，各主体(用户)在动态地进出，主体之间的信任关系是随机建立的。一些信任管理系统[3,4,7]都只解决的是静态信任管理，而忽略了信任管理的动态性。为了处理信任的动态性，作为信任管理的系统应根据网络环境的动态变化来动态地对各主体的信任关系做出评估，并且还需要有效的机制来评价各主体之间的信任，以对相应的信任决策做出及时调整。

本文以模糊理论和图论为基础，研究并提出基于开放式网络环境的自主信任模型，力图解决主观信任的模糊性和主体之间信任关系的动态性，并从理论上进行了相关的分析和

2005-08-29 收到，2006-02-01 改回
成都信息工程学院科技发展基金(CSRF200406)资助课题

求证。

2　信任建立及信任管理

2.1　信任建立

在开放式网络环境中，信任建立是进行信息安全交互的前提和基础。传统上，信任关系建立的依据主要依靠两种途径：一是以前交互过程中各主体直接观察的经验值(直接经验)；二是来自可信第三方的推荐值(间接经验)；也可以同时采取这两种方法。在信息交互过程中，从对信任值的评估来说，对各主体行为的直接观察是必须的。通过结合预期行为并对这些观察结果进行评价，从而产生一个直接经验值。这个直接经验值反映了与预期结果相互关联的观察结果。可信第三方的推荐值提供了信任决策的部分依据，从而可以在陌生主体之间传播信任。如果直接观察的信任值不是足够精确时，来自可信第三方的推荐值就显得更加重要了。在这种情形下，一个主体可能需要更多的信任决策信息，但是由于如果直接观察的信任值不是足够精确，各主体可能丢掉这些不是很精确的信息，只得到很少相关信任信息的推荐值。这时，信任关系的建立就可考虑依靠本地交互信息(与相邻主体进行交互)由各主体自主决定了(将在后面讨论)。

2.2　信任管理的有关问题

关于信任管理的概念，大家公认最早是由 Blaze[7]提出的(虽然在 PGP[8]和 X.509[9]等中曾有过类似问题的提出)。Blaze 把信任管理理解为：采用统一的方法描述和解释安全策略、安全凭证以及用于直接授权关键性安全操作的信任关系。因此，信任管理研究的内容涉及：信任的表述和度量、信任度推导和综合计算。但当今的一些信任管理系统(如 PGP[8]、X.509[9]等)，它们有一个共同的缺陷就是只对信任的静态形式进行确认。这些系统通常都是无条件地接收来自信任方提供的证书，然后做出相应的决策。实际上，开放式网络环境中主体之间信任关系具有模糊性，其建立过程是动态的，会随着时间的推移而改变(比如，在电子商务中，服务商在一段时间内由于所提供的服务及服务质量的不断提高，用户对服务商的信誉度也会不断地提高)。这些信任管理系统关注的只是：信任的收集、评价与信任关系相关的标准，并对此进行监视、针对前面的结果再对当前的信任关系进行评价。这种只对信任关系进行静态形式的确认，是不能适应开放式网络环境发展需要的。

目前，对随时间改变的信任管理还没有合适的解决方案。为了解决主观信任的动态性和模糊性，必须使得解决方案具有自学习能力，即各主体能随着应用环境的改变，而自主地、动态地做出信任决策。

3　模糊自主信任的建立

3.1　自主信任建立的基本思路

通过分析网络信息交互的实际情况，可以发现信任建立是从一组相互信任的主体开始的。例如，最初加入的少数几个主体是相互信任的，而大多数的主体之间的信任关系是不确定的，可以由最初的少数几个主体对他们进行信任评价；各主体与评价主体之间要么是物理上邻居，要么是逻辑上的邻居。建立在这些邻居观察的经验值和收集的证据的基础上，就能评价出他们的信任值(或信誉度)。借助于本地交互信息，随着这种信任评价的不断进行，整个网络就逐渐从一个个“孤立的信任岛”形成一个“相互关联的信任网络”。一些学者已提出过以相邻节点的信息交互为基础的信任评价[10~12]。在文献[10]中，提出依靠相邻节点建立信任的模型(不是直接与相邻接点建立信任)，观察经验值的交互是在相邻的节点之间进行的。在文献[11]和文献[12]中，提出使用简单的本地信息交互规则来评价各主体的信任，并使用加权平均值来对信任的评价进行综合。在文献[11]中，还模仿了多种不同的恶意攻击行为，研究结果表明使用信任值来标注各主体的信任等级，可以杜绝一些应用受恶意节点的影响(比如在 P2P 网络中下载文件)。另外，由于开放式网络环境不具有严格的层次体系结构，可能参与信息交互的各方既没有预先信任的基础，也没有可信的第三方；同时由于网络资源(比如带宽等)的限制，也制约着信息交互双方信任关系的建立速度。

本文借鉴文献[10–12]已有的一些工作，并以模糊集合理论为基础，研究基于开放式网络环境的自主信任建立模型，提出了模糊自主信任建立策略，各主体只依靠本地信息来建立信任，本文将其称之为模糊自主信任模型。

3.2　模糊自主信任的数学模型

为了研究的方便与问题的简化，首先借助于图论，将开放式网络环境模型化为一个无向图 $G(V,E)$ [13]。将各主体看作是图 G 上的一个节点 i (node)或 agent(本文中节点 i 或 agent 是互用的)，节点 i 是集合 V 中的一个元素。在 3.1 节中已讨论过，各主体所需的本地交互信息证据并不是来自网络中的所有主体，而是来自一个称作邻居的子集：$N_i \triangleq \{j \mid (i,j) \in E\} \subseteq \{1,\cdots,N\} \setminus \{i\}$，$N_i$ 表示与节点 i 或 agent 进行信息交互的节点子集合。

3.2.1 主观信任的定量描述　为了评价节点的信任，最直接的方法是让所有的相邻节点对该节点进行评价。但由于评价具有主观性和模糊性，无法用常规精确的数学模型来描述和处理。所以，为了尽可能地反映各节点信任间各种复杂的属性，必须寻求一种既能反映主观信任的模糊性，又能直观、简洁地定量描述主观信任模型的数学方法。因此，将模糊集合理论[14]的隶属函数(隶属度)引入到节点间(主观)信任的研究中，以解决对具有模糊性的主观信任的定量描述。

定义 1　设研究的问题(论)域为 $X=\{x_1,x_2,\cdots,x_n\}$，$x_i(i=1,\cdots,n)$ (即图 G 上的一个节点 i)为论域中的各主体，相邻节点在对 x_i 的一些属性或特征进行评价时，可以用有限个模糊参数 p_k 来刻画，那么称由这有限个模糊参数刻画所生成的向量 $\boldsymbol{v}(x_i)=(x_{i1},x_{i2},\cdots,x_{im})$ 为 x_i 的特征向量。其中，模糊参数是评价各主体的特征参数，比如信誉度、社会身份、

社会地位、违法情况等；关于刻画的问题，可以在主体参与任务时对主体进行刻画，比如在电子商务中，一般在进行交易以前各主体都应注册，在注册时根据各主体提供的信息对其进行“刻画”；$x_{ik}(k=1,2,\cdots,m)$ 是相邻节点对 x_i 在第 k 个特征参数上的评价。

定义 1 描述了各节点在信任域中的信任状态，描述了主体 x_i 的一些属性或特征。而实际上，对 x_i 的刻画存在很大的主观性、不确定性和随机性(表现为模糊性)，因而用常规的数学方法无法有效地描述和处理。如果在评价各主体的特征时引入模糊集合的隶属度理论，就能尽可能地反映主体信任之间各种复杂的属性，又能直观地、简洁地定量刻画各主体的属性或特征。

定义 2 假设论域 $X=\{x_1,x_2,\cdots,x_n\}$ 为非空集合，$x_i(i=1,\cdots,n)$ 是 X 中的元素，对于 $\forall x_i\in X$ 有如下映射关系成立：$\mu_T: X\to[0,1],\ x_i\mapsto\mu_T(x_i)\in[0,1]$，则称集合 $T=\{(x_1|\mu_T(x_1)),(x_2|\mu_T(x_2)),\cdots,(x_n|\mu_T(x_n))\}$ 为 X 上的模糊子集($\forall x_i\in X$)；并称 $\mu_T(x_i)$ 为 x_i 对模糊子集 T 的隶属度，映射 μ_T 称为模糊子集 T 的隶属函数[15]。

定义 1 中，如果用各主体对 p_k 的隶属度所构成的向量来描述主体的属性或特征，更符合实际情况。所以，用各主体对这有限个模糊参数 p_k 的隶属度所构成的向量 $\boldsymbol{v}(x_{ji})=\boldsymbol{v}_{ji}=(\mu_{1i},\mu_{2i},\cdots,\mu_{mi})$ 作为对 x_i 的评价信任向量($\mu_{ji}\in[0,1],\ j=1,2,\cdots,l$)，$\boldsymbol{v}_{ji}$ 是节点 j 对节点 i 的评价信任向量。其中 $\mu_{ki}(k=1,2,\cdots,m)$ 是由节点 j 评价的节点 i (x_i)对模糊参数 p_k 的隶属度。

这样，通过使用隶属度理论，比较客观地描述了相邻节点对某一节点的特征(信任状态)的评价，更符合复杂多变的网络环境的实际情况，完成了主观信任的建模，本文将其称之为模糊信任模型。

3.2.2 信任的评价 每个信任向量都是各相邻节点间的评价，来自于评价者的观察。设 $\boldsymbol{t}_{ji}$ 是节点 i 的信任向量，$\boldsymbol{v}_{ji}$ 是节点 j 对节点 i 的评价信任向量。关于对节点 i 信任值的评价规则可表示为 $\boldsymbol{t}_i=f(\boldsymbol{v}_{ji},\boldsymbol{t}_j,\forall j\in N_i)$。其中，$f(\cdot)$ 是评价函数，即节点 j 对节点 i 的评价。

关于评价结果的综合有这样几种选择：取所有评价信任向量的加权平均值、最大值或最小值。本文选择使用所有评价值的加权平均值(节点 i 的有效评价信任向量等于 $\boldsymbol{v}_{ji}$ 与 $\boldsymbol{t}_i$ 的乘积，即节点 i 信任向量是对 i 所有评价值的加权平均)。于是，关于节点 i 信任向量的评价规则更新为

$$\boldsymbol{t}_i(n)=\frac{1}{d_i}\sum_{j\in N_i}\boldsymbol{t}_j(n-1)\odot\boldsymbol{v}_{ji}(n) \tag{1}$$

其中 n 表示离散的时间，$d_i=|N_i|$ 是节点 i 的邻居节点数，$\odot$表示各对应元素相乘。在后面讨论中，假设 $\boldsymbol{v}_{ji}$ 是一个常信任向量(实际上，这种假设是不合实际的，因为 agent 总是希望根据收集的信息随时调整评价值)。

由于相邻节点的评价值可能随着网络环境的动态变化而变化，所以评价值的综合也要随之变化，且可能需花费较长的时间。但是最终都将综合到稳态，得到综合的评价值。

下面的讨论中用 $\boldsymbol{v}_{ji}$ 代替 $\boldsymbol{v}_{ji}(n)$。定义 $\boldsymbol{D}$ 是一个对角阵，其第 i 个元素为 d_i，矩阵 $\boldsymbol{V}$ 表示所有的评价值。如果节点 i 与 j 不相邻，则 $\boldsymbol{v}_{ij}=[0,\cdots,0]_{1\times m}$。于是节点 i 信任向量的评价规则更新为

$$\boldsymbol{T}(n)=\boldsymbol{D}^{-1}\boldsymbol{V}\boldsymbol{T}(n-1) \tag{2}$$

其中 $\boldsymbol{T}=[\boldsymbol{t}_1,\boldsymbol{t}_2,\cdots,\boldsymbol{t}_N]^{\mathrm{T}}$ 是信任矩阵。为了评价节点之间的信任关系，在稳态时应用某节点的信任向量是否属于或很贴近(根据模糊理论的择近原则[18])某类信任来确定他们之间的信任关系。

定义稳态时的信任向量 $\boldsymbol{t}_i=\lim_{n\to\infty}\boldsymbol{t}_i(n)\ (i=1,\cdots,N)$，$\boldsymbol{c}_j(j=1,\cdots,s)$ 为某类信任(假定有 s 种信任类型)对应的信任向量，先计算贴近度(应用格贴近度[15])：$\sigma(\boldsymbol{t}_i,\boldsymbol{c}_j)=(\boldsymbol{t}_i\circ\boldsymbol{c}_j)\wedge(1-\boldsymbol{t}_i\otimes\boldsymbol{c}_j)$。其中$\circ$表示“内积”，即 $\boldsymbol{t}_i\circ\boldsymbol{c}_j=\vee(\boldsymbol{t}_i\wedge\boldsymbol{c}_j)$；$\otimes$ 表示“外积”，即 $\boldsymbol{t}_i\otimes\boldsymbol{c}_j=\wedge(\boldsymbol{t}_i\vee\boldsymbol{c}_j)$。在稳态时再应用门限规则，门限规则依赖于系统的门限参数 δ，如下所示：

$$\text{节点 } i\begin{cases}\text{属于}c_j\text{类信任，} & \text{如果 } \sigma(\boldsymbol{t}_i,\boldsymbol{c}_j)\ge\delta\\ \text{不属于}c_j\text{类信任,} & \text{如果 } \sigma(\boldsymbol{t}_i,\boldsymbol{c}_j)<\delta\end{cases}$$

3.2.3 分析与讨论 关于评价的可用性、完整性和可靠性也是值得关心的问题。比如，假设节点都是由所有相邻节点进行评价的，这可能会导致没有被评价的节点将被认为是不可信的。完整性和可靠性可以借助于密码技术来实现，比如数字签名。文献[11]讨论的是一个不同于文献[10]的方法，求各评价值的加权平均值是使用分布式 hash 表(DHT)，并由一个具体委派的节点来代替目标节点进行计算得到的。在文献[16]中，提出了一个比较先进的应用于密钥恢复的评价方案，与其差别在于本文是对所有相邻节点评价值的进行综合，而文献[10]考虑的只是所接收到的评价量。

需要客观说明的是：由于本文研究的信任评价是以本地交互信息作为依据，并且在开放式网络环境中对各节点信任评价是完全分散的，所以任何完全信任可能不一定是真实的。本文以建立安全交互的可信网络(即各交互节点根据具体情况动态建立一个完全可信的网络)来解决这个问题，这更符合实际应用的情况。因此，下面研究在开放式网络环境中怎样依靠相邻节点自主地建立一个完全可信或至少相互关联的信任网络，以进一步说明自主信任建立的可行性，并从理论上分析开放式网络中自主建立可信网的条件。

3.3 自主建立可信网络

在实际应用中，许多信任关系的建立都是在一定初始状态下建立起来(前面已经讨论过)的。如果不依赖于事先假定的初始状态，依靠相邻节点的信任评价是否能够自主建立起信任关系？本节主要研究此问题，并提出开放式网络中建立可信网络的实现机制及条件。本研究假定网络中无攻击者，所有节点的行为和评价都是合理的，并承认评价值的不确定性，但没有恶意评价的节点。

首先引入 header(头)的概念来对节点的信任值(信任向量)进行评价，实际上 header 是一个完全可信的 agent(注：这里

完全可信是指信任向量的所有元素均为 1，即 header 是一个完全可信的节点)。比如，header 可能是大家都完全可信的权威，或拥有认证中心签署的证书的 agent。为了简化起见，假设所有的 header 仅评价它们完全信任的节点。因此，如果 b_i 个 header 信任一个节点 i，那么 i 将获取 b_i 个完全可信的评价。于是定义 b_i 为完全信任 i 的 header 的个数。设 $\boldsymbol{B}$ 是一个对角阵，其第 i 个对角元素为 b_i；$\boldsymbol{I}=[1,1,\cdots,1]^{\mathrm{T}}$。于是，式(2)更新为

$$\boldsymbol{T}(n)=(\boldsymbol{D}+\boldsymbol{B})^{-1}(\boldsymbol{V}\boldsymbol{T}(n-1)+\boldsymbol{B}\boldsymbol{I}) \tag{3}$$

当所有的评价为完全可信时，即各节点能够正确地校验相邻节点是可信的。因此有 $\boldsymbol{V}=\boldsymbol{A}$，其中 $\boldsymbol{A}$ 是图 G 的邻接矩阵。

定义矩阵 $\tilde{\boldsymbol{F}}=(\boldsymbol{D}+\boldsymbol{B})^{-1}\boldsymbol{A}$，$\tilde{\boldsymbol{F}}$ 是标准化的邻接矩阵。定义 $\tilde{\boldsymbol{T}}(n)=\boldsymbol{I}-\boldsymbol{T}(n)$，根据式(3)，可以推导出：

$$\tilde{\boldsymbol{T}}(n)=(\boldsymbol{D}+\boldsymbol{B})^{-1}\boldsymbol{A}\tilde{\boldsymbol{T}}(n-1)\triangleq\tilde{\boldsymbol{F}}\tilde{\boldsymbol{T}}(n-1) \tag{4}$$

其中 $\tilde{\boldsymbol{F}}=(\boldsymbol{D}+\boldsymbol{B})^{-1}\boldsymbol{A}$，于是 $\tilde{\boldsymbol{T}}(n)=\tilde{\boldsymbol{F}}^{n}\tilde{\boldsymbol{T}}(0)$。与前面讨论相似，$\tilde{\boldsymbol{F}}$ 也是一个半随机矩阵。

可以证明(见附录)：当 $n\to\infty$ 时，$\tilde{\boldsymbol{F}}^{n}\to 0$，于是 $\boldsymbol{T}(n)\to\boldsymbol{I}$。

推论 1　对于一个相互关联的图，如果总存在一个节点与一个或多个 header 相关联，那么具有信任值(信任向量)为 $\boldsymbol{I}$ 的所有节点在稳态时将获得完全信任。

这样，仅增加一个 header，就确保了一个完全可信网络的建立。

下面考虑具有不确定性的信任评价情况。

定理 1　如果给定信任门限值为 η，那么对于每个节点的 header 的数量必须满足公式：

$$\boldsymbol{B}\boldsymbol{I}\geq\frac{\eta}{1-\eta}(\boldsymbol{D}-\boldsymbol{V})\boldsymbol{I} \tag{5}$$

证明　与前面讨论的相似，设 $\tilde{\boldsymbol{T}}(N)=\boldsymbol{\xi}-\boldsymbol{T}(n)$，将其代入式(3)，有

$$\tilde{\boldsymbol{T}}(n)=(\boldsymbol{D}+\boldsymbol{B})^{-1}\boldsymbol{V}\tilde{\boldsymbol{T}}(n-1)+(\boldsymbol{D}+\boldsymbol{B})^{-1}((\boldsymbol{D}+\boldsymbol{B}-\boldsymbol{V})\boldsymbol{\xi}-\boldsymbol{B}\boldsymbol{I}) \tag{6}$$

如果设式(6)右边的最后一项为 0，那么当 $n\to 0$ 时，$\tilde{\boldsymbol{T}}(n)\to 0$，因而有 $\boldsymbol{T}(n)\to\boldsymbol{\xi}$。

根据决策规则 $\boldsymbol{T}=\lim_{n\to\infty}\boldsymbol{T}(n)\geq\eta\boldsymbol{I}$，因而有 $\boldsymbol{\xi}\geq\eta\boldsymbol{I}$。考虑到 $\boldsymbol{\xi}\geq\eta\boldsymbol{I}$ 这种情况，由于 $(\boldsymbol{D}+\boldsymbol{B})^{-1}((\boldsymbol{D}+\boldsymbol{B}-\boldsymbol{V})\boldsymbol{\xi}-\boldsymbol{B}\boldsymbol{I})=0$，于是有 $\boldsymbol{B}\boldsymbol{I}\geq[\eta/(1-\eta)](\boldsymbol{D}-\boldsymbol{V})\boldsymbol{I}$。

与此相似，对于不相关联的图，本定理分别处理相互关联的各部分。

因此，通过引入一定数量的 header，在理论上不但证明而且还提出了建立一个完全可信网络的设计方法。而这种方法仅使用本地交互信息，也不依赖于初始的设置，就得到了所希望的结果。这也进一步说明了自主信任建立策略的可行性。

4　仿真实验的研究与分析

前面从理论上研究了模糊自主信任建立的可行性，但由于各节点的信任值的评价是由所有相邻节点评价的综合，本节通过仿真实验研究并分析信任评价达到稳态时所花的时间(即信任评价的综合速率)；由于信任建立过程的动态性，本节以小世界网模型为实验环境来分析信任评价的综合速率，进一步验证模糊自主信任建立策略的可行性和合理性。

首先引入Perron-Frobenius定理[17]，由公式 $\boldsymbol{A}^{n}=\lambda_1^{n}\boldsymbol{v}_1\boldsymbol{u}_1^{\mathrm{T}}+O\left(n^{m_2-1}\left|\lambda_2\right|^{n}\right)$ 来确定随机矩阵$\boldsymbol{A}$。其中 λ_1 为最大特征值，$\boldsymbol{u}_1$ 和 $\boldsymbol{v}_1$ 分别是两个特征向量；λ_2 是次大特征值，m_2 是 λ_2 的代数重数。于是 $\boldsymbol{A}^{n}$ 的综合率为秩 $n^{m_2-1}\left|\lambda_2\right|^{n}$。由于标准的邻接矩阵是随机矩阵，因此具有较小 λ_2 的信任值综合速率更快。

现在的问题是：什么样的网络或网络拓扑结构才具有更小的 λ_2？1998年Watts和Strogatz提出了众所周知的小世界网络模型[18]，随后关于网络拓扑的研究引起了广泛的注意。小世界网络模型有两个突出的特征：在任一对节点之间具有较高的聚合系数和较小的距离(路径)。这表明了在一个给定的庞大网络中，各节点能够与其它节点进行通信。

在本文中，主要研究所谓的 ϕ 小世界网络模型[19]，该模型是在一个点阵网络中增加少数的边来建模的。该网络最初是具有周期性边的二维点阵网，各节点的相邻节点是动态变化的。新边的增加是通过随机地选取两个没有连接的节点来进行的。在仿真研究中，假定在点阵中有 400 个节点。在初始的点阵网中，每个节点有 4 个相邻的节点，边的总数为 800。每次仿真要进行若干轮，在每轮中有 2 个新的边被随机加入到网络中，并计算次大特征值 λ_2 和综合时间。图 1 表明了 λ_2 随新增边的数量变化的情况。图 2 表明了随着新边界的增加，综合时间的实际变化情况。仿真实验表明，增加 8 个新的边，即仅增加总边数的 1%，综合时间从 5000 轮降低到了 500 轮。这也说明具有小世界网络特性的网络与常规的点阵网络相比，其自主信任的建立速度更快。这个结论也为提高网络管理的性能的研究指明一个新思路。

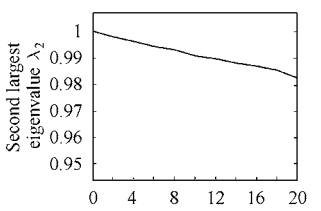

图 1　次大特征值 λ_2 随新增边变化的情况

Fig.1 The situation which the second largest eigenvalue λ_2 changes along with number of edges added

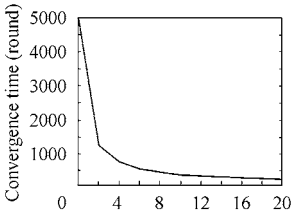

图 2　综合时间随新增边变化的情况

Fig.2 The situation which convergence time changes along with number of edges added

5　结论

在网络世界中，信任建立是网络信息安全的重要前提和基础。本文的主要工作：(1)从分析开放式网络环境中有关信任的问题和主观信任的模糊性入手，引入模糊集合理论的隶属度概念来描述信任的模糊性，解决了信任模型的建模问题；(2)以图论为基础，将网络环境模型化为一个无向图

$G(V,E)$，定义了基于本地信息交互的信任评价规则；(3)提出了基于开放式网络环境中模糊自主信任模型，具体研究了自主信任建立策略及建立完全可信网络的实现机制及条件；(4)通过仿真实验讨论了网络拓扑结构对自主信任建立的影响，并以小世界网络模型(ϕ -model)为基础分析讨论了自主信任建立的速度问题，这为网络管理的研究提供了一个有价值的新思路。本文提出的模糊自主信任建立策略中，采用的是加权平均。虽然十分简单粗糙，但这为在开放式的网络环境中自主地建立信任提供了一个新的研究方向。同时，我们也相信对于以本地信息为基础模糊自主信任的建立还有更好的规则或策略，这还有待进一步研究。除此之外，在前期研究工作还证实了对付恶意攻击具有好的效果(由于篇幅的限制，在本文中没有具体讨论)，关于这些工作的有关理论证明也还需要进一步研究。

附录

如果 $\tilde{\boldsymbol{F}}$ 是一个半随机矩阵，那么当 $n\to\infty$ 时，$\tilde{\boldsymbol{F}}^n\to 0$。

证明　定义 $\tilde{\boldsymbol{F}}^n=\left\{\tilde{f}_{ij}^{(n)}\right\}$。

不失一般性，假定 $\sum_{k=1}^{N}\tilde{f}_{1k}^{(1)}<1$，　$j\neq 1$，　$\sum_{k=1}^{N}\tilde{f}_{jk}^{(1)}=1$。

定义正整数 $m_j=\min\left\{n\mid \tilde{f}_{1j}^{(n)}>0\right\},\forall 2\le j\le N$ 和 $m_1=0$，那么有 $\tilde{f}_{1j}^{(n)}\begin{cases}=0, & \text{如果} n<m_j\\ >0, & \text{如果} n=m_j\end{cases}$。

事实上，m_j 表示在节点 1 和 j 之间的最短路径。由于图 G 是关联的，所以 $m_j<\infty$。可以从下列两种情况中得到证明。

情况 1　$\forall 1\le j\le N$，如果 $l\ge m_j+1$，则有 $\sum_{k=1}^{N}\tilde{f}_{jk}^{(l)}<1$。

情况 2　设 $m=\max\{m_1,\cdots,m_N\}<\infty$，则有 $\sum_{k=1}^{N}\tilde{f}_{jk}^{(m+1)}<1$，$\forall 1\le j\le N$。因此，$\tilde{\boldsymbol{F}}^n$ 的最大特征值严格小于 1。于是当 $n/m\to\infty$ 时，$\tilde{\boldsymbol{F}}^m=(\tilde{\boldsymbol{F}}^m)^{n/m}\to 0$。

参 考 文 献

[1] Gambetta D. Can We Trust Trust? [M] In D. Gambetta editor, Trust: Making and Breaking Cooperative Relations. Basil Blackwell: Oxford, 1990: 213–238.

[2] Jøsang A. Prospectives of modeling trust in information security [A]. In: Proceedings of the 2nd Australasian Conference on Information Security and Privacy [C]. Sydney, Australia, 1997: 219–231.

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

[4] Blaze M, Feigenbaum J, Keromytis A D. Keynote: Trust management for public-key infrastructures [A]. In: Christianson B, Crispo B, William S, *et al*.. eds. Cambridge 1998 Security Protocols International Workshop [C]. Cambridge, UK, April 15-17, 1998. Berlin: Springer-Verglag, 1999: 59–63.

[5] Beth T, Borcherding M, Klein B. Valuation of trust in open networks [A]. In: Gollmann D. ed. Proceedings of the European Symposium on Research in Security (ESORICS) [C]. Brighton, United Kingdom, November 1994: 3–18.

[6] Jøsang A. Trust-Based decision making for electronic transactions [EB/OL]. In: Proceedings of the 4th Nordic Workshop on Secure Computer System(NORDSEC'99) [C]. Stockholm, Sweden, Stockholm University Report 99-005, 1999.

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

[8] Pretty good privacy user's guide [S]. Distributed with the PGP software. Version 8.0 .2003.

[9] Housley R. Internet X.509 Public Key Infrastructure, Certificate and CRL Profiles[S]. RFC2459, 1999.

[10] Sonja Buchegger, Jean-Yves Le Boudec. The effect of rumor spreading in reputation systems for mobile Ad-hoc networks [A]. In Proceedings of Modeling and Optimization in Mobile, Ad hoc and Wireless Networks (WiOpt) [C], Sophia-Antipolis, France, March 2003: 66–75.

[11] Sepandar D. Kamvar, Mario T. Schlosser, Hector Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks [A]. In Proceedings of the Twelfth International World Wide Web Conference [C]. Budapest, Hungary, 2003: 640–651.

[12] Sergio Marti, Hector Garcia-Molina. Limited reputation sharing in p2p systems [A]. In Proceedings of the 5th ACM Conference on Electronic Commerce [C]. New York, NY, USA, 2004: 91–101.

[13] Tutte W T. Graph Theory [M]. Cambridge University Press, 2004.09: 78–97.

[14] L A 扎德著, 陈国权译. 模糊集合、语言变量及模糊逻辑 [M]. 北京: 科学出版社, 1982: 56–75.

[15] 谢季坚, 刘承平. 模糊数学方法及其应用[M]. 华中科技大学出版社, 2000: 16–20.

[16] Chan Haowen, Perrig A, Song Dawn. Random key predistribution schemes for sensor networks [A]. In Proceedings of the 2003 IEEE Symposium on Security and Privacy [C]. IEEE Computer Society. 2003: 175–183.

[17] Bremaud P, Chains M. Gibbs fields, Monte Carlo simulation, and queues [M]. Texts in Applied Mathematics; 31. Springer-Verlag New York, Inc., 1999: 234–266.

[18] Watts D J, Strogatz S H. Collective dynamics of "small-world" networks [J]. *Nature*, 1998, 393: 440–442.

[19] Watts D J. Small Worlds: the Dynamics of Networks Between Order and Randomness [M]. Princeton University Press, 2004: 124–147.

张仕斌： 男，1971 年生，副教授，主要研究方向为信息安全理论与技术、基于网络的计算机应用技术等.

何大可： 男，1944 年生，教授，博士生导师，主要研究方向为信息安全、并行推理与计算等.

遠藤　誉：女，1942 年生，教授，日本内阁府综合科学技术会议专门委员，主要研究方向为信息技术、网络安全等.