

对等网中基于种群进化的信誉模型

鲍翊平 姚 莉 张维明 唐九阳

(国防科学技术大学信息系统与管理学院 长沙 410073)

(国防科学技术大学 C¹ISR 技术国防科技重点实验室 长沙 410073)

摘 要 信誉系统是应对对等网信任危机的关键途径。提出了一种新的基于种群进化的信誉模型。该模型将对等网视为社会生态系统,将节点的信誉评估过程模型化为一种进化过程,通过引入交叉和变异,节点能快速有效地评估潜在交易对象的信任度,从而最终提高其网络适应能力。通过仿真对模型进行了验证。

关键词 对等网,信誉模型,种群,进化

中图分类号 TP393 文献标识码 A

Swarm-Evolution-based Reputation Model for Peer-to-Peer Networks

BAO Yi-ping YAO Li ZHANG Wei-ming TANG Jiu-yang

(College of Information Systems and Management, National University of Defense Technology, Changsha 410073, China)

(C¹ISR Technology National Defense Key Lab, National University of Defense Technology, Changsha 410073, China)

Abstract Reputation system is the key approach to fight against the trust crisis of Peer-to-Peer networks. A novel reputation model based on swarm evolution was proposed in this article. In the model, the Peer-to-Peer network is viewed as social ecosystem, the process of reputation evaluation is modeled as an evolutionary process for peers. By using the strategy of crossover and selection, the peers can rapidly and efficiently evaluate the trust value of potential partners, and finally improve the ability of their fitness. In order for verifying its performance, a simulation experiment for this model was also provided.

Keywords Peer-to-Peer networks, Reputation model, Swarm, Evolution

1 引言

在对等网中,由于没有实用的方法来评估节点及其服务的质量,因此节点不知道哪些节点可安全访问,并且最能满足需求;相反,恶意节点则可能会提供低质量甚至恶意的或误导性服务,而不担心受到惩罚^[1,2]。例如,在 KaZaA 网络中,超过 50% 的流行歌曲都有严重的污染,而且污染拷贝所占的比例随时间的变化缓慢上升^[3];在 eDonkey 系统中,也有半数流行文件是受污染的或是伪造的;Overnet 网络的情况也是如此^[4];Gnutella 中的一些用户通过篡改运行在自己主机上的代码,改变文件共享的方式;此外,一些恶意用户通过 Gnutella 系统传播 VBS. Gnutella worm 蠕虫病毒^[5]。

因此,有必要在对等网中引入一种使得节点能够安全、透明地与更可信的节点进行交互的有效机制。考虑到 P2P 网络及其节点的表现行为与人类社会及其人们在相互交流方面的相似性,人类社会中的信誉机制被引入对等网,产生了对等网的信誉系统(Reputation System)^[6]。

现有信誉系统信誉评估大致分为基于全局信誉度和基于局部信誉度评估两类^[7],其信誉评估一般都是基于信任方自

身直接经验和来自第三方(推荐方)或公开可用的关于受信方的间接经验(推荐经验)的融合,只是在经验信息的利用、利用的范围、利用的侧重点和计算的方式方法上各有差异。典型的模型包括:对反馈信息进行简单(加权)求和或平均的模型、贝叶斯模型、离散模型、信念模型、模糊模型和流模型等^[7]。

现有的信誉模型有些还处于理论研究阶段,有的已经成功实现了商业应用。但是这类模型都是从传统的计算模式出发,着重于个体(在集中式信誉系统中则依赖单个中心节点,而在分布式信誉系统中则是依赖单个节点)在信息搜集处理方面的能力,没有考虑节点个体的进化特性以及多个节点作为一个群体可能涌现出来的群体智能。

从单个节点来讲,在信誉机制的作用下,节点会由初始情况下对其它节点可信程度的“无知”而逐渐变得更加“老练”,能越来越精确地判断节点的可信性,从而选择更可信的节点进行交易。节点的这一变化过程,是不断地模仿和试错的过程,体现了节点在面对环境和和其它节点时的动态适应性,表现出了进化的特征。

从多个节点构成的群体来讲,由于单个节点在不断进化,各节点又能同时与环境和其它节点交换信息、互相影响彼此

到稿日期:2010-02-05 返修日期:2010-04-23 本文受国家自然科学基金(70971134,90716015)资助。

鲍翊平(1981—),博士生,主要研究方向为计算机网络安全、信任管理,E-mail:aban_bao@gmail.com;姚 莉(1965—),博士,教授,博士生导师,主要研究方向为人工智能、智能决策;张维明(1963—),博士,教授,博士生导师,主要研究方向为分布式信息系统、智能决策;唐九阳(1978—),博士,副教授,主要研究方向为对等计算、无线传感器网络、信息集成。

的进化过程,节点之间就能够产生协作行为,最终形成各个节点间以及节点与环境之间的共同适应。共同适应促进了网络的良性演化,使整个系统趋向更高级的有序化发展。

本文的贡献在于改变了传统对等网信誉系统的计算模式,从种群进化的角度提出一种新的对等网中基于种群进化的信誉模型(a Swarm-Evolution-based Reputation Model for peer-to-peer networks, SERM),模型将对等网视为生态网络,通过在信誉模型中引入选择、交叉、变异算子,使得诚实个体节点能快速进化,最终提高自身适应性(即一定时期内成功交易率);恶意节点会被逐渐孤立,并最终“死亡”。

本文旨在构造一个用于对等网环境的全局信任模型,并给出模型数学表述和分布式进化方法,从而使任意节点可以随时地、较方便地获取其他节点的全局信任度。分析和仿真说明,本文提出的模型不仅克服了经典模型 EigenRep^[8]的部分局限性,而且具有较好的工程可行性。

2 相关概念

本节介绍本文涉及到的相关概念及其定义。

2.1 信任、信誉和信誉系统

目前学术界还没有关于信任、信誉和信誉系统的一致定义。

文献[2]指出信任是当事双方的直接关系,分别称之为信任方(Trustor)和受信方(Trustee)。

信任方有时候可能要从特定的第三方获取关于受信方的信任相关信息,这个第三方称之为推荐方(Recommender)。

定义 1(信任, Trust) 信任是信任方期望某一受信方执行事关信任方利益的给定行为的主观概率^[9]。

在定义 1 中,信任从根本上定义为信任方对受信方可靠性的评估(以概率的形式)。用信任度 TD 量化表示,取值范围是 $[0,1]$,0 表示完全不可信,1 表示完全信任。

信誉的概念与信任紧密相关,但明显又有区别。本文中,我们基于简明牛津字典定义信誉。

定义 2(信誉, Reputation) 信誉就是通常所说的或据信的关于一个人或物的品质和名望。

信誉是群体对个体(受信方)可信程度的综合度量,用信誉度 RD 表示,取值范围是 $[0,1]$ 。

通常来说,信任方在获取到某一受信方的信誉度时,还要考虑信誉度本身的可信性,定义为信心。

定义 3(信心, Confidence) 信心就是信任方对信誉度值本身可靠性的判定。

信心用信心度 CD 量化表示,取值范围是 $[0,1]$ 。

节点 i 对节点 j 的信任度由信誉度和信心度组成:

$$TD_{ij} = (RD_{ij}, CD_{ij}) \quad (1)$$

信誉系统是一种重要的技术,它鼓励良好的在线行为,并且惩罚卑鄙的表演者。其基本思想是让交易双方互相评价,在完成交易之后,使用特定评价综合得出一个代表信誉度的数值,它可以帮助信任方判断潜在的交易方是否可信。

2.2 种群、个体节点和适应度

定义 4(种群, Swarm) 规模为 N 的种群 G 是对等网中应用本信誉系统的节点集合,它是一个七元组:

$$G = (P, N, TrustR, TransR, EvolS, f, t) \quad (2)$$

其中,

(1) $P = \{p_i | 1 \leq i \leq N\}$, 是种群中的节点集合;

(2) N 是种群规模;

(3) $TrustR$ 是有向信任关系集合:

$TrustR = \{(p_i, p_j, TD_{ij,t}) | p_i, p_j \in P\}$, $TD_{ij,t}$ 是 t 时刻节点 p_i 对节点 p_j 的信任度;

(4) $TransR$ 是有向交易关系集合:

$TransR = \{(p_i, p_j, t, Sat) | p_i, p_j \text{ 在 } t \text{ 时刻交易}\}$, $Sat \in \{-1, 1\}$, 表示交易结果,其中 -1 表示不满意, 1 表示满意,用 $Sat_{ij,t}$ 表示 p_i 与 p_j 在 t 时刻交易的结果;

(5) $ES = \{SE, CE, ME\}$ 是进化策略集合,分别是选择、交叉和变异策略;

(6) f 是节点适应度函数,用节点在一定时间内的交易成功率表示, $f(p_i, t)$ 表示节点 p_i 在时间 t 的交易成功率;

(7) $t(t \geq 0)$ 表示时间,种群的状态会随时间的变化而演化。

定义 5(个体节点, Individual Peer) 个体节点 $p_i (1 \leq i \leq N)$ 指的是种群中的单个节点(简称节点),其感知能力与行为只能针对有限的局部环境。 t 时刻 p_i 的状态用一个五元组表示:

$$p_{i,t} = (id_i, loc_i, TDV_{i,t}, FV_{i,t}, NList_{i,t}) \quad (3)$$

其中,

(1) id_i 是节点 p_i 的编号,是节点的唯一标识。

(2) loc_i 是节点 p_i 的位置信息,其它节点可用此信息对节点进行定位。

(3) $TDV_{i,t}$ 是 t 时刻节点 p_i 保存的关于其它节点的信任度,以向量形式表示:

$$TDV_{i,t} = (TD_{i1,t}, TD_{i2,t}, \dots, TD_{ij,t}, \dots, TD_{iN,t}) \quad (4)$$

式中, $i \neq j$ 且 $1 \leq j \leq N$ 。

(4) $FV_{i,t}$ 是 t 时刻节点 p_i 的适应度。

$$FV_{i,t} = f(p_i, t) = \alpha \frac{\sum_{j=k=0}^t (Sat_{ij,k} + 1)/2}{1 + \sum_{j=k=0}^t |Sat_{ij,k}|} + (1 - \alpha)$$

$$\frac{\sum_{j=k=t-\Delta T}^t (Sat_{ij,k} + 1)/2}{1 + \sum_{j=k=t-\Delta T}^t |Sat_{ij,k}|} \quad (5)$$

公式的前半部分是所有历史交易的交易成功率,后半部分是距离 t 时刻 ΔT 时间内的历史交易的交易成功率, α 是偏好系数。 α 偏大,表示对历史交易成功率越看重,偏小则表示对近期交易成功率更看重。

同理,定义 $FV_{ij,t}$ 是 t 时刻节点 p_i 对 p_j 的适应度。

$$FV_{ij,t} = f(p_i, t) = \alpha \frac{\sum_{k=0}^t (Sat_{ij,k} + 1)/2}{1 + \sum_{k=0}^t |Sat_{ij,k}|} + (1 - \alpha)$$

$$\frac{\sum_{k=t-\Delta T}^t (Sat_{ij,k} + 1)/2}{1 + \sum_{k=t-\Delta T}^t |Sat_{ij,k}|} \quad (6)$$

(5) $NList_{i,t}$ 表示节点所能感知到的局部环境,称为邻域,邻域中的节点称为节点的邻居节点, t 时刻节点 p_i 感知到邻居节点集合,即

$$NList_{i,t} = \{p_j | 1 \leq j \leq N, TC_{ij,t} \geq TD_0\} \quad (7)$$

指的是,对于节点 p_i 来说,信任度大于常量 TD_0 的所有节点。

定义 6(适应度, Fitness) 个体节点对于环境的适应程

度,我们认为节点在对等网中的成功交易率反映了其适应程度。成功交易率越高,则其适应度越高。

3 基于种群进化的信誉模型

我们认为,信誉系统中节点的最终目的是为了提高自己的适应度。而为了提高其适应度,节点必须提高自身判别其它节点“好坏”、“善恶”的能力,从而在交易时选择更可信的节点,并且避免与可信度低的节点的交易,提高交易成功率。

因此,对于节点 $p_i (1 \leq i \leq N)$ 来说,就是使其关于其它所有节点的信任度向量 $TDV_{i,t}$ (类似于 GA 中的基因) 中的每一个元素尽可能地与相应节点的真实可信程度相符。

3.1 节点种群的进化思想

节点能作用于自身和环境,并能对环境做出反应。种群进化系统的基本思想为:将传统遗传算法(GA)中的每个个体形成节点,每个节点采用进化机制,能够同时与环境和其他节点交换信息,互相影响彼此的进化过程,使各个节点之间能够产生协作行为,最终形成各个节点之间以及节点与环境之间的共同适应^[10]。

在种群进化模型中,将遵循以下的一些原则:每个节点都有初始适应度;节点具有局部性,其感知能力和行为只能针对有限的局部环境,即邻域;由于环境资源的有限性,节点之间存在着激烈的竞争,适应度较低的节点将死亡,适应度较高的节点则会保持其基因,这一行为称为适者生存原则;每个节点具有交叉能力,节点在其邻域内找到合适的配偶进行交叉,把优良的基因传给下一代。另外,节点会与外部环境或其它节点进行交互,交互的结果将导致节点产生变异,以提高对环境的适应能力。

3.2 节点邻域的建立与更新

在节点种群进化系统中,由于节点的感知能力与行为只能针对有限的局部环境,为了让节点快速进化,节点就需要与自己的邻居节点交换信息。因此,如何定义节点的邻域是一个非常关键的问题。

在对等网中,节点会根据自身所具有的自主性与协调性,自主地选择更有利的对象进行协作。本模型中,节点会将与自己有过交易且交易成功的节点接纳为其邻居节点。

由于节点种群活动在很大程度上是一种社会现象,本文采用文献[10,11]的智能协作机制,以人类社会的“关系网模型”来完成节点邻域的建立及更新,使其更符合真实的复杂适应系统,从而进一步加快了信息的扩散过程,快速而有效地完成了整体进化过程。

(1) 邻域初始化

新节点 $p_i (1 \leq i \leq N)$ 加入到种群之后,种群会随机选择 N_{init} 个节点作为 p_i 的初始邻域。初始情况下这些节点的信任度为(0.5,0.5)。

(2) 邻域更新

若节点 $p_i (1 \leq i \leq N)$ 与节点 $p_j (1 \leq j \leq N)$ 第一次进行交易,且交易成功,那么 p_i 将 p_j 加入到其 $NList_{i,t}$,并更新其对 p_j 的信任度。

若节点 p_i 与节点 p_j 不是第一次交易,且本次交易失败,如果其对 p_j 的信任度达到临界值 TD_0 ,则将 p_j 从邻居节点中删除。

3.3 进化策略分析

进化是为了让节点更准确地评价其潜在交易对象的信任

度。一般来讲,节点可以通过两种策略进行进化:交叉和变异。一方面,信任方 $p_i (1 \leq i \leq N)$ 在与受信方 $p_j (1 \leq j \leq N)$ 交易(在文件共享系统中,信任方是资源请求方,受信方是资源提供方)之前, p_i 如果发现 $TDV_{i,t}$ 中对受信方 p_j 信誉度的信心不足,则会向其较为信任的邻居节点发送查询请求,利用邻居节点的反馈,更新其 $TD_{ij,t}$,这是交叉操作。另一方面, p_i 与 p_j 完成交易之后, p_i 会对 p_j 进行评价,并将评价结果反映到 $TD_{ij,t}$ 中,这是变异操作。

(1) 交叉操作

交叉操作是协作行为,模拟了“从别处获得经验”。对于生存在环境中的节点,它将其与邻域中的节点发生协作,交互信息,以提高自身进化速度。

若节点 p_k 是节点 p_j 下一次交易的可选交易对象,设节点 p_j 是 p_i 的邻居节点。

节点 p_i 在时刻 t 向信任度较高的前 K 个邻居节点(这些节点并不知道 p_i 的查询目的,从而避免了针对 p_k 的恶意反馈)发起查询,邻居节点 p_j 返回其 $TDV_{j,t}$ 。

定义相异度(Difference Degree)为任意两个 $TDV_{i,t}$ 的相异性程度,则可将 p_i 和 p_j 的相异度用下式表示:

$$DD_{ij,t} = \sum_{k=0}^N ((RD_{ik,t} - RD_{jk,t})^2 + (CD_{ik,t} - CD_{jk,t})^2) \quad (8)$$

式中, $i, j \neq k$ 。

$DD_{ij,t}$ 指出了 p_i 和 p_j 在评价其它节点时的差异性。差异性越大,表明节点提供的信任度向量越不可靠,对方有可能是恶意节点。为了尽量避免可能的恶意节点提供虚假信息, p_i 选择 $DD_{ij,t}$ 较小的节点或节点集合进行交叉操作。

假设 p_i 选择和 p_j 进行交叉。若有, $CD_{ik,t} < CD_{jk,t} - \eta$, 那么令

$$TD_{ik,t} = ((RD_{ik,t} + RD_{jk,t})/2, (CD_{ik,t} + CD_{jk,t})/2) \quad (9)$$

就是说,如果 p_i 在自己对 p_k 的信誉值的信心不足时,发现 p_j 对节点 p_k 的信誉的信心程度更高,那么 p_i 认为 p_j 对节点 p_k 的认识更加充分,因而会倾向相信 p_j 的评价结果。需要注意的是,如果存在多个这样的 p_j ,则需要基于差异性随机选择某个邻居进行交叉。

(2) 变异操作

变异操作是自学习行为,模拟了“根据自身经验学习从而提高适应度”。节点 p_i 在与 p_j 交易后,会根据交易成功与否,更新自己对 p_j 的信任度 $TD_{ij,t}$ 。

若交易成功:

$$TD_{ij,t} = (\min(RD_{ij,t} + \beta, 1), CD_{ij,t}) \quad (10)$$

若交易失败:

$$TD_{ij,t} = (\max(RD_{ij,t} - \gamma, 0), CD_{ij,t}) \quad (11)$$

式中, $\beta, \gamma \in [0, 1]$,表示交易结果对信任度的影响,一般来讲 $\beta < \gamma$,这意味着“知己难寻,冤家易结”。

$$CD_{ij,t} = \lambda CD_{ij,t} + (1 - \lambda)(FV_{ij,t} - FV_{ij,t}) \quad (12)$$

式中, $\lambda \in [0, 1]$, λ 表示信心度对适应度变化的敏感程度。 p_i 对 p_j 的适应度变化反映了 p_j 近期行为的波动。行为的波动会对信心度产生影响。

3.4 信誉模型分析

SERM 首次提出了采用仿生进化的方式构造信誉模型。由于对等网可视为一个社会生态系统,因此将网络中的节点视为可进化的种群个体是一个天然的选择。

(下转第 82 页)

[6] 胡海江,张凤登.一种新的无线传感器网络分簇模型[J].传感技术学报,2006,2(19):477-480

[7] Ko Young H, Park Chang-Sup, Song In Chu, et al. An efficient void resolution method for geographic routing in wireless sensor networks [J]. The Journal of Systems and Software, 2009, 6(82):963-973

[8] 唐启涛,陶滔,伍海波.基于最小生成树的 LEACH 路由算法研

究[J].计算机技术与发展,2009,4(19):109-111

[9] Gibson J D. The mobile communication handbook[M]. Boca Raton: CRC Press, 1999

[10] Heinzelman W B, Chandrakasan A P, et al. An application specific protocol architecture for wireless microsensor networks [J]. IEEE Transactions on Wireless Communications, 2002, 1(4):660-670

(上接第 56 页)

EigenRep 是对等网中较为典型的基于全局可信度的信誉系统。其核心思想是当节点 p_i 需要了解任意节点 p_j 的全局可信度时,首先从 p_i 的交易伙伴(曾经与 p_i 发生过交易的节点)获知节点 p_j 的可信度信息,然后根据这些交易伙伴自身的局部可信度(从 p_j 的眼光来看)综合出 p_j 的全局可信度。EigenRep 易造成全网迭代;在计算可信度时没有考虑对恶意节点的惩罚问题。

SERM 能有效降低网络通信量,一方面仅向较可信的部分节点发送查询请求,排除了大部分可信度较低的节点;另一方面,随着节点适应度的不断提高,其查询对象的范围会不断缩小。

SERM 考虑了恶意行为的惩罚问题,满意行为获得奖励,而不满意行为获得惩罚,且惩罚力度较大,这对恶意行为起到了良好的抑制作用。

4 实验与分析

我们以文件共享应用为背景,对 SERM 进行了仿真。仿真结果以节点相对于理想情况下的下载成功率作为评价指标。我们在 CPU 为 PIV 1.80GHz,内存 1GB 的计算机上,采用 JAVA 进行了仿真。

对于规模为 1000 个节点的仿真网络,我们设定的文件总数为 10000。将 10000 个文件随机分配到所有 1000 个节点,并保证每个文件至少被一个诚实节点拥有。每个用户在整个仿真过程中必须完成 100 次交易(下载 100 次),每次交易目标为从其不曾拥有的文件中随机选择一个并试图进行下载。交易的成功使得该用户拥有该文件,失败的交易不会增加该用户拥有的文件。

仿真假设系统中只存在两类节点,即诚实节点和恶意节点,其中诚实节点指的是提供真实上载和真实反馈的节点,而恶意节点指的是只提供不真实文件服务的节点。仿真实验验证了恶意节点的规模对 SERM 的影响。实验表明,在单纯存在恶意节点的情况下,SERM 比 EigenRep 具有较高的下载成功率,如图 1 所示。

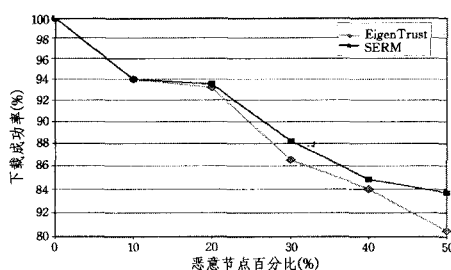


图 1 不同规模的恶意节点下载成功率对比

结束语 本文提出了一种全新的对等网中基于种群进化的信誉模型 SERM。它将对等网视为社会生态系统,节点通过交叉和变异不断进化,从而能选择更可信的节点进行交易,并避免有害节点的伤害。仿真结果表明模型在抑制恶意节点方面性能良好。

需要说明的是,SERM 只是一个初步的模型,在针对模型本身的恶意攻击方面,模型并没有提出明确的机制。但是,模型基于信任度和推荐相似度选择节点的推荐信息应能有效防御恶意节点的不实推荐攻击。

参考文献

[1] 纪雯.对等环境下信誉机制的若干关键问题研究[D].合肥:中国科学技术大学,2009

[2] Jøsang A. Prospectives for Online Trust Management[J]. Working Paper(IEEE Transactions on Knowledge and Data Engineering), 2008

[3] Liang J, Kumar R, Xi Y, et al. Pollution in file sharing systems [C]//Proceedings of the IEEE Infocom 2005, 2005

[4] Liang J, Naoumov N, Ross K W. The Index Poisoning Attack in P2P File-Sharing Systems[C]//Proceedings of IEEE Infocom, 2006

[5] Farhad M. Gnutella Bandwidth bandits[EB/OL]. <http://www.linux.com/feed/24453/>, 2002

[6] Huang Quan-neng, Song Jia-xing, Liu Wei-dong, et al. Survey of Reputation System on Peer-to-Peer Network [J]. Mini-Micro Systems, 2006, 27(7): 1176-1181

[7] Jøsang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision [J]. Decision Support Systems, 2007, 43(2): 618-644

[8] Kamvar S D, Schlosser M T, Garcia-Molina H. The EigenTrust Algorithm for Reputation Management in P2P Networks[C]//the Twelfth International World Wide Web Conference. Budapest, 2003

[9] Gambetta D. Can We Trust Trust? [M]//D. Gambetta, ed. Trust: Making and Breaking Cooperative Relations, Basil Blackwell, Oxford, 1990: 213-238

[10] Pan Xiao-ying, Liu Fang, Jiao Li-cheng. Multiobject Social Evolutionary Algorithm Based on Multi-Agent [J]. Journal of Software, 2009, 20(7): 1703-1717

[11] Chen R Q, Lu G. The relation Web model: An organizational approach to agent cooperation based on social mechanism [J]. Journal of Computer Research and Development, 2003, 40(1): 107-114