

基于博弈论的移动自组织网络的信任管理方法

郭晶晶¹, 马建峰^{1,2}, 李琦¹, 万涛³, 高聪¹, 张亮¹

(1. 西安电子科技大学 计算机学院, 陕西 西安 710071; 2. 通信信息控制和安全技术重点实验室, 浙江 嘉兴 314033;
3. 华东交通大学 信息工程学院, 江西 南昌 330013)

摘要: 采用博弈论的思想为节点间的间接信任信息获取建立了博弈模型, 提出了惩罚机制并给出了节点的效用函数。此外, 建立了信任演化的复制动态方程来研究在不同参数下节点的演化稳定策略。通过实验验证了方法的正确性及有效性, 证明该模型可使节点为了获得最大利益而在间接信任评估过程中趋于选择同邻居节点合作, 从而提高信任管理系统的可用性与有效性, 同时验证了节点在不同前提条件下的演化稳定策略。

关键词: 移动自组网; 信任管理; 演化博弈论; 复制动态方程

中图分类号: TP309

文献标识码: A

文章编号: 1000-436X(2014)11-0050-09

Game theory based trust management method for mobile ad hoc networks

GUO Jing-jing¹, MA Jian-feng^{1,2}, LI Qi¹, WAN Tao³, GAO Cong¹, ZHANG Liang¹

(1. School of Computer, Xidian University, Xi'an 710071, China;

2. Science and Technology on Communication Information Security Control Laboratory, Jiaxing 314033, China;

3. School of Information Engineering, East China Jiaotong University, Nanchang 330013, China)

Abstract: A game model is proposed for the indirect trust information obtaining process. A suitable punishment mechanism and design the utility function for nodes in a MANET is given. Moreover, with evolutionary game theory, the trust evolution of nodes using replicator dynamic equation is analyzed and several theorems to illustrate preconditions under which each evolutionarily stable strategy can be achieved are proposed. Experiments verified the correctness and effectiveness of proposed method and simulated the dynamic evolutionary trend of the nodes under different parameters which experimentally proves the proposed theorems.

Key words: MANET; trust management; evolutionary game theory; replicator dynamic equation.

1 引言

移动自组网 (MANET) 是由一组带有无线通信收发装置的移动终端节点组成的一个多跳、临时、无中心的网络, 网络中每个终端都可以自由移动, 因此网络的拓扑结构会动态变化, 节点间的通信不依赖于任何固定基础设施, 而是基于节点间的互相协作保持网络互连。保证移动自组网的安全是

MANET 得到广泛应用的前提, 信任管理提供了有效的机制来评估网络中某一节点的可靠性, 目前国内外已有许多针对移动自组网中的信任管理机制^[1~7]的研究。由于移动自组网拓扑结构的高度动态性, 在大多数研究工作中, 评估者通过主观观察及来自邻居节点的间接信任推荐来计算一个节点的信任度。然而, 在实际情况中, 节点出于节省资源以及保护隐私等方面的考虑, 其行为会呈现出一定的理

收稿日期: 2014-08-14; 修回日期: 2014-10-16

基金项目: 长江学者和创新团队发展计划基金资助项目(IRT1078); 国家自然科学基金委员会—广东联合基金重点基金资助项目(U1135002); 国家科技部重大专项基金资助项目(2011ZX03005-002); 中央高校基本科研业务费基金资助项目(JB42001-12)

Foundation Items: Program for Changjiang Scholars and Innovative Research Team in University(IRT1078); The Key Program of NSFC-Guangdong Union Foundation (U1135002); Major National S&T Program(2011ZX03005-002);The Fundamental Research Funds for the Central Universities (JB142001-12)

性倾向,即拒绝响应其他节点的间接信任信息请求消息,同时希望其他节点都可以对其发出的间接信任信息请求消息进行响应来追求自身利益最大化,这势必会影响到信任管理系统的良好运行。当大量节点都表现出自私行为时,信任管理系统的效果将会大打折扣,以至于节点做出错误的信任决策而造成损失。因此,研究一种激励移动自组网中节点主动参与到提供间接信任证据过程的方法,提高现有信任管理方案的效果从而保障网络中节点的利益是非常必要的。

针对上述问题,在假设节点是理性的基础上,提出了一种基于进化博弈论的惩罚机制来激励网络节点自愿与其他节点合作参与到间接信任推荐的过程中,对节点间的协作过程进行了建模与分析,对比节点采取不同策略(合作/非合作)时的效用,并得出了激励一致性条件。同时,对该机制的稳定性进行分析,并通过实验验证其有效性。

不同于常规信任管理方法中注重信任评估算法的有效性,本文强调了信任信息来源的保障问题,如何才能获得足够多的信任信息以供节点推理计算出更加准确的结果来驱动其做出合理的行为决策,这一点对新加入网络的节点更为重要。

本文采用博弈论为信任信息获取过程建模,并可以根据具体网络环境与特点来调整模型参数,使信任系统达到最佳状态。

2 背景与相关工作

Marsh 在 1994 年首先系统地阐述了信任的形式化问题,并着眼于信任的主观性给出了具体的信任模型^[8]。目前,信任已成为了计算机网络安全中的研究热点,国内外的研究学者对移动自组网中的信任管理机制也已经进行了一系列研究^[9-11]与分析^[12,13]。信任建立过程主要包括了 4 个阶段:信任初始化、证据收集、信任计算与决策、信任更新。其中,证据收集过程中,节点会收集来自直接观察和间接观察的信息^[14-16],然后根据这些信息计算与分析得出其他节点的综合信任度 $T = \omega_{\text{direct}} t_{\text{direct}} + \omega_{\text{indirect}} t_{\text{indirect}}$, ω_{direct} 和 ω_{indirect} 分别是直接信任与间接信任对综合信任度的影响因子, $\omega_{\text{direct}} + \omega_{\text{indirect}} = 1$ 。间接信任信息来自于网络中其他节点提供的推荐信息。然而,实际情况中,节点出于资源有限以及保护隐私等方面的考虑,其行为会呈现出一定的理性趋势,即拒绝响应其他节点的请求,同时希望其他节点都可以

对其发出的请求进行响应来追求自身利益最大化,当大量节点都表现出自私行为时,信任管理系统的效果将会大打折扣,以至于节点做出错误的信任决策而造成损失。这一现象属于博弈论中的经典问题“囚徒困境(prisoner's dilemma)”,因此可以运用博弈理论针对节点的自私行为设计合理的激励机制使节点自愿加入到间接信任推荐过程中,保证信任管理机制的有效性。

博弈论作为应用数学的一个分支,主要研究理性参与者间存在冲突与合作时的决策数学模型^[17]。一个理性的参与者总会采取能够使自己获得最大效用的策略,这里的效用为其所得利益与损失之差。目前,已有大量基于博弈论的研究对网络中的交互行为进行建模与分析。闻英友等^[18]提出了一种基于博弈论的移动自组网惩罚机制,使一个节点为其他节点转发信息的所得效用大于采取不合作策略的效用,从而保障自组网的可用性及整体网络性能。Yu 等^[19]运用博弈论对移动自组网中的合作激励与安全问题进行了分析,提出了基于信誉的防欺诈、抗攻击的合作激励策略,可以有效激励节点选择合作策略。Shen 等^[20]利用博弈论分析了网络中的节点采用全局信任管理机制来控制有害流量的行为,并提出了一种惩罚措施促使每个节点都为整个网络的良好运作贡献力量。Marcin 等^[21]利用演化博弈理论分析了网络规模与网络中节点的类型对节点间进行合作的影响。Li 等^[22]研究了 2 种合作执行机制(cooperation enforcement mechanisms)中的激励因素的有效性。

3 间接信任信息获取博弈模型

移动自组网的拓扑动态性决定了网络中的节点在计算评估其他节点的信任度时需要向其邻居节点发出间接信任信息请求消息并期望邻居节点能够积极响应,使其决策结果更加准确。当间接信任信息在最终评估结果中所占比重越重时,其带给该节点的利益也越多。当一个节点 A 收到了来自其他节点的间接信任信息请求时,节点 A 会选择对自己最有利的策略(响应或忽略), A 在网络中继续活动的时间以及来自其他节点的间接信任信息对其带来的利益都将是其考虑的因素,因此,可针对节点的预期活动时间与间接信任信息的影响因子来设计灵活的惩罚机制,以降低自私节点在该网络中活跃时期的整体收益来促成合作。

本文根据重复博弈理论,将邻居节点间的间接信任信息获取过程看作一个多次博弈过程,建立间接信任信息获取重复博弈模型,对节点的整体收益进行分析,求解纳什均衡,最终得出激励一致性条件。

3.1 单阶段博弈

对邻居节点间的间接信任信息获取过程进行建模,为本文所讨论的移动自组织网络做出如下假设。

1) 整个移动自组网由 N 个理性节点构成,节点会向其相邻节点发送关于某一节点的间接信任信息的请求消息,此过程为直接通信,不涉及报文转发。

2) 整个系统时间由一系列离散的时隙 t 构成,在每个时隙内,单阶段博弈都会发生,每个节点至少会向邻居节点发送一个间接信任信息请求消息,且在同一时隙内,网络的路由状态不会发生变化,确保每一消息均能抵达目标节点。

3) 所有节点发出一个消息消耗相同的能量 c ,接收消息的能耗忽略不计。

下面定义移动自组网中节点间的单阶段间接信任信息获取博弈模型。

定义 1 单阶段间接信任信息获取博弈的基本式为一个三元组, $G = (P, S, \mu)$, 其中, P 为博弈参与者集合(网络中 2 个邻居节点), $P = \{i, j\}, i, j \in N$, (N 是网络中的节点集合), S 是每个节点可以采取的策略集, $S = \{s_1, s_2\} = \{\text{合作}(C), \text{不合作}(UN)\}$, μ 为节点的效用函数。

定义一个节点 i 在时隙 t 的效用函数为

$$\mu_i(S'_i, S'_j) = S'_j b_i - S'_i (c n_i^s + p) \quad (1)$$

其中, S'_i, S'_j 分别是节点 i 和节点 j 在时隙 t 时选择的博弈策略; b_i 是当邻居节点选择合作策略时,节点 i 的收益, $b_i = \delta e^{w_m^i}$, 其中, δ 是由于邻居节点合作 i 可以得到的最大收益, w_m^i 为间接信任信息对节点 i 的信任决策的影响因子, $0 \leq w_m^i \leq 1$; n_i^s 是节点 i 在一个时隙内发出的响应其他节点的间接信任信息的消息数量; p 是节点 i 选择合作策略后,因为揭露隐私而造成的损失。

类似地,节点 j 的效用函数就是 $\mu_j(S'_i, S'_j) = S'_i b_j - S'_j (c n_j^s + p)$ 。

如果节点 i 选择合作策略,那么它会诚实地响应其他节点的间接信任请求消息,此时 $S_i = 1$, 否则它会忽略该消息不做任何事情, $S_i = 0$ 。当 2 个邻居

节点进行单阶段博弈时,博弈双方的收益矩阵如表 1 所示。

博弈节点 (i, j)	j 合作 (C)	j 不合作 (UN)
i 合作 (C)	$(b_i - c n_i^s - p, b_j - c n_j^s - p)$	$(-c n_i^s - p, b_j)$
i 不合作 (UN)	$(b_j, -c n_i^s - p)$	$(0, 0)$

根据 2×2 双矩阵对策的求解方法,可以得出当 $b_k > c n_k^s + p, k \in \{i, j\}$ 时,博弈双方的优超策略都是不合作策略,此时博弈达到纳什均衡。网络中所有节点都无法获取来自其邻居节点的间接信任信息,那么信任管理机制中的间接信任就丧失了功效,且所有节点的收益为 0,这便形成了典型的“囚徒困境”。

3.2 重复间接信任信息获取博弈

为了打破上节所述的困境,必须引入合适的惩罚策略,本文采用文献[18]中提出的严厉针锋相对策略,在时隙 t 时,若某一节点采取了不合作策略,那么在接下来的 T 个时隙中,所有邻居节点将对其采取不合作策略作为惩罚,并且在惩罚期内,该节点必须无条件选择合作策略,否则,惩罚将变为无限期。在惩罚期结束后,节点的自私行为将被遗忘。

某一节点如果在一次博弈结束后仍然会待在目前所在网络中,那么势必会进行连续的博弈过程,那么它必然会考虑之前的行为为其将来的利益带来的影响,因此本节将前面介绍的单阶段博弈过程扩展为一个重复博弈的过程。

定义 2 记重复间接信任信息获取博弈为 $G(L)$, L 为节点预期还要在该网络中活动的时隙数,某一节点在 $G(L)$ 中的收益为各时隙收益的贴现值之和,那么节点 i 在整个重复博弈中的预期收益可表示为

$$U_i = \mu_i(S_i^1, S_j^1) + \sigma \mu_i(S_i^2, S_j^2) + \dots = \sum_{t=0}^L \sigma^t \mu_i(S_i^t, S_j^t) \quad (2)$$

其中, σ 为贴现因子, $0 \leq \sigma \leq 1$, 节点 i 预计在该网络中活跃的时间越久,那么节点越注重长期利益,相应的 σ 也越大,反之越注重眼前利益, σ 越小。在本文中,令 $\sigma = -\frac{1}{L+1} + 1$ 。一般来说,相对稳定的网络中节点对应的 σ 较大,而临时构建的、动态性强的网络 σ 较小。

接下来，分析节点采取不同策略时所得的预期收益。为了便于分析，假设节点在每个时隙内发送的消息数都相等，根据前面叙述，可知如果理性节点 i 在当前时隙选择了不合作策略，那么其预期收益为

1) 若 i 不接受惩罚继续选择不合作

$$U_i^{UN-1} = \mu_i(UN, C) + \sigma \sum_{t=1}^L \sigma^t \mu_i(UN, UN) = \mu_i(UN, C) = b_i \quad (3)$$

2) 若 i 接受惩罚，但在惩罚期结束后继续选择不合作

$$U_i^{UN-2} = \mu_i(UN, C) + \sum_{t=1}^T \sigma^t \mu_i(C, UN) + \sigma^{T+1} (\mu_i(UN, C) + \sum_{t=1}^T \sigma^t \mu_i(C, UN)) + \dots = \sum_{k=0}^{L/(T+1)} \sigma^{k(T+1)} (\mu_i(UN, C) + \sum_{t=1}^T \sigma^t \mu_i(C, UN)) \quad (4)$$

若理性节点 i 在网络中活跃期间一直选择合作，则其预期收益为

$$U_i^C = \sum_{t=0}^L \sigma^t \mu_i(C, C) \quad (5)$$

为了激励理性节点采用合作策略，必须保证当其选择合作策略时所得收益大于选择不合作策略时所得收益。那么必须使式(6)成立。

$$\begin{cases} \sum_{t=0}^L \sigma^t \mu_i(C, C) \geq b_i \\ \sum_{t=0}^L \sigma^t \mu_i(C, C) \geq \sum_{k=0}^{L/(T+1)} \sigma^{k(T+1)} (\mu_i(UN, C) + \sum_{t=1}^T \sigma^t \mu_i(C, UN)) \end{cases} \quad (6)$$

在节点 i 做出决策前，必定会权衡 2 种选择带来的利益，如果上式成立，那么 i 必定会选择合作策略，否则将选择不合作策略。因此必须选择合适的参数来确保式(6)成立来激励节点间的合作。化简上式后得到

$$\frac{-\mu_i(C, UN)}{\mu_i(UN, C)} = \frac{|\mu_i(C, UN)|}{\mu_i(UN, C)} \leq \frac{(\sigma - \sigma^{T+1})}{(1 - \sigma)} \quad (7)$$

式(7)即为重复博弈的激励一致性条件，保证了每个单阶段子博弈中，博弈双方选择（合作，合作）策略为完美纳什均衡，从而整个重复博弈过程也出

于纳什均衡状态。由于式(7)的左端的取值依赖于 b_i 、 c 、 n_i^s ，而 b_i 的值取决于 ω_m^i 的值，假设 n_i^s 取全网节点响应间接信任信息请求消息的平均值， c 与 ω_m^i 由节点自身的状态以及所处环境所决定。式(7)左端的值由 σ 与 T 决定，设函数 $f(\sigma, T) = \frac{(\sigma - \sigma^{T+1})}{(1 - \sigma)}$ ，那么 $f(\sigma, T)$ ，如图 1 所示。

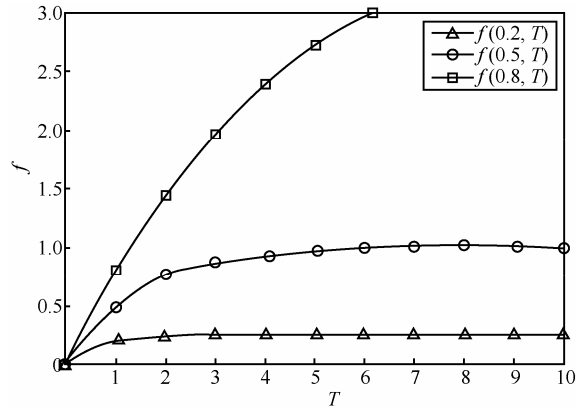


图 1 函数 $f(\sigma, T)$

4 间接信任信息获取博弈的演化稳定策略

本节将建立演化博弈模型来分析网络中节点达成均衡状态的演化过程，解释自私节点在该惩罚机制下由自私变为合作的演化过程，并分析该机制的稳定性。

文中提出的博弈模型中只有 2 个可选策略，即合作与不合作，各节点根据其他节点的策略来调整自己的选择来达到利益最大化。演化博弈模型中参与节点的收益矩阵如表 2 所示，其中

$$U(C, C) = U_i^C = \sum_{t=0}^L \sigma^t \mu_i(C, C) = \frac{1 - \sigma^{L+1}}{1 - \sigma} \mu_i(C, C)$$

$$U(C, UN) = \sum_{k=0}^{L/(T+1)} \sigma^{k(T+1)} (\mu_i(C, UN) + \sum_{t=1}^T \sigma^t \mu_i(UN, C)) = \frac{1 - \sigma^{L+1}}{1 - \sigma^{T+1}} \left(\mu_i(C, UN) + \frac{\sigma - \sigma^{T+1}}{1 - \sigma} \mu_i(UN, C) \right)$$

$$U(UN, C) = U_i^{UN-2} = \frac{1 - \sigma^{L+1}}{1 - \sigma^{T+1}} \left(\mu_i(UN, C) + \frac{\sigma - \sigma^{T+1}}{1 - \sigma} \mu_i(C, UN) \right)$$

$$U(UN, UN) = \sum_{t=0}^L \sigma^t \mu_i(UN, UN) = 0.$$

令 $\theta(t) = \{\theta, 1 - \theta\}$ 为时隙 t 时的混合策略， θ 代

表网络中选择了合作策略的节点的比例, 那么选择不合作策略的节点的比率为 $1-\theta$ 。根据演化博弈理论^[23], 选择合作策略的节点的期望收益为

$$u(s_1, \theta(t)) = \theta U(C, C) + (1-\theta)U(C, UN) \quad (8)$$

选择不合作策略的节点的期望收益为

$$u(s_2, \theta(t)) = \theta U(UN, C) + (1-\theta)U(UN, UN) \quad (9)$$

整个网络的平均收益为

$$\bar{u}(\theta(t), \theta(t)) = \theta u(s_1, \theta(t)) + (1-\theta)u(s_2, \theta(t)) \quad (10)$$

那么, 信任进化的复制动态方程为

$$\begin{aligned} F(\theta) &= \dot{\theta} = \theta(u(s_1, \theta(t)) - \bar{u}(\theta(t), \theta(t))) \\ &= \theta(1-\theta)U(C, UN) \end{aligned} \quad (11)$$

式(11)描述了演化系统中的协作群体动态。令 $F(\theta)=0$, 那么 $\theta_1=0, \theta_2=1$ 或 $U(C, UN)=0$ 为其解。根据演化稳定策略的特性, 一个稳定的状态必然可以抵抗微小的干扰, 这与微分方程的稳定性原理是一致的, 即当 θ 是一个稳定状态时, $F'(\theta) < 0$ 必然成立。下面计算该机制的演化稳定策略并分析其稳定性。

表 2 演化博弈参与节点收益矩阵

博弈节点 (i, j)	j 合作 (C)	j 不合作 (UN)
i 合作 (C)	$U(C, C), U(C, C)$	$U(C, UN), U(UN, C)$
i 不合作 (UN)	$U(UN, C), U(C, UN)$	$U(UN, UN), U(UN, UN)$

定理 1 当 $U(C, UN)=0$ 时, $\forall \theta \in [0, 1]$ 都是演化稳定均衡解。

证明 由于 $F'(\theta) = (1-2\theta)U(C, UN)$, 当 $U(C, UN)=0$ 时, 对于 $\forall \theta \in [0, 1]$, 有 $F'(\theta) = 0$, 意味着外界扰动并不会改变系统的状态, 因此系统处于稳定状态中, 因此 $\forall \theta \in [0, 1]$ 都是演化稳定均衡解。

当 $U(C, UN)=0$ 时, $\frac{1-\sigma^L}{1-\sigma^{T+1}}(\mu_i(C, UN) + \frac{\sigma-\sigma^{T+1}}{1-\sigma}\mu_i(UN, C)) = 0$, 因此满足 $L=0$ 或 $\frac{-\mu_i(C, UN)}{\mu_i(UN, C)} = \frac{\sigma-\sigma^{T+1}}{1-\sigma}$ 。

若 $L=0$, 即节点在当前时隙结束后会马上离开网络, 因此它不会再去关心选择合作或非合作策略来谋取更多利益, 那么节点的策略也必然不会改变。

若 $L \neq 0$, 那么由 $\frac{-\mu_i(C, UN)}{\mu_i(UN, C)} = \frac{\sigma-\sigma^{T+1}}{1-\sigma}$ 得到

$$\sum_{i=0}^L \sigma^i \mu_i(C, C) = \sum_{k=0}^{L/(T+1)} \sigma^{k(T+1)} (\mu_i(UN, C) + \sum_{i=1}^T \sigma^i \mu_i(C, UN)),$$

即节点选择合作策略与选择非合作策略的收益是相同的, 因此节点没有足够的动力去改变目前的策略, 系统将处于稳定状态。

定理 2 若 $U(C, UN) > 0$, 只有 $\theta=1$ 是演化稳定均衡解。

证明 因为 $F'(\theta) = (1-2\theta)U(C, UN)$, $F'(1) = -U(C, UN) < 0$, $F'(0) = U(C, UN) > 0$, 所以只有 $\theta=1$ 是演化稳定均衡解。

当 $\frac{1-\sigma^L}{1-\sigma^{T+1}} \left(\mu_i(C, UN) + \frac{\sigma-\sigma^{T+1}}{1-\sigma} \mu_i(UN, C) \right) > 0$, 即 $\frac{-\mu_i(C, UN)}{\mu_i(UN, C)} > \frac{\sigma-\sigma^{T+1}}{1-\sigma}$ 时, 节点选择合作策略会

比选择非合作策略得到的更多的利益, 即使节点目前所选的是非合作策略, 在经过多轮博弈后, 最终会选择合作策略以谋取最大利益。因此, 无论目前网络中的非合作节点的比例是多少, 最终该比例将会变为 0。

定理 3 若 $U(C, UN) < 0$, 只有 $\theta=0$ 是演化稳定均衡解。

证明 该定理的证明与定理 2 类似, 因此本文中不再赘述。该定理说明了如果 $U(C, UN) < 0$, 无论目前网络中合作节点的比例是多少, 最终该比例将会变为 0, 因为节点选择非合作策略会比选择合作策略得到更多的利益。

综上所述, 一个包含了间接信任的信任管理系统必须满足定理 2 来激励节点去选择合作策略, 从而保证整个网络的安全性与稳定性。同时, 在设计信任管理系统时必须避免满足定理 1 或定理 3, 否则节点将不会改变当前状态或经过多轮博弈后将选择非合作策略作为稳定状态, 导致信任管理系统的失效。

5 实验与讨论

通过实验来验证激励一致性条件的正确性和有效性, 以及间接信任信息获取博弈演化的正确性与稳定性。实验环境为 Intel 奔腾双核处理器 Q9550, 2.83 GHz, 4 GB 内存, Windows 7 操作系统, Dev-C++ 编程环境。采取的仿真方法如下。

随机生成网络拓扑结构, 假设仿真区域的大小为 $200 \text{ m} \times 200 \text{ m}$, 所有节点都随机分布在该区域中, 在每个时隙中, 每个节点都随机挑选其邻居节点生成间接信任信息请求消息, 每个节点在一个时隙内

均可发出随机数量的消息。当收到请求消息时，各节点根据当前状态，遵照式 (2) 对可行策略进行评估，确定最终的策略（响应或忽略请求）。每一次博弈结束后，系统记录参与节点的消息发送与回应情况，在下一时隙仿真时，各节点参照系统记录结果选取策略。在仿真过程中，每个实验进行 10 次，取 10 次结果的平均值。

如果一个信任管理系统中对某一节点的信任评估结果考虑了来自其他节点的间接信任推荐信息，那么节点间的相互合作将对信任评估结果产生积极的影响，若缺乏适当的惩罚机制，那么节点将根据利益最大化原则趋于拒绝提供相关信息，随着时间的推移，这样的自私节点将越来越多，越来越多的节点将无法获取间接信任信息，从而影响了信任评估结果，降低了信任管理机制的可用性。由于合作节点比率越高，节点的间接信任信息获取率也相应越高，因此以各节点的平均间接信任信息获取率来评价网络中节点的整体合作意愿，在本文中，将节点的平均间接信任信息获取率定义为 $\sum_{i=1}^N \frac{r_i}{s_i} / N$ ，其中， N 为网络中的节点数量， r_i 为节点 i 收到的间接信任信息响应消息的数量， s_i 为节点 i 发出的间接信任信息请求消息的数量。

在实验过程中，为了方便分析，设定效用函数中的 $b_i = 30$ ， $p = 5$ ， $e = 0.5$ ，在现实情况中，这些值会随着具体的网络环境而改变，那么也可以设定相应的其他参数值来满足激励条件，使节点都趋向于选择合作策略。

5.1 激励一致性条件验证

1) 节点自私性对信任管理系统的影响

图 2 给出了一个由 50 个节点组成的自组网在不同惩罚力度下，经过 20 轮博弈后节点的间接信任信息获取率与自私节点比率间的关系，很显然，随着自私节点的增加，间接信任信息获取率响应下降，直至整个信任管理机制的间接信任评估机制失效。

2) 节点预期活跃时间 (参数 L) 对协作性的影响

在该实验中，测试了节点预期活动时间 (L) 对节点行为的影响。在各组实验中，假设网络中初始有 50% 的合作节点，图 3 给出了网络中的节点在不同参数设置下经过 30 轮博弈后的平均间接信任信息获取率。图例中的 N 代表网络中的节点数量。

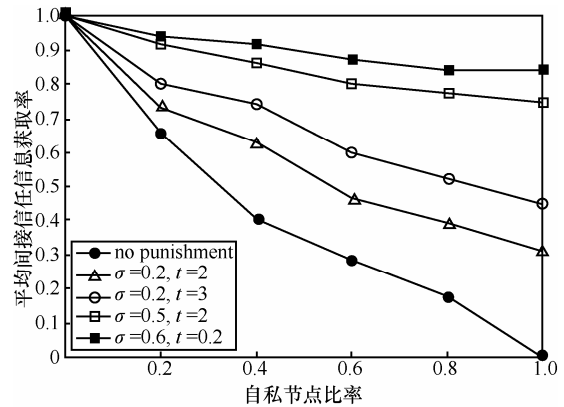


图 2 无惩罚机制时自私节点比率对间接信任信息获取率的影响

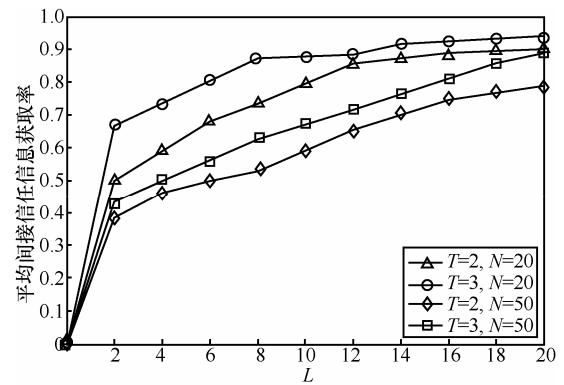


图 3 参数 L 对节点协作性的影响

可以看出，当其他参数一致时，网络中节点数量与节点平均间接信任信息获取率成反比，造成这一现象的原因是随着网络中节点数量的增加，每个节点在一个时隙内接收到的间接信任消息也会相应增多，而此时惩罚力度 (T) 并没有变化，因此对节点的震慑能力有所减弱，导致一部分节点选择非合作策略，使节点的间接信任信息获取率下降。此外，网络规模相同时，加大惩罚力度，间接信任信息获取率也随之升高，然而当 L 没有足够大时，惩罚措施的效果也有限，因为未来的利益对节点的吸引力不够强，节点更注重眼前利益，所以节点会选择非合作策略使当前利益最大化。因此，可以根据网络的具体情况设置合适的参数使得节点的合作率达到本文需求。

3) 惩罚力度 (参数 T) 对节点协作性的影响

在该实验中，验证并分析惩罚力度对节点协作性的影响，假设该网络由 50 个节点组成，在初始时刻有 50% 的节点选择合作策略，在取不同的 σ 值的情况下，经过 20 轮博弈后网络中节点的平均间接信任信息获取率与惩罚力度的关系如图 4 所示。从图 4 中可以看出在同一惩罚机制下，节点的预期

活跃时间越长（即 L 越大，相应 σ 也越大），经过一段时间后节点平均间接信任信息获取率越大，意味着合作节点越多。这一现象主要是因为 L 越大，未来的利益对节点越重要，因此节点迫于获取长期最大利益而不得不采取合作策略。同时可以看出当 σ 不变时，惩罚措施越严厉，节点的合作意向也越明显，这也与常识相符。

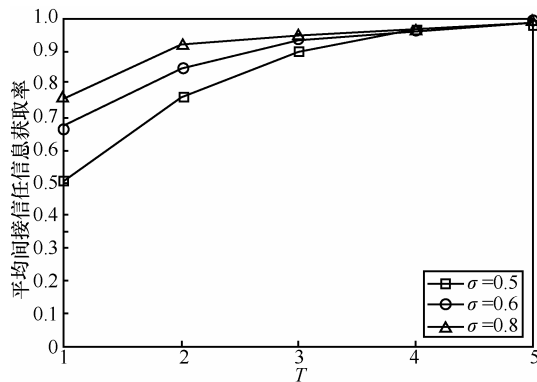


图 4 参数 T 对节点协作性的影响

4) 惩罚机制有效性验证

在该实验中，在不同的网络环境中验证提出的惩罚机制的有效性，由于目前没有应用博弈论针对间接信任信息获取过程提出的惩罚机制，因此图 5 对比了采用文中提出的惩罚机制与不采取任何惩罚机制的信任管理系统中节点间的协作性。假设网络中有 50 个节点，该实验假设网络比较稳定 ($L \rightarrow \infty$)，未来利益与眼前利益对于节点同样重要。从前文可知，如不采取惩罚机制，那么 T 等于 0。在经过 50 轮博弈后，如图 5 所示，总体来看，由于惩罚对节点的威慑，采取惩罚机制时比不采取时节点平均间接信任信息获取率更高。在其他条件相同时，网络中自私节点的比例越高，惩罚机制产

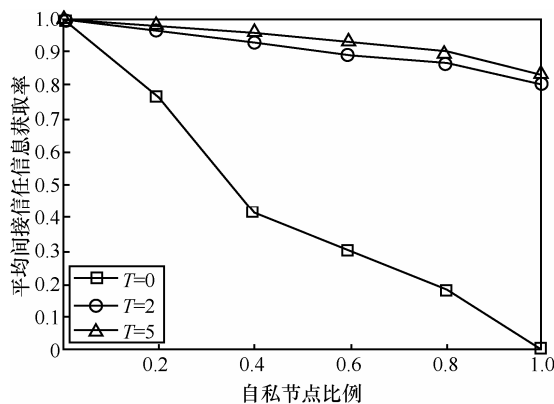


图 5 采取与不采取惩罚机制的信任管理系统中节点间的协作性比较

生的积极作用越突出，当自私节点比例为 80% 时，没有惩罚措施的信任管理机制只能获得约 20% 的间接信息，而惩罚力度为 $T=2$ 时的间接信息获取率可达 87%， $T=5$ 时的间接信息获取率更达到了 93%，那么后者必然使整个信任管理系统中的节点最终得到更准确的信任信息来选择最佳的交互对象。

5.2 演化稳定策略验证

使用不同参数值来验证演化稳定策略。取 3 组参数值来满足定理 1 到定理 3 的前提条件，它们分别是：

- 1) $L=1, \sigma=0.5, T=1$;
- 2) $L=4, \sigma=0.8, T=1$;
- 3) $L=0.25, \sigma=0.2, T=1$ 。

第 1 组参数值相应的进化曲线如图 6 所示，图例中的符号 θ_0 表示在初始时刻网络中合作节点的比例。可以从图 6 中看出无论式(11)的初始值是多少，随着网络的演化，合作与非合作节点的比率并没有发生显著变化，都是维持初始值的水平，即 θ 的值并没有改变。造成这一现象的原因就是由于节点选择合作与非合作所得利益都是相等的，因此没有足够的动力去改变目前的策略。因此整个网络中的节点的策略选择维持原有状态，这与定理 1 的结论一致。

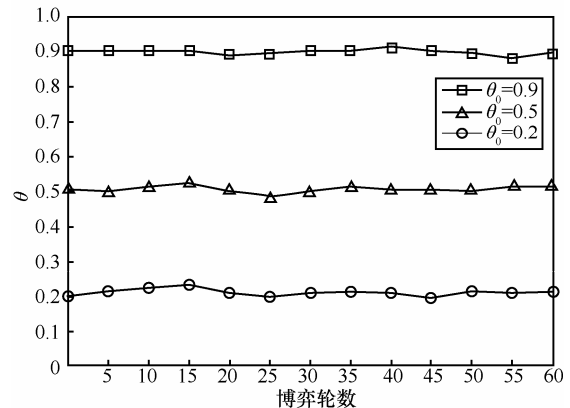


图 6 参数组 1 对应的进化趋势曲线

第 2 组数值相应的进化趋势曲线如图 7 所示。图中的参数值满足定理 2 的前提条件，从图 6 可以看出当式(11)的初始值是 0.80 时，意味着 80% 的节点的初始状态为选择合作策略，经过大约 30 轮的博弈之后，选择合作策略的节点的比率变为了 1 并保持稳定。当式(11)的初始值是 0.40 时，意味着 40% 的节点的初始状态为选择合作策略，经过大约 60 轮的博弈之后，选择合作策略的节点的比率变为 1 并保持稳定。这一结果表明了在初始时刻，无论选

择合作的节点的比率为多少，只要满足定理 2 的前提条件，经过一段时间的博弈，最终网络中所有节点的策略最终都将演化为合作策略。

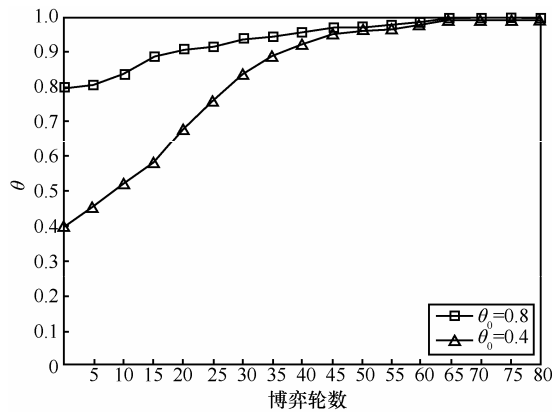


图 7 参数组 2 对应的进化趋势曲线

第 3 组数值相应的进化趋势曲线如图 8 所示。从图中可以看出无论初始时刻有多少节点选择了合作策略，经过一段时间的博弈，最终网络中所有节点都将趋于选择非合作策略，这是因为节点经过博弈后发现选择非合作策略可得到更多的利益，因此系统最终达到的稳定状态就是选择合作策略的节点比率为 0，这与定理 3 的结论相符。

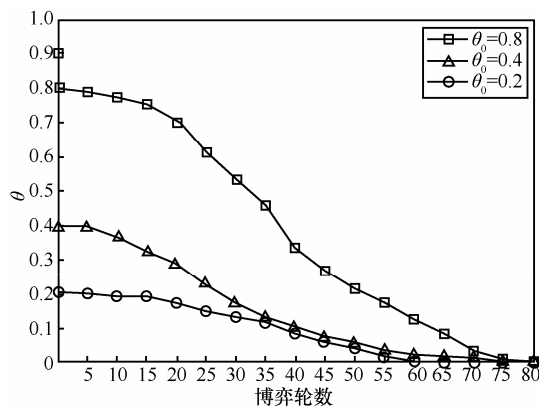


图 8 参数组 3 对应的进化趋势曲线

6 结束语

移动自组网中的信任管理机制可以帮助节点间建立信任并降低信息交互带来的风险。由于节点的自私性，导致节点不愿为其邻居节点提供间接信任信息，同时希望自己得到尽可能多的间接信任信息，长此以往，信任管理机制中的间接信任评估将失去意义。采用博弈论的思想为节点间的间接信任信息获取建立了博弈模型，提出了惩罚机制并给出了节

点的效用函数，此外，建立了信任演化的复制动态方程来研究在不同参数下节点的演化稳定策略。这些演化稳定策略表明了节点在间接信任评估过程中选择策略的演化过程。网络中的节点通过持续的调整自己的策略，最终使网络达到了一个稳定状态。实验结果验证了给出的方法的正确性及有效性，证明了该模型可使节点为了获得最大利益而在间接信任评估时选择同邻居合作，提高信任管理系统的可用性与有效性，与此同时，分析了各个参数对节点行为的影响，同时也通过对不同的参数进行实验，验证了节点的演化稳定策略，这些实验都为设计信任管理机制时选择合适的参数奠定了基础。

参考文献：

- [1] CHO J, SWAMI A, CHEN I. A survey on trust management for mobile ad hoc networks[J]. Commun Surveys & Tutorials, 2011, 13(4): 562-583.
- [2] YU H, SHEN Z, MIAO C. A survey of trust and reputation management systems in wireless communications[J]. Proc IEEE, 2010, 98(10): 1752-1754.
- [3] BUCHEGGER S, LE BOUDEEC J. Performance analysis of the confidant protocol[A]. Proc 3rd ACM Int Symp on Mobile Ad Hoc Networking & Computing[C]. 2002.
- [4] MICHIARDI P, MOLVA R. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks[A]. Proc 6th Int Conf Commun Multimedia Security[C]. 2002.
- [5] HE Q, WU D, KHOSLA P. SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks[A]. Proc IEEE Wireless Commun Syst Netw Conf[C]. 2004.
- [6] ALMENAREZ F, MARIN A, DIAZ D. Developing a model for trust management in pervasive devices[A]. Proc 4th Annu IEEE Int Conf Pervasive Comput Commun Workshops[C]. 2006.
- [7] BOUKERCH A, XU L, EL-KHATIB K. Trust-based security for wireless ad hoc and sensor networks [J]. Comput Commun, 2007, 30(1): 2413-2427.
- [8] MARSH S. Formalising Trust as a Computational Concept[D]. Scotland: University of Stirling, 1994.
- [9] CHO J H, SWAMI A, CHEN I R. Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks[J]. Journal of Network and Computer Applications, 2012, 35(3): 1001-1012.
- [10] ZAFAR S, SONI M K. Trust based QoS protocol (TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET[A]. Optimization, Reliability, and Information Technology (ICROIT), 2014 International Conference on IEEE[C]. 2014.173-177.
- [11] EISSA T, RAZAK S A, KHOKHAR R H, et al. Trust-based routing mechanism in MANET: design and implementation[J]. Mobile Networks and Applications, 2013, 18(5): 666-677.
- [12] OMAR M, CHALLAL Y, BOUABDALLAH A. Certification-based trust models in mobile ad hoc networks: a survey and taxonomy[J]. Journal of Network and Computer Applications, 2012, 35(1): 268-286.
- [13] GONZALEZ J M, MOHD A, JAMES B D J. Trust-based approaches to solve routing issues in ad-hoc wireless networks[A]. A Survey, 2011

International Joint Conference of IEEE TrustCom-11/IEEE ICES-11/FCST-11[C]. 2011.

- [14] WENZHONG Y, CUANHE H, BO W. A general trust model based on trust algebra[A]. Int Conf in Multimedia Inf Networking and Security[C]. 2009.125-129.
- [15] CHEN A, XU G, YANG Y. A cluster-based trust model for mobile ad hoc networks[A]. The 4th Int Conf on Wireless Communications, Networking and Mobile Computing[C]. 2008.
- [16] SEREDYNSKI M, BOUVRY P, KLOPOTEK M A. Modelling the evolution of cooperative behavior in ad hoc networks using a game based model[A]. IEEE Symp on Computational Intelligence and Games[C]. 2007.
- [17] ROGER B, MYERSON. Game Theory: Analysis of Conflict[M]. Harvard University Press, 1991.
- [18] 闻英友, 赵博, 赵宏. 基于博弈理论的移动自组网激励机制研究[J]. 通信学报, 2014,35(4):44-52.
WEN Y Y, ZHAO B, ZHAO H. Study on game-based incentive mechanism of mobile ad hoc network[J]. Journal on Communications, 2014, 35(4): 44-52.
- [19] YU W, LIU K J R. Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks[J]. IEEE Transactions on Mobile Computing, 2007,6(5):507-521.
- [20] SHEN Y, YAN Z, RAIMO K. Game theoretical analysis of the acceptance of global trust management for unwanted traffic control[A]. IEEE International Conference on High Performance Computing and Communications&2013 IEEE International Conference on Embedded and Ubiquitous Computing[C].2013.
- [21] SEREDYNSKI M, BOUVRY P. Analysing the development of cooperation in MANETs using evolutionary game theory[J]. The Journal of Supercomputing, 2013, 63(3): 854-870.
- [22] LI Z, SHEN H. Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks[J]. Mobile Computing, IEEE Transactions, 2012, 11(8):1287-1303.
- [23] WEIBULL J W. Evolutionary Game Theory[M]. Cambridge, MA: MIT Press, 1995.

作者简介:



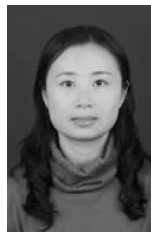
郭晶晶 (1988-), 女, 陕西榆林人, 西安电子科技大学博士生, 主要研究方向为网络安全、信任管理、隐私保护等。



马建峰 (1963-), 男, 陕西西安人, 西安电子科技大学教授、博士生导师, 主要研究方向为密码学、无线和移动安全、系统可生存性等。



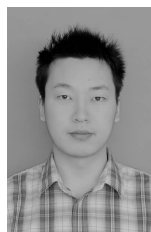
李琦 (1989-), 男, 江苏淮安人, 西安电子科技大学博士生, 主要研究方向为信息安全与基于属性的密码学。



万涛 (1975-), 女, 江西南昌人, 西安电子科技大学博士生, 主要研究方向为密码学、网络与信息安全。



高聪 (1985-), 男, 陕西榆林人, 西安电子科技大学博士生, 主要研究方向为网络与信息安全、服务计算以及面向服务的体系结构。



张亮 (1987-), 男, 陕西西安人, 西安电子科技大学博士生, 主要研究方向为计算机网络与安全技术、访问控制技术及应用。