ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*, Vol.19, No.3, March 2008, pp.755−768
DOI: 10.3724/SP.J.1001.2008.00755

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

# 基于重复博弈的无线自组网络协作增强模型*

陆 音+, 石 进, 谢 立

(南京大学 计算机软件新技术国家重点实验室,江苏 南京 210093)

# Repeated-Game Modeling of Cooperation Enforcement in Wireless Ad Hoc Network

LU Yin+, SHI Jin, XIE Li

(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)

+ Corresponding author: Phn: +86-25-66836890, E-mail: luyin2004@gmail.com, http://www.nju.edu.cn

**Lu Y, Shi J, Xie L. Repeated-Game modeling of cooperation enforcement in wireless ad hoc network. *Journal of Software*, 2008,19(3):755−768.** http://www.jos.org.cn/1000-9825/19/755.htm

**Abstract**: Due to the absence of centralized authority, the service reliability of wireless ad hoc network is seriously affected by selfish actions of the rational nodes during the packet forwarding. This paper proposes a repeated-game model of node behavior that takes account of the selfish nodes' future payoff expectations and their long-term desires for profit. An incentive-compatible condition under which the selfish one will be deterred from cheating by the subsequent punishments and then turn to cooperate is shown analytically. The impacts on the selfish nodes' behaviors, which are induced by their willingness for future collaboration, the parameter settings of punishment mechanism and the efficiency of misbehavior detection, are also discussed. Simulation results show that, the increase of network scale, the deterioration of node's collaborative patience and the low misbehavior detection efficiency will motivate entities toward self-interested action, but this tendency can be neutralized by a careful configuration of the punishment mechanism in the model.

**Key words**: repeated game; wireless ad hoc network; Nash equilibrium; cooperation enforcement; selfishness

**摘 要**: 在缺乏集中控制的无线自组网络中,节点在转发过程中所表现出的自私行为将严重影响其网络服务的可靠性.在节点理性假设的基础上,针对自组网络节点的预期收益及其协作交互过程建立了一个重复博弈模型,提出了一个激励一致性条件,在此条件下,节点将迫于惩戒机制威慑而自愿采取合作策略;并分析了节点对将来利益重视程度、机制参数和作弊检测效率对协作效果的影响.仿真结果表明,通过合理选择惩戒机制参数,能够有效抵御网络规模的增长及节点合作意愿、作弊检测效率的降低所导致的协作性削弱,进而提高存在自私节点时的整体网络性能.

**关键词**: 重复博弈;无线自组网络;纳什均衡;协作增强;自私性

**中图法分类号**: TP393 **文献标识码**: A

无线自组网络提供了一种无须基础设施支持的节点互连途径.依靠独立节点、采用完全分布式的协作方式实现全网的运行是其主要特点,其可用性直接依赖于参与节点无偿与他人协作的意愿及其协作程度.

* Supported by the National High-Tech Research and Development Plan of China under Grant No.2003AA142010 (国家高技术研究发展计划(863))

Received 2006-09-18; Accepted 2007-02-08

目前的无线自组网络是基于节点合作这一基本假设的,而事实上,由于缺乏集中控制机制来确保协作的实施,这使得其自主节点的行为呈现出一定的理性化趋势:为了追求自身最大利益,节点在使用网络资源的同时,拒绝耗费自身有限的能量为他人提供转发服务,这种自私性的作弊行为严重影响了网络的性能[1].研究表明,即便存在着小部分的自私节点(10%~40%),也将导致网络吞吐性能的显著(16%~32%)下降[2].如何有效地促进节点间的协作,从而保障自组网络的可用性及其整体性能,逐渐成为其系统设计上需要考虑的一个关键问题.

目前,针对 Ad Hoc 网络中协作激励的研究大致可分为外在、内在两种角度.前者通过引入虚拟流通和协作信誉等外部机制来迫使节点协作;而后者则通过分析和利用利益驱动的本质对节点决策行为的影响来引导合作,它又可分为机制设计[3]与博弈论分析两个主要研究领域.与前者相比,由于考虑了节点动机,后者不仅简化了分布式环境下的协作促进机制,而且也便于实现更为准确、全面的协作趋势估计.

现有的机制设计模型,如 VCG(Vickrey-Clarke-Groves)路径拍卖模型[4]等,大多利用节点对转发代价之外的超额奖赏的贪婪来鼓励协作.其研究主要针对路由博弈(routing game),且多数建立在一次性博弈[5]的分析基础上.实际上,鉴于节点转发能耗通常远远大于路由能耗,对节点在转发博弈过程(forwarding game)中所体现出的协作性进行分析显得更为重要;而与近乎一次性的路由过程相比,考虑到转发交互本质上的重复性,将其视为一个重复参与协作增强机制所引入的多阶段博弈[5]的过程显然更为合理.但是,VCG 机制并没有为转发博弈的分析提供便利,它在多次博弈场合并不是策略可验证的[6],这使我们不得不采取其他途径来考察转发的重复性对节点协作的影响.

另一方面,在已有的博弈论协作分析模型中,尽管节点的理性因素已得到了普遍的重视,但其参与协作的耐心即节点对自身将来利益的重视程度却没有足够地加以考虑,目前,主流的工作多数考虑的是根据历史收益记录来平衡节点间的相互贡献,多关注于节点对等量回报的理性索取,而忽略了其对将来利益的期望.事实上,当与 Ad Hoc 网络存在长期依赖关系时(如在参与无线组播业务时),节点显然比临时性使用网络时(如只是在发送数条消息报文时)更具合作的意愿,此时,其决策行为将不再仅由历史或眼前利益所决定,而更取决于它对将来利益的评价.在重复转发过程中,耐心因素的影响力可以是决定性的:当理性节点拥有足够的协作耐心,但却预见到其作弊行为将不可避免地招致惩罚并导致未来获益降低时,出于对得不偿失的恐惧,它将不会存在真正实施作弊的动机.这一观察为我们促进节点协作提供了一个新思路,即针对不同的节点耐心来设计对应的惩戒机制,以降低自私节点对将来获利期望的方式来震慑其偏离企图,从而敦促其协作.

为了实现上述思路,首先必须对节点预期收益进行建模和分析.重复博弈理论[5]提供了一个合适的工具.通过将转发协作抽象成相邻节点之间的多次博弈过程,并将节点耐心描述为继续参与下一阶段博弈的概率,重复博弈使用纳什均衡这一概念来对利益冲突环境中节点理性行为所导致的稳定局势进行预测.当节点根据他人行为始终选择最有利于己的协作策略时,其相互最佳响应便构成了自组网络中的一个纳什均衡.这一整体网络状态的意义在于激励一致性:此时,任何节点均不会产生偏离的企图,因为这将降低其收益.重复博弈的分析视角为我们从节点自身角度来引入相应的协作促进机制,同时考察耐心因素对其理性响应的影响提供了便利,而纳什均衡概念的引入则使我们在对局中个体的分析基础上进一步获得对网络全局协作状态的理解成为可能.

本文在节点理性假设的基础上提出了一种基于本地作弊检测的作弊惩戒机制,同时,建立了一个面向重复转发博弈的协作分析模型,并得出了一个激励一致性条件,当它满足条件时,节点将自愿采取合作策略,且整个网络的协作状态将处于纳什均衡.进而分析了节点耐心与惩戒机制参数对协作性的影响,并结合检测机制的效率对该条件进行了扩展.最后对其分析结论进行了仿真验证.

本文第 1 节介绍相关工作.第 2 节给出重复性策略转发模型及激励一致性条件.第 3 节对模型进行分析和扩展.第 4 节论述仿真过程及结论.第 5 节给出模型对比及讨论.最后对本文进行总结.

## 1 相关工作

目前,针对 Ad Hoc 节点的协作增强模型可分为如下几种类型:

1) 虚拟流通模型,如 Nuglet[7],Sprite[8]等.节点参与转发赚取货币并用于发送是其基本思路.由于其依赖于

不可篡改的计费硬件或集中控制的结算中心,因而不太适合分布式自治环境,同时也无法保证收支平衡[9].网络边缘节点因拥有货币较少而无法通信,而流量密集区域的节点则因积累货币过多而完全可选择不予合作.

2) 基于本地行为检测的协作信誉模型.Marti[2]等人提出了 Watchdog 和 Pathrater,通过侦听本地节点行为来评估路由可靠性,以避免选择自私节点所在路径,这反而奖赏了其自私行为.为改善 Watchdog 检测效率,Mahajan 提出了一种匿名广播的本地行为检测协议 Catch[10].Buchegger 和 Michiardi 等人则分别提出了 Confidant[11]和 Core[12]两种基于 Watchdog 的信誉模型,尝试以消息交换方式来传播节点信誉并促进合作.其不足在于信誉维护、传播及节点信任机制复杂且不可靠,容易导致信誉不一致[13]的问题.

3) 机制设计模型,如 Ad Hoc-VCG[4],Corsac[14]和 Team[15],Rpp[16]等.其大多基于 VCG 机制[4],而忽略了转发过程的重复性.由中继者报价、发送者给予选定路由中中继者一定数量的超额红利来激励合作是其核心思想.为鼓励诚实报价,发送者经拍卖支付的总费用一般远高于实际所需的代价,这使得收支平衡问题进一步恶化[3].

4) 基于博弈论的模型.Felegyhazi 提出了一种基于节点拓扑依赖关系的博弈分析模型[17],Altman 等人则在前者基础上进一步提出了一个调整转发概率的模型[18].此外,Srinivasan 还提出了 GTFT(generous Tit-For-Tat model)模型[19],尝试以针锋相对的转发策略来平衡节点间的相互贡献;最后,Levin[20]给出了一种以拥塞信道手段来强制协作的思路.其中,Felegyhazi 和 Altman 的模型均引入了对拓扑的依赖性,其均衡状态的结论唯有在满足特定条件时方可应用,而这要求节点必须了解全局拓扑结构.与前者不同,GTFT 采取了节点与网络间而不是多个节点间博弈的分析角度,从而避免了上述依赖性,但它仅考虑了历史收益对节点决策的影响,而没有考虑其将来获利的期望.在 Levin 的工作中,尽管作者证明了纳什均衡的存在性,但却没有提出具体的协作促进机制.鉴于上述工作与本文的接近性,我们将在第 5 节进一步给出详细的对比论述.

针对上述博弈模型的不足,本文从节点与邻居博弈的角度提出了一种重复策略转发博弈模型.其不同之处主要在于:充分考虑了节点对将来获利的期望,提出利用节点对惩罚的恐惧而不是对奖赏或回报的贪婪来敦促协作;具体给出了一种降低自私者收益预期的惩戒机制,并结合重复博弈这一视角进行了建模,得出了一个协作性判定条件;同时,将作弊检测效率纳入模型因素,对上述条件进行扩展,并据此考察了其对协作性的影响.

## 2 重复性策略转发模型

### 2.1 单阶段策略转发博弈

本节将针对 Ad Hoc 网络中的节点转发博弈过程(forwarding game)进行形式化定义.首先给出如下假设:

1) 整个 Ad Hoc 网络 $G(V,E)$由 $N$ 个理性节点构成,$G$ 为任意连通图,$V,E$ 则分别为节点及链路集合.

2) 当且仅当节点 $u,v$ 处于彼此传输范围时,其间链路$(u,v)\in E$,且 $E$ 中所有链路均是双向的.

3) 任意两节点之间的通信至少经由 1 个以上的中间节点转发实现.我们不考虑直接通信的情况.

4) 整个系统时间由一系列离散的协作时隙 $t$ 构成,在任一时隙中,每一网络节点均有 1 个报文需要发送.

5) 假定同一时隙中路由状态不会发生改变,且单一时隙长度足以保证每一报文均能抵达目标节点.

6) 所有报文长度相同.发送、转发单个报文将消耗相同的能量 $c$,而接收、处理报文时,其能耗则被忽略.

考虑到节点转发能耗一般远大于路由能耗,我们对路由协议进行了抽象和简化,仅将其视为一个求取任意节点对之间优化路径的函数 $R$,而不考虑路由过程中的节点博弈(routing game).不妨假设当邻居节点合作时,节点成功发送 1 个报文时的收益为 $b$,同时,假定其接收报文的收益为 0;可将时隙 $t_j$ 中节点 $i$ 的收益函数表述为

$$u_{ij}(T,F,S)=T\cdot(S\cdot b-c)-F\cdot c\cdot n_{ij} \tag{1}$$

其中,$n_{ij}$ 为 $i$ 在时隙 $t_j$ 中转发的报文数量;$T,F$ 和 $S$ 均为二值布尔变量,其取值为 0 或者 1:$T$ 代表着 $i$ 是否发送了自己的数据包,而 $F$ 则表示节点是否转发了他人的数据包;我们用 $S$ 来代表当前时隙中 $i$ 的邻居是否合作,即 $i$ 的发送是否有效.

我们可以将节点 $i$ 的策略 $a_i$ 定义为三元组$(T,F,S)$的形式,并假定全部节点均以式(1)作为策略选择偏好,且所有节点始终同时决策.上述定义构成了一个单阶段策略转发博弈.

由式(1)可见,无论 $S$ 取值如何,即无论邻居是否协作,$T$=1 且 $F$=0 时的收益总是最大,即策略(1,0,*)为整个博

弈的优超策略,当所有理性节点均采取这一策略时,$G$ 将处于纳什均衡.不难发现,其中并不存在任何协作行为,且所有节点收益均为 0.这一稳定状态显然不是我们所期望的.

### 2.2 基于本地检测的孤立惩戒机制

我们认为,导致上述协作困境的原因在于节点全然无须考虑自私行为对将来收益的影响.事实上,如果作弊将会招致相应惩罚,那么节点将不得不考虑其代价,当后继惩罚将损害其将来利益,并超过当前作弊的短期获利时,它将对节点产生足够的威慑,从而迫使其转而采取协作的态度.

为便于分析,不妨假定 $G$ 采用了一种 Watchdog 协议 $D$,以帮助节点检测邻居作弊行为.我们初步假设 $D$ 是理想化的,即其检测概率为 1.一旦 $i$ 在时隙 $t_j$ 中作弊,它将立即被邻居发现,邻居们将通过 $D$ 迅速达成一致,并且从 $t_{j+1}$ 开始,对 $i$ 实施 $p$ 个时隙的集体孤立,所有以 $i$ 为源或目标的报文将被拒绝转发.

当孤立结束后,$i$ 可以选择重新加入网络,但它必须提供 $r$ 个时隙的无偿转发服务;在此过程中,邻居节点仍然拒绝为 $i$ 提供服务,直到 $r$ 个时隙结束,$i$ 再次回到网络,其作弊历史被遗忘.

### 2.3 重复策略转发博弈

惩戒机制的引入,使得理性节点不得不考虑当前行为对后继博弈阶段的影响.此时,它与邻居之间的多次交互已不再是一系列相互独立的单阶段博弈,而应当被整体地视为一个无限重复的多阶段扩展博弈过程,即构成了一个重复策略转发博弈.

需要指出的是,我们之所以可将上述博弈过程视为无限重复的,是因为节点无法预知博弈何时终止.从博弈论的观点来看,当终点无法预测时,局中人将不得不以无限重复的方式来评估当前策略及其对后继局势的影响.这一假设在转发场景中是合理的,它使得节点无法准确判断某次惩罚是否会因网络运行终止而得不到正确的实施,从而杜绝了其利用这一知识对作弊策略进行逆向推导的可能.

根据重复博弈论中基于贴现准则[5]的收益评估方式,节点 $i$ 在时隙 $t_k$ 时的预期收益 $U_{ik}$ 可表述为

$$U_{ik}=\sum_{j=k}^{\infty}\delta^{j-k}u_{ij},$$

其中,$u_{ij}$ 代表 $i$ 在 $t_k$ 时刻之后所要采取的一系列策略的单阶段收益.$\delta$为贴现因子,其取值范围为(0,1),它可以被视为对节点协作耐心的综合度量:$\delta$越大,则 $i$ 越耐心,也越重视长期利益;反之,则 $i$ 越注重眼前利益;在无限重复博弈中,它也可以被理解为博弈不会于下一时隙终止的概率.$\delta$取值一般由自组网络性质与应用场景决定,临时构建网络其值通常要小于长期存在的网络,而应用模式相对稳定的网络,$\delta$则要大于高度动态的网络.

根据 $u_{ij}$ 的定义,表 1 给出了 $i$ 在重复转发博弈各阶段中的最佳响应策略 $a_i^*$ 及其对应的单阶段收益 $u_i(a_i^*).n_i$ 为当前时隙内 $i$ 所需转发的报文数目.可以看出,当 $i$ 因作弊而被孤立时,其最佳响应策略将是保持沉默;而在重入阶段中,$i$ 的最佳响应策略是不发送自身数据,仅转发他人的报文.

**Table 1** Best-Response strategies and their utilities in repeated forwarding game

**表 1** 重复转发博弈各阶段中节点的最佳响应策略及其对应收益

| Strategy | Abbr. of $a_i^*$ | $(T,F,S)$ | Corresponding $u_i(a_i^*)$ | |
|---|---|---|---|---|
| Defection (cheating) | $D$ | (1,0,1) | $u_i(D)$ | $b-c$ |
| Cooperation | $C$ | (1,1,1) | $u_i(C)$ | $b-(1+n_i)c$ |
| To cope with isolation | $I$ | (0,0,0) | $u_i(I)$ | 0 |
| To cope with reentering | $B$ | (0,1,0) | $u_i(B)$ | $-c\cdot n_i$ |

### 2.4 激励一致性条件

为便于分析,我们假设在稳定的网络状态下,节点 $i$ 在每一个时隙中所需转发报文数量的平均值基本为一定值.考察重复转发博弈过程可以发现,一旦 $i$ 选择作弊,那么此刻它将采取持续作弊的策略.这是因为,如果一次作弊能够令 $i$ 额外获利,那么在孤立-重入结束之后,$i$ 将再次面临同样的决策场景,即在无限重复的转发博弈过程中,重入网络之后的作弊节点所面临的子博弈局势恰好为原博弈本身.

为消除节点作弊动机,必须保证 $i$ 持续合作时的收益不低于重复作弊收益.这一条件可用贴现形式表述为

$$\sum_{t=0}^{\infty}\delta^t u_i(C)\geq\sum_{k=0}^{\infty}\delta^{k(p+r+1)}\left[u_i(D)+0+\delta^{p+1}\sum_{t=0}^{r-1}\delta^t u_i(B)\right] \tag{2}$$

其中,左式为持续合作时 $i$ 获得的折现收益,右式为 $i$ 选择作弊时的收益现值.在每一个理性节点决定作弊之前,它们均将对作弊所带来的收益进行评估,而只有当式(2)不成立时,它才会真正实施作弊.作为系统设计者,我们可针对不同的$\delta$值,以适当调整 $p,r$ 参数的方式来影响右式,令其条件成立,从而使节点放弃偏离企图.

从式(2)右端还可以看出,惩戒机制对作弊行为的惩罚实际上是通过重入阶段的负收益来实现的,其主要取决于 $r$;而另一方面,$p$ 则更多地体现为一种通过时间因素调节惩罚严厉程度的手段,因为孤立阶段的存在并不会直接降低 $i$ 的收益,但它却会减少后继作弊收益和重入阶段负收益的折现.将式(2)化简可得

$$u_i(C)\geq\frac{1-\delta}{1-\delta^{p+r+1}}u_i(D)+\frac{\delta^{p+1}-\delta^{p+r+1}}{1-\delta^{p+r+1}}u_i(B) \tag{3}$$

由式(3)可见,当 $i$ 非常注重眼前利益,即$\delta$趋近于 0 时,右式极限为 $u_i(D)$,$i$ 将一定选择作弊.同样地,当 $p=r=0$ 时,无论$\delta$取值如何,式(3)也将永不成立,此时,整个重复转发博弈将最终退化为一系列独立的单阶段博弈.由于失去了惩戒机制的震慑,节点将全部选择作弊.这一观察与第 2.1 节的分析相一致.

假定 $b>(1+n_i)c$,由表 1 可知,$u_i(C)=u_i(D)+u_i(B)>0$,因此可将式(3)进一步化简为:

$$\frac{u_i(D)}{|u_i(B)|}\geq\frac{1-\delta^{p+1}}{\delta-\delta^{p+r+1}} \tag{4}$$

其中,$p,r$ 不能同时为 0.式(4)即为重复策略转发博弈中的激励一致性条件.当对于所有节点,上式均满足时,合作成为每一节点应对惩戒机制的最佳响应策略,任何理性节点均无法形成足够的动机来偏离这一决策,因此,根据相互最佳响应的纳什均衡定义,整个博弈局势将处于纳什均衡状态.

由式(4)可见,其左端由作弊净收益与惩罚代价等两部分组成,其取值依赖于 $b,c$ 和 $n_i$;而右式则完全由$\delta$和两个惩戒机制参数构成,其中,$\delta$由网络及应用的本质所决定,而 $p$ 和 $r$ 则从系统设计角度提供了一种可行的机制调节手段,以帮助我们在不同的网络环境中实现不同程度的协作激励.

对于系统设计者而言,为了能够依据式(4)的条件选取适当的机制参数配置,必须首先预计其左式的取值.一般可以采用全网节点平均转发数据包的最大数量 $n$ 来替代 $n_i$ 以求取左式.该方式的合理性在于,如果在最保守的转发情况下,$i$ 的获益能够保障,那么在通常情况下,其收益显然也能得到保证.$n$ 的取值由系统设计者对网络规模和协作性程度的估计所决定,在协作要求最为严厉的极端场合中,$n=N-1$.

在实际自组网络中,对于每一节点而言,$b,c$ 取值可能是不一样的,其由节点自身关注的各种因素所决定.如报文信息量、QoS 等级与当前剩余能量等,这些因素均被抽象为式(4)左端的比值形式,而与右端完全无关.在必要情况下,我们可以将它们在条件左端加以显式定义,从而为协作性分析提供便利.

## 3 模型分析及扩展

本节首先分析惩戒机制的参数变化对于激励一致性条件以及节点协作行为的影响,然后分析了$\delta$的有效限界,并给出了对应 $p,r$ 参数的配置范围.最后,为考察本地检测机制效率的影响,我们对式(4)进行了扩展.

### 3.1 惩戒机制参数对协作性的影响

**命题 1**. $r$ 的增加有助于形成对自私行为的威慑,从而促进节点协作.

证明:不妨令式(4)左端为 $A$,并将右式视为一个三元函数 $f(\delta,p,r)$.对 $f$ 求 $r$ 的偏导可知$\partial f/\partial r$ 非正.因此,在给定 $p,\delta$和 $A$ 的前提下,增大 $r$ 将导致 $f$ 变小,式(4)条件因而更容易满足.得证. □

**命题 2**. 当 $r=0$ 时,增加 $p$ 将有助于增强对自私行为的威慑;当 $r=1$ 时,$p$ 的变化对节点协作行为无影响;而当 $r>1$ 时,$p$ 的增加却会减轻对作弊行为的威慑,从而削弱其协作促进效果.

证明:注意到 $p,r$ 均$\in N^0$ 且不同时为 0.考察$\partial f/\partial p$,当 $r>1$ 时其值非负;当 $r=1$ 时,$f(\delta,p,r)=1/\delta$,式(4)条件与 $p$ 无关;而当 $r=0$ 且 $p\geq1$ 时,$\partial f/\partial p$ 非正,因而得证. □

命题 1 说明,$r$ 越大,则节点收益估计中因作弊所遭受的损失就越大,节点便越倾向于合作,这与直觉相符.命题 2 则表明,重入阶段存在与否将直接决定 $p$ 的机制调节效果.当 $r>1$ 时,$p$ 的增加对惩罚性负收益的削弱实际上超过了对后继作弊收益的抑制,这说明一味消极孤立却不给予足够多的实质性惩罚,只会更加纵容节点作弊.

当 $r=0$ 时,孤立的作用将单方面体现为对后继作弊收益的削弱,因此效果与增大 $r$ 类似.但需要指出的是,当 $p\to\infty$ 时,$f(\delta,p,0)$ 的下极限为 $1/\delta$,而当 $r$ 非 0 时,$1/\delta$ 却是整个 $f$ 的上限.这表明单纯孤立的惩戒机制在最有效的情况下也不可能获得比存在惩罚时的最差场合更好的激励效果.

### 3.2 协作耐心的限界及机制参数配置范围

**命题 3.** 当 $\delta<\delta_{\min}=1/(A+1)$ 时,无论 $p,r$ 取何值,激励一致性条件永不满足.

证明:当给定 $\delta,p$ 时,$\partial f/\partial r$ 非正,因此,当 $r\to+\infty$ 时,$f$ 将取极小值 $1/\delta-\delta^p$,当 $p=0$ 时,该值将取最小值 $1/\delta-1$,这也是整个 $f$ 的全局下限.当 $1/\delta-1>A$ 时,式(4)永不成立. □

命题 3 表明,当节点极端注重眼前利益时,由于协作环境过于恶劣,惩戒机制将完全失效.然而,考虑到 $A=(b-c)/nc$,即使在这种悲观场合下,系统设计者依然能够通过限制最大转发数量 $n$ 来调节 $A$ 以令式(4)成立,从而牺牲惩戒机制的可扩展性来换取其有效性.

**命题 4.** 当 $\delta>\delta'_{\max}=1/A$ 时,对于任何满足 $r\geq1$ 的 $p,r$ 参数组合,激励一致性条件均满足.

证明:当 $r=1$ 时,$f(\delta,p,1)=1/\delta$,而当 $r>1$ 时,$\partial f/\partial p$ 非负,$p\to+\infty$ 时,$f$ 取极大值为 $1/\delta$,因此,$1/\delta$ 即为 $r\neq0$ 时 $f$ 的极大值.当 $\delta>1/A$ 且 $r\geq1$ 时,任何 $p,r$ 参数均满足式(4). □

上述命题展现了一种较为乐观的协作场景,即当节点对将来利益的重视高于一定程度时,仅需 1 个重入时隙便足以震慑其自私行为.

**命题 5.** 当 $\delta\geq\delta_{\max}=1/(A-1)$ 且 $A\geq2$ 时,除 $p=r=0$ 之外的任意 $p,r$ 参数组合均满足激励一致性条件.

证明:当 $A\geq2$ 时,$\delta_{\max}>\delta'_{\max}$,由命题 4 可知,$r\geq1$ 的任意 $p,r$ 参数均满足式(4).当 $r=0$ 且 $p\geq1$ 时,$\partial f(\delta,p,0)/\partial p$ 非正,则当给定 $\delta\geq\delta_{\max}$ 时,$f(\delta,1,0)$ 即为 $r=0$ 时 $f$ 的上界. □

这一命题表明,即使节点非常耐心,惩戒机制依然有必要存在,尽管除 $p=r=0$ 之外它可以任意配置.因为当 $p=r=0$ 时,节点绝不会自发地选择协作.

上述关于 $\delta$ 限界及 $p,r$ 范围的结论为分析重复策略转发模型中的节点协作程度提供了基础依据,这使我们能够对惩戒机制的适用性及其有效程度作出迅速判断.这里,我们具体给出一个当 $\delta_{\min}\leq\delta\leq\delta'_{\max}$ 时的分析实例.在该实例中,$\delta=0.7,b=1,c=0.04663,N=20,n=16$,则有 $A=1.2777,\delta_{\min}=0.439,\delta'_{\max}=0.782$.

图 1 为 $r\geq1$ 时曲面 $z=f(0.7,p,r)$ 与 $z=A$ 的相交情况,$p$-$r$ 平面中的曲线是二者交线的投影.该线内侧与 $r$ 轴之间所有的 $p,r$ 组合均满足式(4).图 2 为 $f(0.7,p,0)$ 的曲线图,可见,对于 $p\neq0$ 且 $r=0$ 的所有组合而言,式(4)成立.

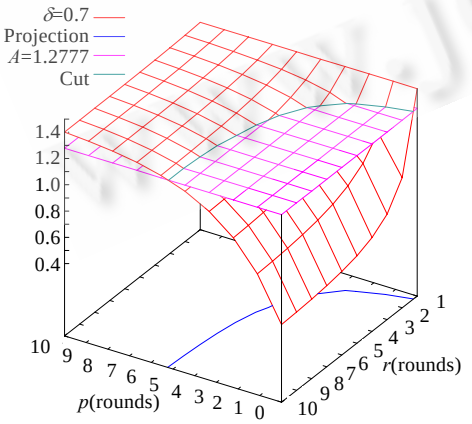


Fig.1 Sample of $p/r$ configuration ($\delta=0.7$, $r\geq1$)

图 1 $\delta=0.7$ 时的 $p,r$ 配置分析实例($r\geq1$)

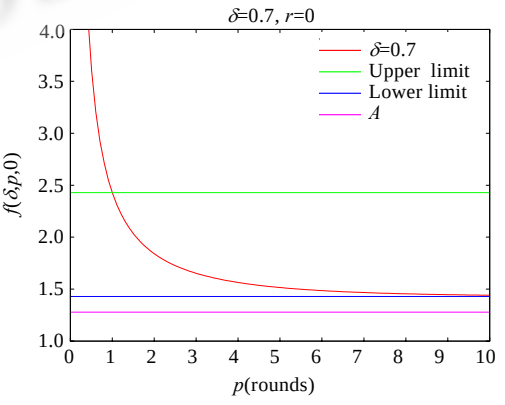


Fig.2 Sample of $p/r$ configuration ($\delta=0.7$, $r=0$)

图 2 $\delta=0.7$ 时的 $p,r$ 配置分析实例($r=0$)

图 3 为 $f$ 与 $A$ 交线投影随 $\delta$ 的变化情况,直观给出了各 $\delta$ 取值下的 $p$-$r$ 配置范围.当 $\delta_{\min}\le\delta\le\delta'_{\max}$ 时,所有位于投影线内侧的组合均满足式(4),如 $\delta$=0.65,当($p$,$r$)为(1,2)时,式(4)成立,而当其为(2,2)时则不然.当 $\delta\ge\delta'_{\max}$ 时,其投影外侧的全部组合均满足式(4).如当 $\delta$=0.85 时,对于所有 $r$=0 且 $p\ge$7 及全部 $r\ge$1 的组合而言,式(4)均成立.

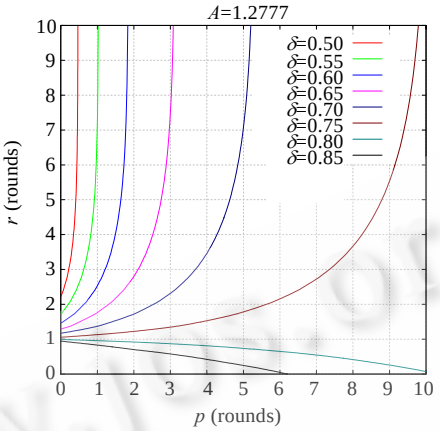


Fig.3 Valid configuration range of $p$/$r$ for different $\delta$

图 3 针对不同 $\delta$ 取值的 $p$,$r$ 配置范围

### 3.3 关于本地检测概率的激励一致性扩展条件

在上文中,我们假设本地检测协议为理想化的,即成功检测出节点作弊的概率为 1.考虑到实际场合中信道干扰、噪声等不可控因素和 Watchdog 机制固有的局限性[2],假设其作弊检测概率小于 1 显然更为合理.

不妨设理性节点 $i$ 作弊时被发现的检测概率为 $q\in(0,1)$,则其作弊 $k$ 次时才被邻居发现的概率为 $(1-q)^{k-1}q$,此时,节点的作弊获益现值为

$$benefit=\sum_{t=0}^{k-1}\delta^t u_i(D)\,.$$

假定当前惩戒机制参数配置为($p$,$r$),则 $i$ 在作弊 $k$ 次被发现后,其自私行为所招致的折现损失为

$$lost=0+\delta^{p+k}\sum_{t=0}^{r-1}\delta^t u_i(B)\,.$$

当 $i$ 在被惩罚且重入网络之后,其将会再次面临相同的决策处境.令 $S_i$ 为当前处境下 $i$ 选择作弊策略时将获得的总收益现值期望,可将 $S_i$ 表述为

$$S_i=\sum_{k=1}^{\infty}q(1-q)^{k-1}\cdot\left[\sum_{t=0}^{k-1}\delta^t u_i(D)+\delta^{p+k}\sum_{t=0}^{r-1}\delta^t u_i(B)+\delta^{p+k+r}\cdot S_i\right].$$

解出 $S_i$ 得

$$S_i=\frac{(1-\delta)u_i(D)+q\delta^{p+1}u_i(B)(1-\delta^r)}{(1-\delta)(1-\delta+q\delta-q\delta^{p+r+1})}\,.$$

为消除理性节点的作弊动机,必须保证持续合作的收益不小于作弊收益期望 $S_i$,因此有

$$\sum_{t=0}^{\infty}\delta^t u_i(C)\ge S_i\,,$$

由上式化简可得

$$\frac{u_i(D)}{|u_i(B)|}\ge\frac{1-\delta+q\delta-q\delta^{p+1}}{q\delta(1-\delta^{p+r})}\qquad(5)$$

式(5)为激励一致性条件的概率扩展形式.当 $q$=1 时,其与式(4)完全一致;而当 $q$=0 时,整个博弈退化成单阶

段转发博弈.由式(5)可见,当$\delta$和 $q$ 均$\in(0,1)$时,右端对 $q$ 的偏导非正,因此,式(5)将随 $q$ 的增大而变得更容易满足,这与直觉相符:检测概率越低,惩戒机制效率就越低,对作弊也就越有利.

值得指出的是,$q$ 值一般由具体的作弊检测机制决定,考虑到 $q$ 随拓扑、信道状况的变化特性,如节点密度及干扰等随机因素,每个节点面临的检测概率并不相同.从式(5)不难发现,根据全网最低检测概率 $q_{\min}$ 所配置的 $p$-$r$ 参数在应用于一般场合时同样有效,即当节点发现在最利己的条件下都不能牟利时,它显然不会作弊.

## 4 模型仿真及分析

### 4.1 仿真概述

在实际 Ad hoc 网络中,来自拓扑、流量及信道的随机性令节点的协作行为变得复杂化.为验证重复策略转发模型的协作增强效果,并考察稳定程度,本文在 JiST/SWANS[21]改进的基础上实现了一个仿真环境.

整个仿真环境由 3 部分要素构成:随机生成的网络拓扑 $G$、路由协议 $R$ 及本地行为检测协议 $D$.此外,输入还包括折现因子$\delta$、惩戒机制参数 $p$,$r$ 和作弊检测概率函数 $q$.其仿真步骤如下:

1) 生成 $N$ 个节点的随机拓扑 $G$.我们沿用了第 3.2 节实例中的参数,$N$ 默认取 20,网络平均直径为 6~8 跳;

2) 随机流量生成.随机挑选源节点以及非相邻的目标节点.任意一个节点在一轮协作时隙中均可发送 10 个报文;

3) $R$ 采用改进了的 Aodv[22]协议.在发送前,源节点将向目标发出显式的路由选定通告,以便沿途各节点统计转发数量,该计数将自动计入下一轮,直到发送完毕后被显式取消;

4) 节点转发决策.各节点依据当前转发数量 $n_i$ 和作弊检测概率 $q_i$,遵照式(5)对可行策略进行评估;其选择包括全部转发或全部不转发,但不包括选择性转发或随机转发,后两者将被 $D$ 检测为作弊;

5) $D$ 采用 Catch[10]协议,通过 Catch 中的 Anv 匿名确认机制实现邻居对作弊者的协同孤立.为不失一般性,我们在仿真过程中对其假设检验过程进行了扩展,用一个作弊检测概率函数 $q$ 来模拟其检测效率;

6) 流量发送与转发之后,节点状态随本地检测结果而改变,统计信息被收集.为简洁起见,路由及检测协议报文不计入转发数量.一轮协作时隙仿真结束.

在仿真过程中,每一类实验共进行 5 次,每次实验由 200 次随机拓扑组成,针对每一拓扑随机产生 400 次流量,并进行共计 10 000 轮仿真.其数据均为 5 次实验的平均值.

考虑到 Ad Hoc 网络传输质量(如传输速率、延迟等)随协作性的降低而产生的劣化本质上源于节点作弊所导致的网络可靠性削弱,我们认为,自组网络的整体可用性是节点协作效果最直接的体现.因此,我们着重考察了其对报文传输成功率的影响.仿真环境中,有效投送率(efficient delivery ratio,简称 EDR)被定义为:所有成功抵达目标的报文与实际有效发送报文的比值.当节点均处于协作状态时,其值将为 1,而当节点均作弊时,其值为 0.

本节首先考察了检测概率为 1 的情况,通过实验分析了节点耐心程度对协作效果的影响及惩戒机制的扩展性,然后验证了 $p$,$r$ 参数的协作性影响.最后进一步给出了检测概率不为 1 时的仿真结论.

### 4.2 自私节点比率对有效报文投送率的影响

首先,我们将网络中的节点分为永远合作节点和自私节点两类.当缺乏约束时,自私节点与邻居的交互将退化为单阶段转发博弈,随着其数量的增加,越来越多的传输路径被打断或网络被分割,从而降低全网的传输成功率.图 4 中,$\delta$=0 的曲线给出了上述情况的仿真.

其他 5 根曲线绘出了惩戒机制存在时的情况.可以看出,随着合作节点的增加,投送率较之不使用惩戒机制时有明显提高;当$\delta$=0.6 时,即便自私节点比率高达 80%以上,配置 $p$=2,$r$=2 也能确保 95%的数据包送抵目的地.鉴于自私节点比率为 1 时,网络协作性将降为最低,我们将在后文中着重考察所有节点均为自私节点的情况.

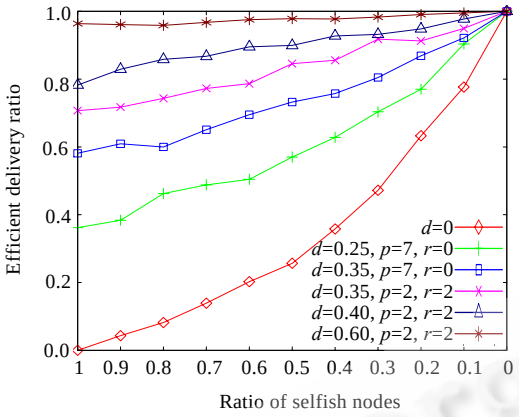


Fig.4 EDR vs. ratio of selfish nodes

图 4 自私节点比率对 EDR 的影响

### 4.3 节点耐心程度对协作性的影响及惩戒机制的可扩展性

图 5 为 $p$=7,$r$=0 时有效投送率随$\delta$的变化情况.图中,投送率随$\delta$的增加而明显提高,这说明整个网络的协作性随节点耐心的增长而得到了改善.当$\delta$趋近 1 时,考察曲线 $N$=20,由 $p$-$r$ 配置图 3 可知,当$\delta$>0.85 时,$p$=7,$r$=0 能够确保节点均愿意合作,图 5 证实了这一点,$\delta$>0.85 时,其 EDR 几近为 1;而当$\delta$接近 0 时,其 EDR 降低为 0.

图 5 还表明,随着 $N$ 的增加,单纯依靠孤立的消极惩戒机制的协作促进效果将显著削弱,进而使投送率明显下降.即便$\delta$=1 时,$N$=50 的 EDR 与 $N$=20 相比也下降了 20%,此时,$p$=7,$r$=0 已不能保证合作.因为 $N$ 越大,单一时隙中节点所需转发的报文 $n_i$ 越多,而惩戒机制的威慑力度却相对固定,因此,节点的协作倾向将随之恶化.这说明节点数量越多,越应该采取严厉的惩戒机制配置.

图 6 给出了 $p$=$r$=2 的情况.可以发现,投送率同样随$\delta$而增长,同时,随 $N$ 的增加而降低.注意到,当$\delta$趋于 0 时,各曲线的 EDR 并不为 0,这主要源于作弊节点重入网络时所提供的无偿服务,其贡献非常有限,最多不到 10%.对比图 5、图 6 可见,当 $r$≠0 时,$N$ 增长时投送率的降低程度并不及 $r$=0 时显著;而当$\delta$增长时,其对投送率的提高却比 $r$=0 时更为明显.这表明,实质性惩戒对协作性的促进不仅比一味消极孤立更有效,而且更具可扩展性.

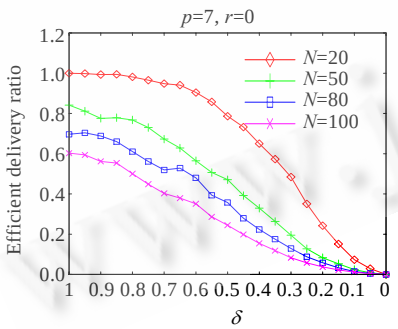


Fig.5 EDR vs. $\delta$ for $p$=7/$r$=0

图 5 节点耐心对 EDR 的影响($p$=7,$r$=0)

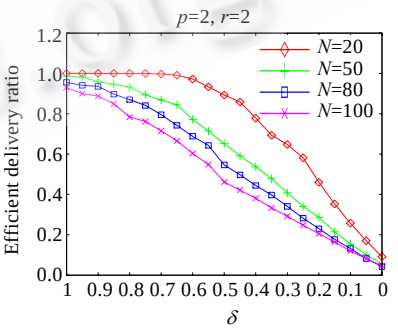


Fig.6 EDR vs. $\delta$ for $p$=2/$r$=2

图 6 节点耐心对 EDR 的影响($p$=2,$r$=2)

### 4.4 机制参数对协作性的影响

图 7 给出了 $r$=0 时 $p$ 的取值对有效投送率的影响,它同时给出了不同节点耐心程度时的情况.可以看出,增加 $p$ 将有助于提高网络协作程度.由于 $r$=0,因此,无论$\delta$取值如何,$p$=0 时的 EDR 均为 0.当$\delta$=0.85 时,$p$≥7 时的投送率已几近为 1,这与图 3 相符.由图 3 还可看到,当$\delta$取 0.7 等值时,不能保证所有节点合作,因此图 7 中,其 EDR

将始终达不到 1.$\delta$取值越低,则 $p$ 增长的积极影响就越有限.当$\delta$=0.3 时,增加 $p$ 最多只能将投送率提高至近 40%.

图 8 为 $r$=2 时 $p$ 对投送率的影响情况.命题 2 表明,当 $r\neq0$ 时,增加 $p$ 反而会降低网络的协作性.图 8 证实了这一点.当$\delta$取值较高时,这一弱化并不明显;而当节点耐心较低时则较为显著:曲线$\delta$=0.3 在 $p$=0 和 $p$=9 时,其投送率相差近 25%.由图还可见,无论 $p$ 为何值,$\delta$=0.85 时的投送率始终为 1;而$\delta$=0.7 时的投送率则直到 $p$>2 时才降至 1 以下.上述结论均与图 3 一致.

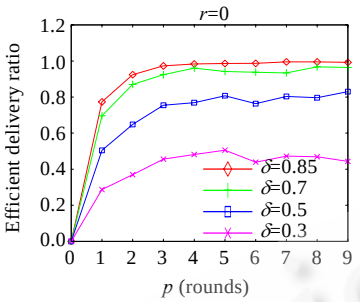


Fig.7 Effective delivery ratio vs. $p$ for $r$=0

图 7 参数 $p$ 对有效投送率的影响($r$=0)

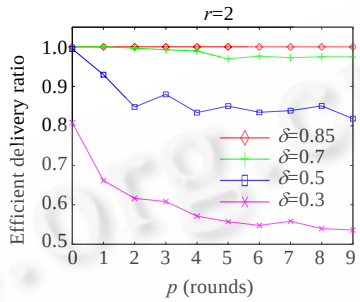


Fig.8 Effective delivery ratio vs. $p$ for $r$=2

图 8 参数 $p$ 对有效投送率的影响($r$=2)

图 9 表明,与增加 $p$ 相比,增加 $r$ 将会对节点间的协作性起到显著的促进作用,而这一效果在节点耐心程度较低时尤为明显.以$\delta$=0.3 为例,对比图 7 和图 9,由前者可知,当 $p$=2,$r$=0 时,其投送率只有近 40%,单纯通过增加 $p$,其 EDR 提高不到 10%;而后者则表明,当我们增加 $r$ 时,却能将 EDR 再提高 30%以上.上述观察有力地说明:是否存在着重入阶段,对于惩戒机制协作增强效果的影响非常显著.

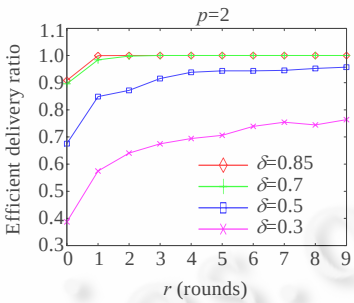


Fig.9 Effective delivery ratio vs. $r$ for $p$=2

图 9 参数 $r$ 对有效投送率的影响($p$=2)

### 4.5 作弊检测效率对协作性的影响

#### 4.5.1 作弊检测及孤立机制仿真

我们采用了 Catch 的 Anv 匿名邻居确认机制来实现不受作弊者行为影响的协同孤立.同时,使用了一个作弊概率检测函数 $q$ 作为仿真输入来模拟不同检测机制的效率.其中,Anv 机制的仿真步骤如下.

1) 在一轮流量转发之前,节点 $te$ 的每一个邻居 $t$ 均匿名广播一个随机令牌的散列;

2) $te$ 必须无条件重放该消息,以便所有邻居均能获知,否则,$t$ 将拒绝为 $te$ 提供后继服务;

3) 当一轮转发结束后,每一邻居 $t$ 将根据自身侦听结果来判断 $te$ 是否作弊;

4) 如果 $t$ 认为 $te$ 正常,$t$ 将以匿名广播方式公开令牌明文,并由 $te$ 重放;反之,则拒绝公开明文;

5) 当其他邻居发现没有收到某些散列的明文时,即可断定至少有 1 个邻居认为 $te$ 作弊,因此从下轮开始,所有邻居对 $te$ 实施联合孤立.同时,$te$ 亦可得知邻居个数及其是否认为自己在作弊.

上述机制有效的前提在于其消息匿名性.研究表明,采用信号强度检测对匿名邻居进行选择性区分的作弊

策略将对其产生较大负面影响,从而降低作弊检测概率[10].而邻居数量越多,信道越嘈杂,接收能级重叠范围越广,则越不容易区分其邻居,检出作弊行为的几率就越高.事实上,这体现出了基于 Watchdog 的本地检测机制的一个显著共性[10]:邻居数量越多,网络局部节点密度越大,则异常行为的检测概率越高.

鉴于采用不同统计检验方式的 Watchdog 机制可能具备不同的作弊检测效率,为体现其对于整体协作性的本质影响,同时不失一般性,我们使用了一个检测作弊概率函数 $q(m)$,$m$ 为邻居数量,且 $q(m)$随 $m$ 正相关.当节点作弊时,其邻居将以 $q(m)$的概率达成一致并对其进行惩罚.

4.5.2 理想化固定检测概率的协作性影响

为便于比较,我们首先考察了一个最悲观的理想化情况,即所有节点均面临相同的最低检测概率 $q_{\min}$ 的场合,此时,$q(m)$与邻居数量无关.当检测概率处处最低时,任意一个节点作弊而不被发现的可能性最大,因此,整个网络的协作性将达到降低检测概率所能达到的下限.

图 10 和图 11 给出了固定检测概率场合下 $q_{\min}$ 随节点耐心对投送率所造成的影响.可以看出,无论 $r$ 是否为 0,有效投送率均随 $q_{\min}$ 而下降,这与直觉一致:检测概率的降低将削弱惩戒机制对自私行为的威慑;同时,由图 10 和图 11 可见,当节点非常耐心时,$q_{\min}$ 的降低对 EDR 的负面影响有限,但随着 $\delta$ 的减少,其协作性削弱将日益明显.

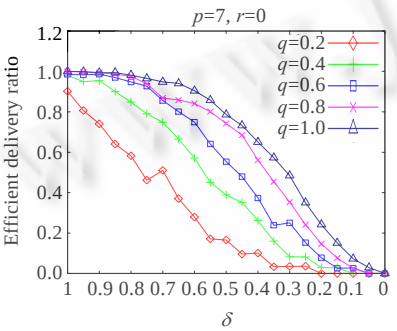


Fig.10 EDR vs. $\delta$ for fixed detecting probability

图 10 固定检测概率随$\delta$对投送率的影响

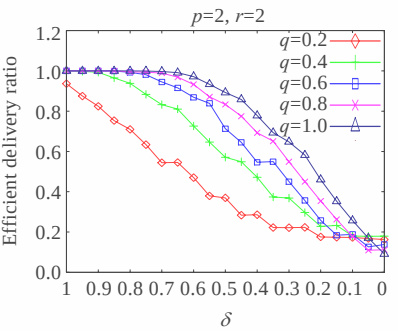


Fig.11 EDR vs. $\delta$ for fixed detecting probability

图 11 固定检测概率随$\delta$对投送率的影响

图 12 和图 13 分别给出了不同 $q_{\min}$ 场合下 $p$-$r$ 参数对协作促进效果的影响,其$\delta$均取 0.85.图 12 说明,当 $r$=0 时,在相同 $p$ 参数下,EDR 随检测概率明显降低,尤其当 $p$ 值较小时.当 $p$=9 时,$q_{\min}$=0.2 较 $q_{\min}$=1 的投送率也下降了近 30%.这说明,当 $r$=0 时,单纯增加 $p$ 并不足以抵消检测概率降低而导致的协作性损失.

图 13 则表明,当 $r\neq0$ 时,随着 $r$ 的增长,惩戒机制抵御检测概率降低的能力也随之增强.当 $r$ 增长至一定程度时,即便在检测概率处处最低的情况下,$q_{\min}$ 的降低对协作性的削弱也几乎可以忽略.以 $q_{\min}$=0.2 为例,当 $r$>8 时,其投送率已几近为 1.由于此时惩戒非常严厉,这使得理性节点即使在作弊检测概率很小的情况下也不敢贸然犯险.

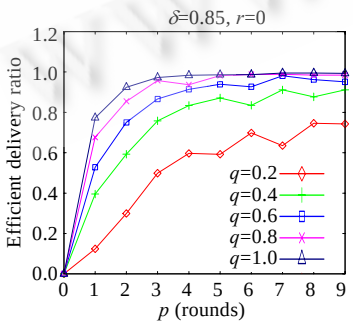


Fig.12 EDR vs. $p$ for fixed detecting probability

图 12 $p$ 随固定检测概率对投送率的影响

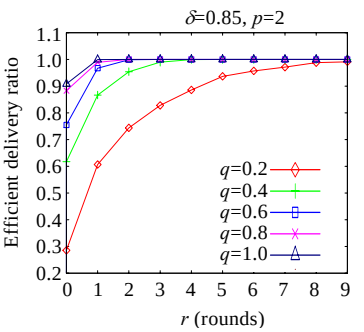


Fig.13 EDR vs. $r$ for fixed detecting probability

图 13 $r$ 随固定检测概率对投送率的影响

4.5.3 对不同检测概率函数的非敏感性

为了验证实际网络中随邻居数量增长的作弊检测概率的影响,我们首先考虑了 $q(m)$随 $m$ 线性增长且当 $m\geq 10$ 时恒为 1 的情况,并假设此刻 $m$ 的增长对检测概率的改善是均等的.

考虑在某些实际场合中,$q(m)$为阈值形式更为合适:当邻居较少时,$m$ 的增长对检测概率的影响并不显著;而当超过某临界值时,检测概率将迅速提高.为体现这种一般化的情景,我们采用一个 $S$ 形函数来描述 $q(m)$:

$$q(m)=\frac{1}{1+e^{w(d-m)}}.$$

式中的 $w$ 用来表示 $S$ 形函数的陡峭程度,$w$ 值越大,则 $q(m)$越呈现出阈值形态;$d$ 为阈值中点,当 $m=d$ 时,$q(m)$为 0.5.我们考察了两类情况:一类为 $w=\ln(4)/(2-d)$时的情况,不妨将此时的 $q(m)$记为 $sigmoid(d)$;而另一类则直接取 $w=1.5$,$d=3.5$,记为 $normal()$.二者的区别在于,当 $m\geq 2$ 时,$sigmoid(d)$能够保证 $q(m)$至少在 0.2 以上($m=1$ 的节点无须考虑是否参与转发);而 $normal()$则更接近现实情况,它取 3.5 为中点,当 $m>6$ 时近似为 1.

图 14 和图 15 给出了不同检测概率函数在不同$\delta$值下对有效投送率的影响.可以看出,当 $q(m)$为线性函数或 $sigmoid(d)$时,由于其 $m\geq 2$ 时的检测概率均大于等于 0.2,因此,其投送率均比 $q_{\min}=0.2$ 时要高,但都比 $q_{\min}=1$ 时要小;另一方面,由于 $normal()$取值小于 $sigmoid(3)$,因此,其投送率也低于后者.实验表明,尽管检测概率函数的具体形式及其定量的仿真结果各有不同,但协作性随检测机制效率的提高而得到增强这一定性结论并没有改变.

为体现 $r$ 的增加对实际检测概率降低的抑制作用,图 15 给出了 $p=2$,$r=7$ 的情况.从图 13 可知,在 $q(m)=0.2$ 的场合下,当 $p=2$,$r=7$ 且$\delta=0.85$ 时,其 EDR 在 95%以上;图 15 则表明,在所有 $q(m)$始终高于 0.2 的情况下,随$\delta$增长的投送率均先于 $q=0.2$ 达到 1.这不仅再次说明了严厉的惩戒机制能在很大程度上抵消较低检测概率对协作性的削弱,而且也验证了可根据较低的检测概率来配置 $p$-$r$ 参数,从而在一般场合下实现协作性增强的结论.

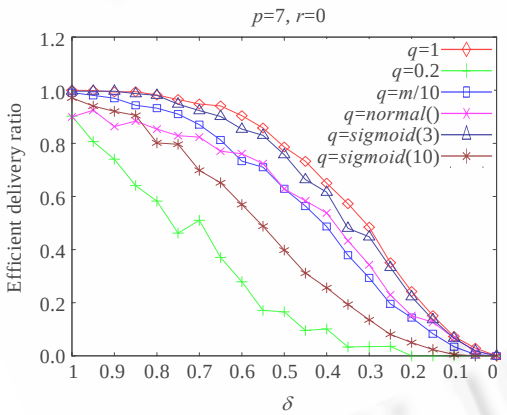


Fig.14 EDR vs. $\delta$ for different probability function

图 14 不同检测概率函数随 $\delta$ 对投送率的影响

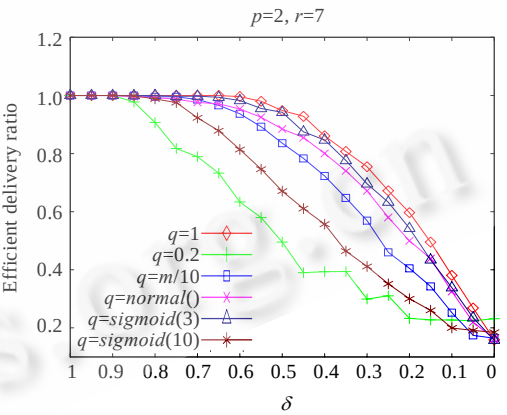


Fig.15 EDR vs. $\delta$ for different probability function

图 15 不同检测概率函数随 $\delta$ 对投送率的影响

## 5 模型对比与讨论

本节将对文献[17,19,20]等 3 个与本文工作最为接近的博弈论协作分析模型进行对比论述.

在文献[17]中,作者提出了一个基于拓扑相关性的协作模型,其研究主要针对自发均衡,即考察在特定拓扑条件下,不采用额外促进机制来实现转发协作的可能性,而本文研究则主要针对如何以主动方式来实现协作激励;作者给出了一个基于拓扑依赖图的元模型,并得出了若干均衡条件,但这些条件很难直接应用,因为其判定依赖于全局拓扑信息,而这一局限本质上源于作者所采用的节点间相互博弈的研究角度;在本文中,我们采用了节点与邻居间博弈的建模方式,与前者相比,其本地化视角更有利于简化决策分析和相关机制设计,从而更具实用性.此外,由于作者侧重于从拓扑关系方面考察协作性,因此没有考虑节点获利期望.最后作者得出结论,在随机网络中以偶然形式满足拓扑条件,实现自发均衡的概率很小,为保障合作,协作增强机制几乎总是必需的.

文献[19]中,作者提出了一种针对不同会话能级来调整节点转发率的协作模型.其节点与网络博弈的建模角度与我们的基本相似,但分析思路却存在本质不同.他们采用的是一种根据历史记录来平衡节点/网络相互贡献的方式,而本文则提出通过影响节点对未来收益的估计来引导其协作,我们认为,后者在重复转发场景中更能反映出节点动机的不同.作者在文中对各能级的优化转发率(normalized acceptance rate,简称 NAR)进行了求解,并提出了一种收敛于 NAR 的转发算法 GTFT.然而,为计算 NAR,必须获知所有节点的能级及其作为源或中继的概率分布,作者并没有指明如何获得这些信息;而在本文的模型中则并没有利用任何全局信息假设,其惩戒机制完全可以是全分布式的.另一方面,由于将不同节点归纳成若干能级,GTFT 忽略了个体的差异性和机制的公平性:仿真表明,个别节点在能级为 $i$ 的会话中的重复作弊行为将极大地降低所有能级为 $i$ 的会话吞吐率,即便其中继路径完全由合作节点组成;这对合作节点并不公平,同时也存在着较大的安全隐患;最后,GTFT 也没有考虑协作保障机制,它不能确保节点履行转发承诺;而在我们的模型中,个别作弊行为并不会导致大面积诚实节点被处罚;我们直接采用了本地行为检测的惩戒机制,其本身即具有良好的协作保障性,同时便于与其他安全机制兼容.

与本文提出的孤立/重入机制不同,文献[20]给出了一种以拥塞信道手段来强迫协作的激进思路.其分析角度及重复博弈假设与本文类似,但不同的是,作者使用的是均值准则而不是折现准则,因此,并没有考虑将来利益重视程度的影响.文中作者还从理论上证明了均衡的存在性,但却没有给出具体机制;事实上,为拥塞作弊者,惩罚者必须付出数倍于平时的能耗,同时将妨碍所有 2 跳邻居的通信,作者没有指明如何来平衡上述效率与公平性的损失及其协作性收益,也没有给出仿真验证,因此,其思路的可行性与安全性仍有待评估.我们认为,其研究的价值在于,它明确指出了孤立手段无法有效应对节点与邻居共谋;鉴于本文主要关注理性节点的个体行为,因此没有考虑这一情况.采取孤立-拥塞复合机制、以联盟博弈思路来考虑共谋问题是我们正在尝试的工作.

## 6 结 论

本文针对 Ad Hoc 节点转发过程,提出了一个基于本地检测及孤立惩戒机制的重复博弈转发模型.与已有的工作相比,该模型充分考虑了节点理性,提出以降低作弊者预期收益、利用其对后继惩罚的恐惧来敦促协作,并分析了合作期望、惩戒机制与检测机制效率对协作的影响.仿真结果表明,通过合理选择惩戒参数,可以有效抵御网络规模的增长及节点耐心程度、检测机制效率的降低所导致的协作性削弱,提高自组网络的可靠性能.

值得指出的是,本文研究的目的在于提出一个考察节点转发协作性的分析框架,从模型角度深化对转发动机的理解,进一步发掘协作激励可利用的现实因素,并据此定义实现优化协作的交互策略,从而为转发保障协议设计提供指导.将本文的结论整合进 Catch[10]协议,并在现实环境中考察其协作增强效果是我们下一步的工作.

**References**:

[1] Urpi A, Bonuccelli M, Giordano S. Modeling cooperation in mobile ad hoc networks: A formal description of selfishness. In: Proc. of the Int'l Symp. on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOPT 2003). 2003. ftp://ftp-sop.inria.fr/maestro/WiOpt03PDFfiles/urpi10.pdf

[2] Marti S, Giuli T, Lai K. Mitigating routing misbehavior in mobile ad hoc networks. In: Proc. of the ACM MobiCom 2000. New York: ACM Press, 2000. 255−265.

[3] Elkind E, Sahai A, Steighlitz K. Frugality in path auctions. In: Proc. of the ACM-SIAM Symp. on Discrete Algorithms. Philadelphia: Society for Industrial and Applied Mathematics. 2004. 701−709.

[4] Anderegg L, Eidenbanz S. Ad hoc VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish Agents. In: Proc. of the ACM MobiCom 2003. New York: ACM Press, 2003. 245−259.

[5] Osborne MJ, Rubinstein A. A Course in Game Theory. Cambridge: MIT Press, 1994.

[6] Afergen M, Using repeated games to design incentive-based routing systems. In: Proc. of the IEEE INFOCOM 2006. Washington: IEEE Computer Society, 2006. 1−13.

[7] Buttyan L, Hubaux J. Stimulating cooperation in self-organizing mobile ad hoc networks. ACM/Kluwer Mobile Networks and Applications, 2003,8(5):579−592.

[8] Zhong S, Chen J, Yang YR. Sprite: A simple cheat-proof credit-based system for mobile ad hoc networks. In: Proc. of the IEEE INFOCOM 2003, Vol.3. Washington: IEEE Computer Society, 2003. 1987−1997.

[9] Huang E, Crowcroft J. Rethinking incentives for mobile ad hoc networks. In: Proc. of the ACM SIGCOMM Workshop on Practice and Theory of Incentives in Networked Systems 2004. New York: ACM Press, 2004. 191−196.

[10] Mahajan R, Rodrig M. Sustaining cooperation in multi-hop wireless networks. In: Proc. of the USENIX NSDI 2005 Symp. on Networked Systems Design & Implementation (NSDI 2005). Berkeley: USENIX Association, 2005. 231−244.

[11] Buchegger S, Boudec Le JY. Performance analysis of the confidant protocol: cooperation of nodes fairness in dynamic ad-hoc networks. In: Proc. of the ACM Int'l Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc 2002). New York: ACM Press, 2002. 226−236.

[12] Michiardi P, Molva R. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Proc. of the IFIP-Communication and Multimedia Security Conf. 2002. 107−121.

[13] Hu JY. Cooperation in mobile ad hoc networks. Technical Report, CS-TR-050111, Florida State University, 2005. http://www.cs.fsu.edu/research/reports/TR-050111.pdf

[14] Anderegg L, Eidenbenz S. On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks. In: Proc. of the ACM MobiCom 2005. New York: ACM Press, 2005. 117−131.

[15] Cai J, Pooch U. Play alone or together—Truthful and efficient routing in wireless ad hoc networks with selfish nodes. In: Proc. of the IEEE Int'l Conf. on Mobile Ad-hoc and Sensor Systems (MASS 2004). Washington: IEEE Computer Society, 2004. 457−465.

[16] Wu MY, Shu W. RPP: A distributed routing mechanism for strategic wireless ad hoc networks. In: Proc. of the IEEE Global Telecommunications Conf. (GlobeCom 2004). Washington: IEEE Computer Society, 2004. 2885−2889.

[17] Felegyhazi M, Hubaux JP, Buttyan L. Nash equilibria of packet forwarding strategies in wireless ad hoc networks. IEEE Trans. on Mobile Computing, 2006,5(5):463−476.

[18] Altman E, Kherani A. Non-Cooperative forwarding in ad-hoc networks. In: Proc. of the IFIP Networking 2005. Heidelberg: Springer-Berlin, 2005. 486−498.

[19] Srinivasan V, Nuggehalli P. Cooperation in wireless ad hoc networks. In: Proc. of the IEEE INFOCOM 2003. Washington: IEEE Computer Society, 2003. 808−817.

[20] Levin D. Punishment in selfish wireless networks: A game theoretic analysis. In: Proc. of the ACM Workshop on the Economics of Networked Systems (NetEcon 2006). 2006. http://www.cs.duke.edu/nicl/netecon06/papers/ne06-punishment.pdf

[21] Java in simulation time/Scalable wireless ad hoc network simulator. 2005. http://jist.ece.cornell.edu/

[22] Perkins C, Royer E. Ad-Hoc on-demand distance vector routing. In: Proc. of the IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99). Washington: IEEE Computer Society, 1999. 90−100.

陆音(1978－),男,湖南湘潭人,博士生,主要研究领域为无线自组网络,下一代互联网 NGI.

石进(1976－),男,博士生,主要研究领域为网络安全,系统安全.

谢立(1942－),男,教授,博士生导师,CCF 高级会员,主要研究领域为分布式系统,信息安全.