软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(4):887−899 [doi: 10.3724/SP.J.1001.2013.04290]

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

移动对等网络中自私节点的检测和激励机制*

曲大鹏[1,2], 王兴伟[1], 黄 敏[1]

[1](东北大学 信息科学与工程学院,辽宁 沈阳 110819)

[2](辽宁大学 信息学院,辽宁 沈阳 110036)

通讯作者: 王兴伟, E-mail: wangxw@mail.neu.edu.cn

摘 要: 由于其自身资源等客观因素的限制以及主观态度的影响,移动对等网络中的节点常常表现出自私性,因此,检测并激励自私节点合作成为当前重要的研究内容.通过允许节点自由表达其主观转发态度,实现对自私节点的检测.即在路由选择时,不仅考虑到链路质量和节点能量等因素决定的路径的客观转发概率,而且考虑到路径上节点自私性影响下的主观转发概率,以选择出综合转发概率最高的路径,从而减轻自私节点的影响.当节点自私度过重时,设计了一个基于惩罚机制的激励合作模型以鼓励节点参与合作.根据节点自私行为的危害程度,对其采取相应的惩罚措施.节点之间的监控机制和严格的惩罚机制保证了防策略性的实现.模拟实验结果表明,该检测和激励机制不仅能够在节点能量受限和理性自私的情况下寻找到合适的路由,而且能够激励过于自私的节点积极参与网络活动.

关键词: 移动对等网络;检测机制;激励机制;自私节点;重复博弈

中图法分类号: TP393 **文献标识码**: A

中文引用格式: 曲大鹏,王兴伟,黄敏.移动对等网络中自私节点的检测和激励机制.软件学报,2013,24(4):887−899. http://www.jos.org.cn/1000-9825/4290.htm

英文引用格式: Qu DP, Wang XW, Huang M. Selfish node detection and incentive mechanism in mobile P2P networks. Ruanjian Xuebao/Journal of Software, 2013,24(4):887−899 (in Chinese). http://www.jos.org.cn/1000-9825/4290.htm

Selfish Node Detection and Incentive Mechanism in Mobile P2P Networks

QU Da-Peng[1,2], WANG Xing-Wei[1], HUANG Min[1]

[1](College of Information Science and Engineering, Northeastern University, Shenyang 110819, China)

[2](School of Information, Liaoning University, Shenyang 110036, China)

Corresponding author: WANG Xing-Wei, E-mail: wangxw@mail.neu.edu.cn

Abstract: Due to the limitation of own resource and the influence of subjective attitude, the nodes in mobile peer-to-peer networks often show selfish behavior. Detecting and stimulating selfish nodes to cooperate is becoming an important research topic recently. By allowing nodes to express their subjective forward attitude freely, the detection mechanism is implemented. Not only is the objective forwarding probability determined by its own resource, but subjective forwarding probability is also determined by selfish nodes that are considered. Therefore, choosing a routing path with the highest integrated forwarding probability can alleviate the influence of selfish nodes. To motivate the excessive selfish nodes to actively cooperate, an incentive and cooperation model based on punishment mechanism is presented. The selfish nodes are punished based on the damage degree of their selfish behavior. The monitor mechanism among nodes and strict punishment mechanism assure that the strategy proof is achieved. Simulation results show that the detection and incentive mechanism can not only discover appropriate routing in the condition of every rational and selfish node has limited resource, but also stimulate selfish nodes to actively cooperate when the degree of nodes' selfishness is high.

Key words: mobile peer-to-peer network; detection mechanism; incentive mechanism; selfish node; repeated game

* 基金项目: 国家自然科学基金(61070162, 71071028, 70931001); 国家杰出青年科学基金(61225012); 高等学校博士学科点专项科研基金优先发展领域资助课题(20120042130003); 高等学校博士学科点专项科研基金(20100042110025, 20110042110024); 工信部物联网发展专项资金; 中央高校基本科研业务费专项资金(N110204003)

收稿时间: 2011-10-09; 修改时间: 2012-02-15; 定稿时间: 2012-07-23

近年来,随着对等模式在有线网络上的成功运行和无线通信技术的快速发展,特别是日益复杂的用户需求对于移动节点之间的协同工作和资源共享提出了更高的要求,出现了一类新型的应用网络——移动对等网络[1].对等网络技术自诞生起就本着“人人为我,我为人人”的理念,但事实上已有研究表明,很多节点只是想从对等网络中获取其他节点提供的服务,而不愿为其他节点奉献[2].在早期,封闭的移动对等网络中所有节点都属于同一个组织,因此能够彼此合作以完成一个统一的目标.但随着移动通信设备,如 PDA、手机等的快速发展和普及,节点可能来自不同的组织,虽然组成一个开放的移动对等网络,但由于每个组织中节点的目标不同,加之节点自身资源如处理能力、电池能量等受限,节点不可避免地存在一定的自私性[3],即多享用其他节点的资源和服务,少共享自己的资源和服务,从而达到节省自身资源的目的.因此,如果节点在选择路由时不考虑自私节点的影响,就会导致其发送的数据包不能顺利地到达目的节点.所以,如何检测网络中的自私节点并对其进行激励合作,从而保证网络的性能,是移动对等网络需要解决的重要问题之一.

针对移动对等网络中自私节点的问题,目前主要有基于信任度的机制和基于博弈的激励机制两种方法[4].前者的基本思想是,如果网络中所有节点都能够参与合作来获得整个系统的最优性能,那么每个节点就能从中得到相应的最优回报.通过观察和监控节点的合作行为并对不合作的节点进行惩罚,从而保证所有节点都能积极合作.根据具体实现方式的不同,可以进一步分为基于信誉的机制和基于支付的机制.基于信誉的机制是根据节点的信誉来评估其信任度,进而作为路由选择的依据.节点的信誉是指所有与该节点有过交互行为的节点对其的综合评价,也是其他节点判断其未来行为的依据[5].Watchdog 和 Pathrater[6]是最早提出的解决网络中自私节点导致路由错误问题的机制.Watchdog 用来检测行为不适当的节点,即每个发送或转发数据包的节点在发送数据包后监控其下一跳节点,如果下一跳节点没有转发,说明它可能存在问题;Pathrater 在收集到的节点详细信息的基础上评定每一条路径的信任等级,尽量避开可能有问题的节点.CORE 机制[7]是在 Watchdog 的基础上提出来的,它通过基于信誉的计算来激励节点进行合作.它整合了主观信誉、间接信誉和功能信誉,分别是指直接获得的信誉、从其他节点获得的信誉和对节点不同功能重要性的判断.基于支付的机制是模仿现实社会中的市场经济活动,利用一种虚拟货币来激励节点合作,即提供服务的节点获得酬劳,而接受服务的节点需要付出相应的费用.Buttyan 等人[8]引入一种安装在节点上的硬件模块——计数器(nuglet counter)来激励节点转发数据包.当节点发送自己的数据包时,计数器数值减少,当节点转发其他节点的数据包时,计数器数值增加.所有的节点必须维持其计数器的值大于 0.Sprite 机制[9]是在网络中确定了一条数据传输的最优路径后,收到数据包的节点保留一个该数据包的收据,中央银行根据最优路径上的节点提交的收据确定它们的收益.文献[10]提出一个简单的流量均衡机制,允许移动节点根据自己的流量放弃包转发,为保证性能,又提出一种协议独立的公平算法鼓励节点积极转发包.

基于博弈的激励机制主要是应用博弈论的相关知识,增强节点之间的合作转发.随着博弈论被应用于无线网络[11],目前得到了广泛的关注.Ad-hoc VCG[12]是通过激励中间节点给出它们转发所需的真实成本,即处于最短路径上的所有中间节点不仅得到其所报的价格,而且还有不包括它的最短路径比原最短路径所多出的机会成本作为额外的报酬,从而实现防策略性.COMMIT[13]在 VCG 的基础上进行改进,通过让数据传输不取决于最优路径上节点的报价,使得节点没有动机去报低价,从而对于在源节点有预算约束的条件下仍然具有防策略性.文献[14]在建立的邻节点之间的单阶段博弈模型基础上进行延伸,并结合重复博弈理论,提出了 3 种激励自私节点的惩罚策略,并分析了各自激励合作转发的条件.

基于信任度的机制相对来说易于实现,但由于整个系统性能最优时不意味着每个节点自身也能达到最优,因此节点存在违背协议的动机,没有从根本上解决问题.同时,信任度主要来源于节点间的历史交互信息,在判断当前状况时,不能高度保证其准确性;基于博弈的机制存在的问题主要是相对成熟的博弈论思想在具体的无线网络实现时要涉及到现实中的很多问题,如通信的可靠性问题等.目前提出的很多机制都是建立在网络中存在中央节点控制的基础上,不是有效的分布式实现.而且,这些机制都着重于通过各种策略激励自私节点进行合作,而没有考虑到由于自身资源的限制,自私节点很难达到完全合作.如果一味进行过重的激励或惩罚策略,自私节点可能直接退出网络,进而造成更大的损失.文献[15]在采用社会网络的方法分析对等网络时发现,适度的

节点自私性反而能够提高网络服务效率.因此,应该在网络正常运行的前提下,允许部分节点具有一定程度的自私性.本文提出了一种针对移动对等网络中自私节点的检测和激励机制.基本思想是,以主观转发概率(subjective forwarding probability,简称 SFP)来描述节点在网络活动中的自私性,以客观转发概率(objective forwarding probability,简称 OFP)来描述其转发能力,在路由选择时,通过考虑路径上所有节点的转发概率(forwarding probability,简称 FP),以实现对自私节点的检测.同时,如果节点的自私度过高,则通过一种基于惩罚的激励机制来鼓励自私节点提高其主观转发概率,实现合作.

本文第 1 节提出自私节点的检测机制,即通过允许节点自由表达其主观转发概率以在选路时避开自私节点.针对节点自私性过重导致网络无法运行的情况,第 2 节提出自私节点的激励机制,通过惩罚措施激励自私节点提高其主观转发概率.第 3 节给出文中机制的相应理论分析.第 4 节给出模拟实验的结果.最后,第 5 节对全文进行总结.

1 自私节点的检测机制

1.1 网络模型

传统路由选择时,我们往往根据一项或多项指标的组合作为选择的标准,如跳数、延迟等.例如,AODV[16]即以跳数作为路由选择的指标.近年来,出现了一些反映路径质量的指标,如 ETX(expected transmission count)[17],它表示在链路上正确传输一个数据包需要的传输次数.每个节点定期地向邻节点广播固定大小的探测包,同时记录过去一段时间内收到的来自其邻节点的探测包的信息.实际收到的探测包的数量与应该收到的探测包的数量的比例就是对应链路的投递率.但这些指标要么没有考虑自私节点的影响,要么直接避开自私节点.现实中自私节点可能只是具有一定的自私度,而非完全自私.如现有两个待选的下一跳节点,一个为合作节点,链路带宽等客观因素决定其转发能力为 0.5,即只能够成功转发收到的数据包的一半;另一个为自私节点,客观转发能力为 1,但自私度为 0.2,即有 80%的概率会转发收到的数据包.显然从整体性能来看,应该选择转发可能性更高的自私节点,而不是像传统机制那样选择合作节点.所以,我们引入转发概率来描述节点对于数据包的实际转发情况,并且用主观转发概率表示节点主观参与网络活动的态度,客观转发概率表示链路带宽、节点处理速度等客观条件限制下节点的转发能力.

在下面具体分析之前,我们首先对网络模型作一些必要的假设:

- 网络 $G(V,E)$表示网络中节点构成的连通图,其中,V表示节点的集合,E表示链路的集合.当且仅当两个节点 u,v 都处于彼此的传输范围内时,它们之间的链路$(u,v)\in E$,所以 E 中的所有链路都是双向的;
- 节点是理性自私的节点,不是危害节点,即可通过谎报自身信息以尽量获取最大化的收益,但不会谎报其他节点信息,同时无节点共谋问题[18];
- 对于来自其他节点且自身不是目的节点的数据包,节点只有两种操作:转发和丢弃.对于因客观因素限制无法转发的数据包,直接丢弃;对于客观因素能够转发的数据包,由其自私性决定转发或丢弃;
- 节点在网络运行过程中处于混杂工作模式,能够偷听到传输范围内其他节点发送的信息;
- 节点初始能量相同且不能补充,在网络运行过程中知道自己的能量情况,且在能量耗尽时会自动退出网络;但参与网络的态度保持理性自私,不因为能量的变化而发生变化.

1.2 节点的客观转发概率

客观因素是指事物自身的属性.对于转发概率,节点的客观因素可分为内部客观因素和外部客观因素两种.前者主要是指受节点能量限制的转发概率,而后者是指受节点的处理能力和相应链路的带宽等客观因素限制的转发概率.

1.2.1 内部客观转发概率

在移动对等网络中,能量是节点的一个重要而有限的资源.对于节点来说,一般情况下,能量越多,对网络运行的参与度越高;对于网络来说,将数据流量发往能量较为充足的节点,避开能量较低的节点可以提高性能,延

长网络生存期.

$$IOFP=energy\_rate=remaining\_energy/initial\_energy \quad (1)$$

式(1)表示用节点的剩余能量与初始能量的比值来表示其内部客观转发概率(inner objective forwarding probability,简称 IOFP).显然,节点的剩余能量越多,它的 IOFP 越高.

1.2.2 外部客观转发概率

外部客观转发概率(external objective forwarding probability,简称 EOFP)反映了节点和相应链路的能力,与路径质量紧密相关.以往研究表明,一般情况下,对链路属性测量越多,得到的路径质量越准确.但也要考虑到测量精度和计算量的问题.目前,无线链路质量主要有 4 个度量参数:接收信号强度指标(received signal strength indication,简称 RSSI)、信干噪比(signal-to-interference-plus-noise ratio,简称 SINR)、包投递率(packet delivery ratio,简称 PDR)和比特错误率(bit error rate,简称 BER).PDR 是目前使用最多且性价比最高的度量参数[19],因此,我们使用 PDR 来表示节点的 EOFP.

在移动对等网络中,相邻节点使用 HELLO 包交换信息,以保证网络的连通性.每个节点定期(每隔 d 秒)广播一个 TTL(time to live,生存时间)值为 1 的 HELLO 包给它的一跳邻节点.因此,我们使用节点 j 单位时间内实际收到来自邻节点 i 的 HELLO 包数量与应该收到的数量之间的比值作为节点 j 的外部客观转发概率.即

$$EOFP=rec(w)/send(w/d) \quad (2)$$

式(2)中,$rec(w)$表示节点 j 在 w 秒内收到的来自邻节点 i 的 HELLO 包的数量,$send(w/d)$表示在 w 秒内,节点 i 发送的 HELLO 包的数量,EOFP 内含了节点 i 到节点 j 之间链路的转发能力和节点 j 的处理能力,我们用它来描述节点 j 对于来自节点 i 的信息的外部客观转发概率.

1.3 主观转发概率

主观因素是指事物自身的意愿.节点的主观转发概率主要指的是在开放的移动对等网络中,每个节点对于网络中其他组织实体的数据传输过程的参与意愿度.由于节点资源受限,而且某些节点可能在本次网络运行中不能获得相关收益,因此需要允许某些节点存在一定的自私性,否则它们可能直接退出本次运行,对于整体性能造成的损失更大.因此,我们引入主观转发概率来描述节点的自私性,取值范围为(0,1).1 表示节点完全合作,在客观能力允许下会转发收到的所有数据包;0 表示节点完全不合作,不参与任何网络活动.SFP 越低,表示节点的自私度越高,丢弃数据包的可能性越大.主观转发概率机制可以使自私节点自由表达意愿,从而合理地节约能量,其他节点也可以在路由选择时,根据实际情况避开 SFP 较低的节点,以保证数据传输.

1.4 自私节点的检测

综上分析可知,传统网络中节点的转发概率就是节点的转发能力,但在移动对等网络中节点的转发概率受 3 个因素决定,是其主观转发概率与内/外客观转发概率之积,如公式(3)所示,它既反映了节点的客观能力,也反映了节点的主观态度:

$$FP_i=SFP_i\times IOFP_i\times EOFP_i \quad (3)$$

为了使相邻节点知道彼此的转发概率,我们对 HELLO 包进行了必要的修改.图 1 表示 HELLO 包的结构,内含包类型、源节点地址、序列号(三者确定一个 HELLO 包)、源节点的 IOFP、SFP 和每个邻节点地址以及在最近 w 秒内收到的来自该邻节点的 HELLO 包的数量,即 EOFP.由于本文使用的 HELLO 包大小为 $(2m+5)\times 4$byte(m 为邻节点的数量),远大于一般网络中只保证连通性的 HELLO 包,更接近普通数据包的大小,因此得到的链路质量更准确.显然,转发概率是节点的乘性参数,所以路径的传输概率是沿途所有节点的转发概率的乘积,即

$$TP_{path}=\prod_{i\in path} FP_i \quad (4)$$

自私节点可以通过降低自己的 SFP 合理地避开网络传输,同时,节点也通过 HELLO 包了解到邻节点的转发概率,从而避免将数据包转发给自私节点或转发概率较低的节点,进而实现自私节点的检测.

packet type
source address
sequence number
IOFP
SFP
neighbor address 1
number 1
…
…
neighbor address *m*
number *m*

Fig.1 Structure of a HELLO packet

图 1 HELLO 包的结构

2 自私节点的激励机制

2.1 节点激励机制

虽然上一节提出的自私节点检测机制允许每个节点根据实际情况自由选择其主观转发概率,但如果没有任何相应的保障机制,则可能会造成自私节点数量过多或节点的自私度过高,从而使得数据在传输过程中无法避开自私节点,性能下降.因此,我们设计了一种基于惩罚的激励机制以保证性能.

2.2 重复博弈

由博弈论的基础知识[20]可知,对于一次性博弈,如囚徒困境,两个自私节点会只关心其一次性的收益,从而选择不合作策略,即尽可能地利用其他节点的服务以达到自身利益最大化.现在,我们考虑两个邻节点之间的博弈,它们的行为集合是{合作,不合作},那么一次性策略见表 1.其中,c 表示某节点对其邻节点采取合作策略时消耗的资源等成本,v 表示两个节点都采取合作策略时双方所获得的收益,n 表示当某节点采取不合作策略而其邻节点采取合作策略时获得的收益,0 表示两个节点都采取不合作策略时双方都不能获得收益.如果两个节点都只关心其一次性收益,那么,两个自私节点会达到{不合作,不合作}.

Table 1 Payoff matrix of one-step game between two neighbor nodes

表 1 邻居节点之间的单阶段博弈收益矩阵

策略	合作	不合作
合作	$(v-c,v-c)$	$(-c,n)$
不合作	$(n,-c)$	(0,0)

但是对于重复博弈,如果选择合适的惩罚机制,那么可能通过一个子完美纳什均衡达到{合作,合作}[21].因此我们设计,一旦节点有不适当的自私行为导致信誉受损,将进入被惩罚期,在此期间,需要一直进行诚实合作以最终恢复其信誉,其他节点不对其提供任何服务,在被惩罚期结束后重新合作.根据重复博弈理论,如果自私行为导致的惩罚高于它所获得的收益,那么理性节点不会发生自私行为,即使发生也会在后面的被惩罚过程中参与合作.我们设定,如果节点在某时刻 t_0 被发现有自私行为,那么在接下来的 T_0 时间内进入被惩罚期,即所有节点都拒绝为其提供任何服务,使得自私节点在被惩罚期内没有任何收益.

2.3 基于惩罚的激励机制

节点的自私行为表现在没有转发应该转发的数据包.由于节点的转发概率受主客观因素共同影响,并且节点主要通过 HELLO 包散布信息,我们据此将节点的自私行为分为两类:一类是谎报信息,即 HELLO 包中 IOFP, EOFP 和 SFP 高于实际值;一类是诚实报告信息,但 SFP 值过低.

对于第 1 类自私行为,首先,由于节点初始能量同构,且在网络运行过程中不能补充能量只能消耗能量,所以,IOFP 在网络运行过程中是一个从 1 严格单调下降到 0 的函数.一旦降到 0,表示该节点耗尽能量应该退出网络.因此,每个节点可以通过接收到的 HELLO 包里面的 IOFP 了解其邻节点的能量情况,一旦发现 IOFP 上升或

者下降到 0 后该节点继续存在,说明该节点谎报了 IOFP,节点通过记录最近一次收到的来自邻节点的 HELLO 包中的 IOFP 的值来进行监控,如果新收到的 HELLO 包中的 IOFP 值高于记录值,说明它谎报信息;其次,在网络运行初期,所有节点都希望通过参与网络活动获得收益,如果降低 EOFP 或者设置过低的 SFP 会导致节点转发概率较低,从而无法吸引其他节点,因此节点会正确汇报 EOFP 和 SFP.但在网络运行过程中,自私节点可能发生丢包行为.上游邻节点会在发送数据包后使用 Watchdog 机制监控下游节点转发情况,如果监控得到的转发概率低于该节点报告的转发概率(考虑误差影响),则说明该节点谎报信息.发现谎报情况的节点生成一个谎报信息包并进行广播,告知网络有节点谎报信息,于是所有节点在未来的网络生存时间内拒绝为其提供任何服务,使得节点只要谎报就不会有任何收益,通过这种最严厉的惩罚机制来杜绝谎报信息情况的出现.

对于第 2 类自私行为,我们设定一个主观转发概率阈值.当 SFP 高于该阈值时,认为节点的自私程度可以接受;否则认为节点的自私度过高,需要进行惩罚以激励其提高参与度.即当节点被检测到 SFP 低于阈值时,则在未来的 T 时间内进行惩罚:

$$T=\begin{cases}\dfrac{\beta-SFP}{\beta}\times T_0, & 0\leqslant SFP<\beta\\ 0, & \beta\leqslant SFP\leqslant 1\end{cases} \tag{5}$$

式(5)中的β表示主观转发概率阈值,T_0 表示基准惩罚时间.当 SFP=0,即节点完全自私时,惩罚时间长度为基准时间长度;当节点的 SFP 超过阈值时,不进行惩罚;否则,按 SFP 与β之间的比例设置惩罚时间长度.

3 防策略性

本文的检测和激励机制保证了防策略性(strategy proof).

证明:防策略性是指在非对称信息博弈中,所有参与者均没有动机对其他参与者说谎或隐藏其私有信息.本文中,节点的私有信息有 3 种:SFP,IOFP 和 EOFP.其中,IOFP 由于其严格单调下降的性质,一旦说谎就会被发现,所以理性节点不会谎报其 IOFP;在网络运行过程中,节点的实际转发概率能够被其上游邻节点通过 Watchdog 机制监控得到,进而能够得到其实际 SFP 与实际 EOFP 的乘积,并且通过 HELLO 包可知其报告的 SFP 与 EOFP 的乘积,因此谎报也会被发现.而且,节点谎报信息被发现后,在未来的网络生存周期内没有任何收益,而节点说谎是为了获得更多的收益,因此理性节点不会说谎,从而实现了防策略性.而且在网络能够正常运行的情况下,允许节点具有一定的自私性,不会执行惩罚机制,从而使得节点更不愿意说谎. □

4 模拟实验

4.1 检测和激励机制的实现

本文提出的检测和激励机制可以在已有路由协议基础上运行,只需略加改动.以按需路由协议为例,源节点发送的控制包沿途收集中间节点的转发概率,目的节点据此评价路径,源节点根据评价信息选择路径.节点需要维持路由表、禁忌列表(存放处于被惩罚期的节点和相应的惩罚期限)、缓冲区(存放最近一段时间发送的数据包)、邻节点信息表等几个数据结构.

为便于实验分析,我们设计了一种基本路由协议:源节点按需生成一个内含源节点地址、序列号、目的节点地址等相关信息的路由请求包(route request,简称 RREQ),该包在网络中广播发送.收到 RREQ 的中间节点首先判断源节点是否为处于被惩罚期的节点:如果不是,正常操作;否则直接丢弃,接着判断自己是否收到过该 RREQ.如果第 1 次收到,那么将自己的节点 id 和转发概率信息存入,再将其转发出去;否则判断新收到的 RREQ 经历路径的转发概率是否高于第 1 次收到的 RREQ 经历路径的转发概率,如果高于,则存入自己的信息并转发,否则直接丢弃.目的节点在收到有效的 RREQ 后,首先生成对应的路由应答包(route reply,简称 RREP)给源节点,再丢弃 RREQ.RREP 在返回源节点的途中,沿途修改中间节点到目的节点的路由表信息,使用对应路径的转发概率作为路由代价,表示其到目的节点的路由信息.源节点收到 RREP 后即建立起一条或几条到目的节点的有效路径.为了自动实现流量均衡,数据包概率型路由如公式(6)所示.当网络中发生路由失效时,发现失效的节点

首先判断自己是否有到目的节点的其他有效路径,如果有,则直接使用,否则生成一个 RREQ 包给目的节点以修复失效路径.

$$p_{i,j}^{d}=\frac{TP_{i,j}^{d}}{\sum_{k\in N_i}TP_{i,k}^{d}} \tag{6}$$

式(6)中,$TP_{i,j}^{d}$ 表示从节点 i 经过下一跳节点 j 到目的节点 d 对应的路径的传输概率,分母表示节点 i 到目的节点 d 的所有可选路径对应的传输概率之和,$p_{i,j}^{d}$ 表示节点 i 在所有可选路径中根据传输概率的数值选择节点 j 作为下一跳节点的概率.节点被选中的概率与对应路径的传输概率成正比.

节点除了维持路由表以选择有效路由外,Watchdog 机制还维持一个缓冲区,内存最近一段时间内发送的数据包,节点在发送数据包后,通过偷听下一跳节点的转发情况得到其最近一段时间内的真实转发概率.如果低于其发布的转发概率,说明该节点谎报信息.为防止误判,设置一个误差范围,如公式(7)所示:

$$(FP_{receive}-FP_{measure})<\varepsilon \tag{7}$$

发现谎报信息的节点生成一个路由谎报包(route LIE,简称 RLIE)并进行广播.RLIE 内含源节点地址、序列号和谎报信息节点地址.收到 RLIE 的节点在将谎报信息节点地址加入自己的禁忌列表后,再将其继续广播,直到生命周期结束.

如果源节点在收到 RREP 后发现由于沿途节点的转发概率过低造成没有有效路径,则生成路由通知包(route notification,简称 RNF),RNF 包含设定的主观转发概率阈值.收到 RNF 的节点首先判断自己的 SFP 是否高于阈值:如果是,则直接转发;否则,先提升自己的 SFP 至阈值,再继续转发,直到生命周期结束.为防止节点盲目要求其他节点,设定源节点在发送 RNF 前先将自己的 SFP 设置为 1,并在未来的生存时间内永远处于合作状态.

根据上面的设定和分析,由于谎报信息的节点将在未来网络生存周期内一直处于被惩罚状态,没有任何收益,所以理性自私的节点不会谎报信息,因此在后面的实验中设定没有节点发生第 1 类自私行为.

4.2 实验设置

我们使用网络模拟软件 NS2 实现了相关机制.50 个移动节点随机分布在一个 1500m×600m 的长方形平面场景中.每个节点使用 IEEE 802.11 无线网络接口,传输距离为 250m,移动方式遵循 Random Waypoint 移动模型:节点以一定的速度向一个随机选定的目标位置移动,接着暂停一个等待时间,再随机选定一个目标,然后向其移动.节点移动速度均匀分布在 0~20m/s 之间.网络模拟时间为 600s.节点停留时间分别是 0s,60s,120s,300s,600s.当停留时间为 0s 时,节点始终保持在运动状态;当停留时间为 600s 时,节点保持在静止状态.网络中随机选定 40 个节点,两个一组作为端节点进行 CBR 连接,共 20 个连接,每个连接的源节点每秒产生 1 个 512 比特的数据分组并发送.其他相关参数见表 2.

Table 2 Other parameter values in simulation experiments

表 2 实验中其他相关参数的设置

Parameter	Value
txPower	0.31J
rxPower	0.35J
w	10s
d	1s
T_0	100s
ε	0.1

为了准确地反映相关性能,我们使用包投递率(packet delivery fraction)和路由开销(routing overhead)作为性能的评价指标.前者表示目的节点正确接收到的数据包占源节点发送的数据包的比例,它直接反映了所选路径的质量;后者是在网络运行过程中传输的控制包占目的节点收到的数据包的比例,信息包以 byte(比特)为单位.由于本文是以待选路径的传输概率作为路由度量,因此采用跳数(hop)、延迟(delay)和 ETX 这 3 种常见的路由标准作为参考.

4.3 性能评价

4.3.1 节点自私性对网络性能的影响

在具体评测本文提出的机制之前,首先分析节点的自私性对于网络性能的危害.为了能够更准确和公正地测试性能,我们使用 AODV 作为基础协议.这里,设置自私节点是对收到的不是发给自己的信息包,根据其自私性进行丢弃.假设节点具有充足的能量.

图 2 中,AODV(*x*)的 *x* 表示自私节点(自私度为 1)数量占网络中节点总数量的百分比.可以看出,当网络中没有自私节点时,AODV 的性能很好;但是,随着网络中自私节点比例的增加,网络性能越来越差.当网络中自私节点的比例占 20%时,网络性能差不多降为原来的一半;当比例增加到 50%,即网络中一半节点都是自私节点时,投递率只有 5%,几乎可以忽略.

图 3 是测试网络中所有节点都是自私节点(自私度不同)情况下的性能.AODV(*x*)的 *x* 表示网络中节点的平均自私度.可以看出,随着节点平均自私度的增加,网络性能越来越差.当节点的平均自私度为 0.1 时,网络性能约为正常情况下的 2/3;当节点的自私度增加到 0.5,即每个节点都有一半的概率表现为自私时,投递率大约只有 13%.

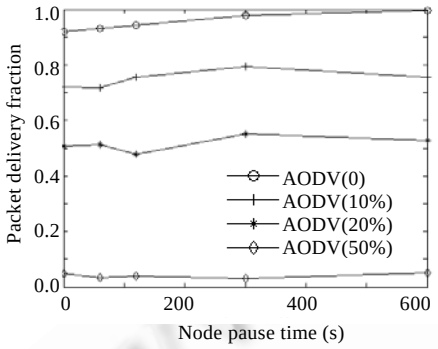


Fig.2 Comparison of network performance under different number of selfish nodes

图 2 不同自私节点数量对应的网络性能比较

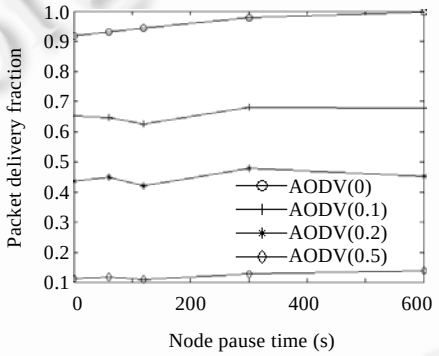


Fig.3 Comparison of network performance under different degree of selfish nodes

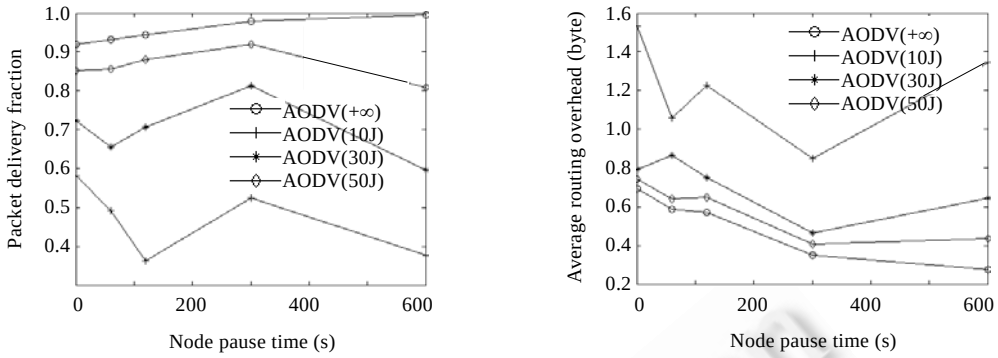
图 3 不同节点自私度对应的网络性能比较

从上面的实验可以看出,即使网络中的节点只有一小部分表现出自私性,包投递率也会显著下降.因此,必须能够检测和规避自私节点,必要时进行激励以提高性能.

4.3.2 节点能量受限对网络性能的影响

下面,我们分析节点能量受限对于网络性能的影响.定义节点能量受限是指节点具有有限的初始能量,随着网络的运行,节点每次发送和接收信息包都消耗一定的能量,忽略计算、存储等操作消耗的能量.一旦节点耗尽自身的能量,即退出网络.

图 4 中 AODV(*x*)的 *x* 表示网络中节点的初始能量,“+∞”表示能量充足,无需考虑能量限制.显然,节点的能量越多,对于网络性能的限制越小,相应的性能也越好.值得注意的是,在节点初始能量较小时,网络性能没有随着节点移动性的下降而变好,而是在静态环境下得到了最差性能.这是因为静态网络中节点保持不动,建立的连接将沿途节点的能量消耗尽后,很难建立起新路径.而动态网络中,由于节点保持运动状态,客观上造成了节点能量消耗均匀分布,从而取得了较好的性能.从图 4(b)中可以看出,节点能量较多时,建立起来的路径基本能够正常工作;而节点能量较少时,可能在网络运行中就退出网络,需要重新寻路,造成了更大的不必要的开销.另外,当节点初始能量过小时,可能会出现某些比较奇怪的现象.例如,当节点初始能量为 10J 时,在节点平均停留时间为 120s 时的包投递率远低于平均停留时间为 60s 和 300s 的包投递率.这主要是因为可能某些节点移动较少,被过度使用所致.



(a) 包投递率 (b) 路由开销(比特)

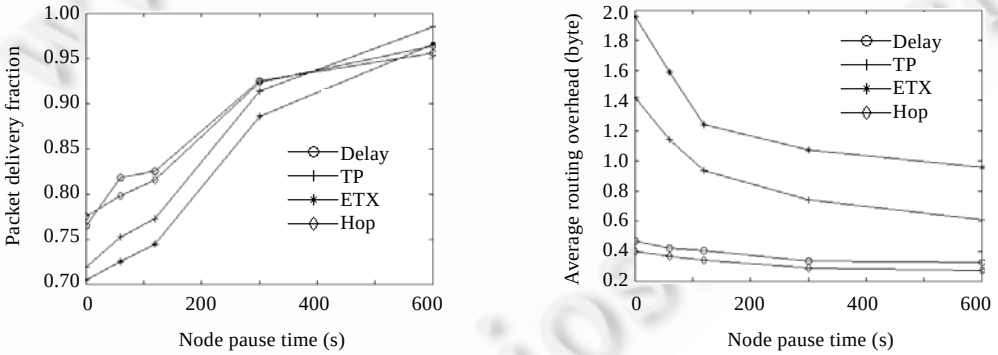
Fig.4 Performance comparison under different initial energy

图 4 不同的节点初始能量对应的性能比较

4.3.3 检测机制的性能

在分析完节点自私性和能量有限性对网络性能的影响之后,我们接着分析检测机制的性能.首先分析在无限制情况(网络中不存在自私节点、节点能量充足)下的性能.注意,由于节点能量充足且无自私节点,所以文中的 IOFP 和 SFP 都设置为 1.这相当于比较传输概率与其他 3 种路由度量的性能.

从图 5(a)可以看出,在无限制情况下,当节点处于静止状态时,使用传输概率作为选路标准的性能略高于使用跳数、延迟和 ETX 作为选路标准的性能,因为它测得的路径质量最准确;但当节点处于运动状态时,使用跳数作为选路标准的性能最好,因为它的反应速度最快,能够适应节点持续运动的情况.图 5(b)表示 4 种选路标准的开销比较.实验中,ETX 使用如参考文献[17]中设定的周期性探测包来测量路径质量,TP 也使用与 ETX 相似的探测包来测量路径质量.为了保证公平性,跳数和延迟中的探测包也采取同样的设置,但是它们的探测包只包括源节点的地址,邻节点在收到探测包后也不执行任何操作,所以开销比较小.



(a) 包投递率 (b) 路由开销(比特)

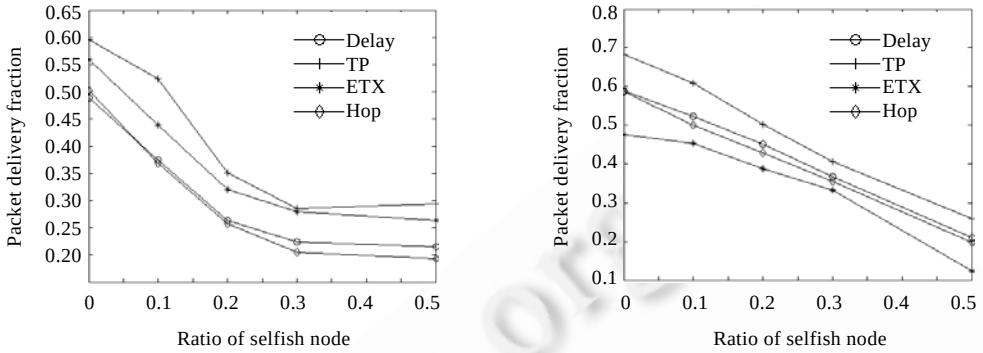
Fig.5 Performance comparison under no selfish node and enough energy

图 5 无自私节点和能量充足情况下的性能比较

接下来,我们分析在网络中存在自私节点、节点能量受限的情况下,即普通的移动对等网络情况下,本文提出的检测机制的性能.其中,静态环境是指网络节点一直保持静止状态,动态环境是指网络节点一直保持运动状态.

根据第 4.3.2 节的结果,我们选定节点初始能量为 30J.从图 6 中可以看出,随着自私节点比例的增加,每种选

路标准的性能都显著下降.但 TP 在选择路径时,能够考虑到节点的自私性和能量受限问题,因此性能最好.特别是在自私节点比例较低的情况下,TP 能够尽量避开自私节点的影响,因此性能优势幅度较大;但在自私节点比例较高的情况下,检测机制也无法完全避开自私节点的影响,因此性能优势幅度较小.Hop 和 delay 的性能相近,而 ETX 因为开销大,又没有针对节点的自私性和能量受限的机制,所以在动态环境中的性能最差.同样,动态环境增加了不同节点之间交互的机会,而且客观上均衡了能量消耗的分布,因此在自私节点比例较低的情况下,网络性能优于静态环境.

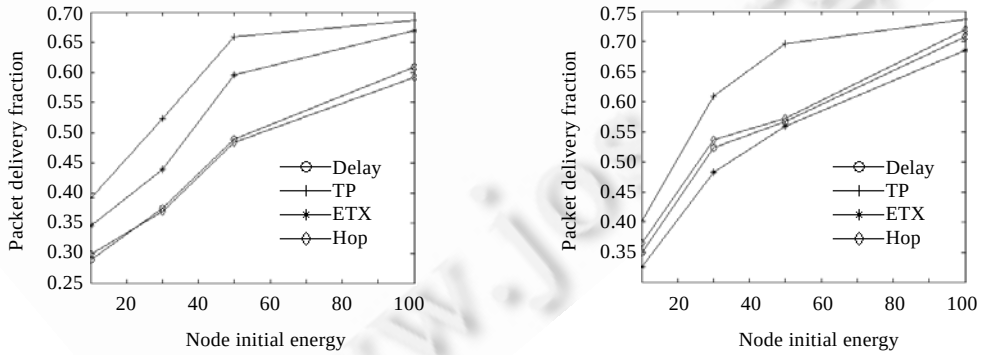


(a) 静态环境 (b) 动态环境

Fig.6 Packet delivery fraction comparison under selfish node and limited energy (30J)

图 6 自私节点和能量受限(30J)情况下的包投递率比较

根据第 4.3.1 节的结果,我们选定节点平均自私度为 0.1.从图 7 中可以看出,随着节点初始能量的增加,每种选路标准的性能都逐渐变好(其中,最后的 100J 表示节点能量充足、没有限制).TP 在选择路径时,能够考虑到节点的自私性和能量受限问题,因此性能最好.特别是在节点初始能量比较合适(如 50J)的情况下,TP 既能均衡流量,又能检测并规避自私节点,因此性能优势幅度最高.在初始能量较低的情况下,节点很容易耗尽能量,因此性能优势幅度较小.Hop 和 delay 的性能相近,ETX 因为开销大,又没有针对节点的自私性和能量受限的机制,所以在动态环境下性能最差.同样,动态环境增加了不同节点之间交互的机会,而且客观上均衡了能量消耗的分布,因此网络性能优于静态环境.



(a) 静态环境 (b) 动态环境

Fig.7 Packet delivery fraction comparison under selfish node (0.1) and limited energy

图 7 自私节点(0.1)和能量受限情况下的包投递率比较

4.3.4 检测和激励机制的性能

最后,我们将检测机制和激励机制结合起来分析性能.节点初始能量设定为 30J,网络处于动态环境.

由于我们设定理性节点不会发生第 1 类自私行为,这里只考虑第 2 类自私行为.图 8 表示当节点发生第 2 类自私行为时,不同的主观转发概率阈值β对于网络性能的影响.当节点的自私度高于阈值时,需要对其进行惩罚.从图中可以看出,通过惩罚机制使得节点的 SFP 提升至允许的阈值,可以提高网络性能,但略低于网络开始时 SFP 就是阈值的情况,主要是因为自私节点有相应的被惩罚期.

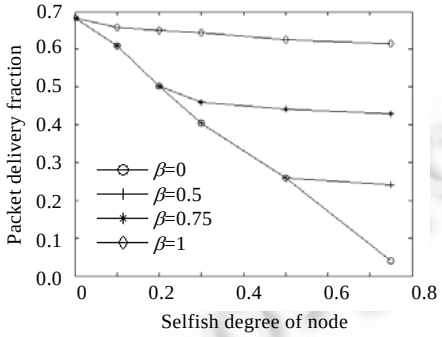


Fig.8 Performance of detection and incentive mechanism with different thresholds

图 8 不同阈值下,检测和激励机制的性能

5 结束语

本文针对自私节点影响移动对等网络性能的问题,提出一种检测机制.通过允许节点自由表达其主观转发意愿实现检测机制,从而在路由选择时既考虑路径质量等客观因素决定的转发能力,也考虑沿途节点自私性决定的主观参与意愿.同时,将节点能量因素也考虑进来,均衡能量,延长网络生存周期.针对节点自私度过重的问题,提出一种激励机制,即根据节点自私行为的危害程度进行相应的惩罚,以激励自私节点.通过节点之间的监控机制实现了防策略性,以保证检测和激励机制的准确、有效.模拟实验证明了其性能.

本文假设节点理性且自私,不是危害节点,不会谎报其他节点的信息,同时无共谋现象.但事实上,属于同一组织的节点可能会为了共同的利益而出现共谋现象,甚至谎报其他节点的情况以达到自己的目的,这也是未来我们需要解决的问题.

致谢 感谢评审人对本文提出的宝贵意见.

References:

[1] Ou ZH, Song MN, Zhan XS, Song JD. Key techniques for mobile peer-to-peer networks. Ruanjian Xuebao/Journal of Software, 2008,19(2):404−418. (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/19/404.htm [doi: 10.3724/SP.J.1001.2008.00404]

[2] Yu YJ, Jin H. A survey on overcoming free riding in peer-to-peer networks. Chinese Journal of Computers, 2008,31(1):1−15 (in Chinese with English abstract).

[3] Yoo Y, Agrawal DP. Why does it pay to be selfish in a manet? IEEE Wireless Communications, 2006,13(6):87−97. [doi: 10.1109/MWC.2006.275203]

[4] Wang Y, Lin C, Li QL, Wang JQ, Jiang X. Non-Cooperative game based research on routing schemes for wireless networks. Chinese Journal of Computers, 2009,32(1):54−68 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2009.00054]

[5] Josang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision. Decision Support Systems, 2007, 43(2):618−644. [doi: 10.1016/j.dss.2005.05.019]

[6] Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. In: Pickholtz RL, Das Sk, Caceres R, Garcia JJ, eds. Proc. of the 6th Annual Int'l Conf. on Mobile Computing and Networking (MobiCom). Boston: ACM Press, 2000. 255−265. [doi: 10.1145/345910.345955]

[7] Michiardi P, Molva R. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Jerman-Blazic B, Klobucar T, eds. Proc. of IFIP TC6/TC11 the 6th Joint Working Conf. on Communications and Multimedia Security: Advanced Communications and Multimedia Security. 2002. 107−121. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.58.4100&rep=rep1&type=pdf

[8] Buttyan L, Hubaux JP. Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile Networks and Applications, 2003,8(5):579−582. [doi: 10.1023/A:1025146013151]

[9] Zhong S, Chen J, Yang YR. Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In: Proc. of the 22nd Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM). San Franciso: IEEE Press, 2003. 1987−1997. [doi: 10.1109/INFCOM.2003.1209220]

[10] Yoo Y, Ahn S, Agrawal DP. Impact of a simple load balancing approach and an incentive-based scheme on Manet performance. Journal of Parallel and Distributed Computing, 2010,70(2):71−83. [doi: 10.1016/j.jpdc.2009.10.005]

[11] Charilas DE, Panagopoulos AD. A survey on game theory applications in wireless networks. Computer Networks, 2010,54(18): 3421−3430. [doi: 10.1016/j.comnet.2010.06.020]

[12] Anderegg L, Eidenbenz S. Ad hoc-VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. In: Johnson DB, Joseph AD, Vaidya NH, eds. Proc. of the Annual Conf. on Mobile Computing and Networking (MobiCom). San Diego: ACM Press, 2003. 245−259. [doi: 10.1145/938985.939011]

[13] Eidenbenz S, Resta G, Santi P. Commit: A sender-centric truthful and energy-efficient routing protocol for ad hoc networks with selfish nodes. In: Proc. of the 19th IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS). Denver: IEEE Computer Society, 2005. 1−10. [doi: 10.1109/IPDPS.2005.142]

[14] Wang B, Huang CH, Yang WZ, Dan F, Xu LY. An incentive-cooperative forwarding model based on punishment mechanism in wireless ad hoc networks. Journal of Computer Research and Development, 2011,48(3):398−406 (in Chinese with English abstract).

[15] Krishnan R, Smith MD, Tang ZL, Telang R. The impact of free-riding on peer-to-peer networks. In: Proc. of the 37th Annual Hawaii Int'l Conf. on System Sciences (HICSS). Big Island: IEEE Computer Society, 2004. 199−208. [doi: 10.1109/HICSS.2004.1265472]

[16] Perkins CE, Royer EM, Das SR, Marina MK. Performance comparison of two on-demand routing protocols for ad hoc networks. IEEE Personal Communications (Special Issue on Ad Hoc Networking), 2001,8(1):16−28. [doi: 10.1109/98.904895]

[17] Couto DS, Aguayo D, Bicket J, Morris R. A high-throughput path metric for multi-hop wireless routing. Wireless Networks, 2005, 11(4):419−434. [doi: 10.1145/938985.939000]

[18] Zhong S, Wu F. On designing collusion-resistant routing schemes for non-cooperative wireless ad hoc networks. In: Kranakis E, Hou JC, Ramanathan R, eds. Proc. of the 13th Annual ACM Int'l Conf. on Mobile Computing and Networking (MobiCom). Montreal: ACM Press, 2007. 278−289. [doi: 10.1145/1287853.1287887]

[19] Vlavianos A, Law LK, Broustis I, Krishnamurthy SV, Faloutsos M. Assessing link quality in IEEE 802.11 wireless networks: Which is the right metric? In: Proc. of IEEE the 19th Int'l Symp. on Personal, Indoor and Mobile Radio Communications (PIMRC). Cannes: IEEE Press, 2008. 1−6. [doi: 10.1109/PIMRC.2008.4699837]

[20] Fudenberg D, Tirole J, Wrote; Yao Y, Huang T, Trans. Game Theory. Beijing: China Renmin University Press, 2010 (in Chinese).

[21] Gui CM, Jian Q, Wang HM, Wu QY. Repeated game theory based penalty-incentive mechanism in Internet-based virtual computing environment. Ruanjian Xuebao/Journal of Software, 2010,21(12):3042−3055 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3717.htm [doi: 10.3724/SP.J.1001.2010.03717]

附中文参考文献:

[1] 欧中洪,宋美娜,战晓苏,宋俊德.移动对等网络关键技术.软件学报,2008,19(2):404−418. http://www.jos.org.cn/1000-9825/19/404.htm [doi: 10.3724/SP.J.1001.2008.00404]

[2] 余一娇,金海.对等网络中的搭便车行为分析与抑制机制综述.计算机学报,2008,31(1):1−15.

[4] 汪洋,林闯,李泉林,王竞奇,姜欣.基于非合作博弈的无线网络路由机制研究.计算机学报,2009,32(1):54−68. [doi: 10.3724/SP.J.1016.2009.00054]

[14] 王博,黄传河,杨文忠,但峰,徐利亚.Ad hoc 网络中基于惩罚机制的激励合作转发模型.计算机研究与发展,2011,48(3):398−406.

[20] Fudenberg D, Tirole J,著;姚洋,黄涛,译.博弈论.北京:中国人民大学出版社,2010.

[21] 桂春梅,蹇强,王怀民,吴泉源.虚拟计算环境中基于重复博弈的惩罚激励机制.软件学报,2010,21(12):3042−3055. http://www.jos.org.cn/1000-9825/3717.htm [doi: 10.3724/SP.J.1001.2010.03717]

曲大鹏(1981－),男,辽宁海城人,博士,讲师,CCF 会员,主要研究领域为移动对等网络.
E-mail: dapengqu@126.com

王兴伟(1968－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为未来互联网,云计算,网络安全,信息安全.
E-mail: wangxw@mail.neu.edu.cn

黄敏(1968－),女,博士,教授,博士生导师,主要研究领域为算法设计与优化.
E-mail: mhuang@mail.neu.edu.cn

Call for papers
The 10th International Symposium on Formal Aspects of Component Software

http://www.jxcsst.com/facs2013/

Keynote Speakers

-- ZHOU Chaochen, Software Institute, Chinese Academy of Sciences

-- Axel Legay (http://people.irisa.fr/Axel.Legay/), IRISA/INRIA, France

-- Jayadev Misra (http://www.cs.utexas.edu/~misra/), University of Texas at Austin, US

Topics of Interest

The symposium seeks to address the development and application of formal methods in all aspects of software components and services. Specific topics include, but are not limited to:

-- formal models for software components and their interaction

-- stochastic techniques for modeling and verification

-- simulation techniques for complex networks of interacting components

-- formal aspects of services, service oriented architectures, business processes, and cloud computing

-- design and verification methods for software components and services

-- composition and deployment: models, calculi, languages

-- formal methods and modeling languages for components and services

-- model based and GUI based testing of components and services

-- models for QoS and other extra-functional properties (e.g., trust, compliance, security) of components and services

-- components for real-time, safety-critical, secure, and/or embedded systems

-- industrial or experience reports, and case studies

-- update and reconfiguration of component and service architectures

-- component systems evolution and maintenance

-- autonomic components and self-managed applications

-- formal and rigorous approaches to software adaptation and self-adaptive systems

Important Dates

-- Abstract submission: July 8, 2013 -- Paper submission: July 15, 2013

-- Notification: September 16, 2013 -- Final version due: October 7, 2013