

文章编号:1007-5321(2020)01-0074-06

DOI:10.13190/j.jbupt.2019-089

基于狄利克雷分布的可信路由转发机制

杜聪¹, 张喆², 李温静², 郭少勇¹, 孟洛明¹

(1. 北京邮电大学 网络与交换技术国家重点实验室, 北京 100876; 2. 国网信息通信产业集团有限公司, 北京 102211)

摘要: 机会移动社群网络易受到不良节点干扰而导致正常通信中断, 现有研究方法普遍存在忽略不良行为差异性, 为此, 提出了基于狄利克雷分布的可信路由转发机制. 利用消息传递过程判断节点的可信度, 提出应对干扰的路由转发机制. 实验结果表明, 在受到不良节点干扰的条件下, 该机制能够准确评估节点, 同时在保持低传输成本的情况下, 传输成功率比传统方法提高了 5% ~ 10%.

关键词: 狄利克雷分布; 机会移动社群网络; 可信路由

中图分类号: TP393

文献标志码: A

Trusted Routing and Forwarding Mechanism Based on Dirichlet Distribution

DU Cong¹, ZHANG Zhe², LI Wen-jing², GUO Shao-yong¹, MENG Luo-ming¹

(1. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;

2. State Grid Information and Telecommunication Group Company Limited, Beijing 102211, China)

Abstract: The opportunistic mobile social network is vulnerable to the interruption of normal communication due to the interference of bad nodes. Existing research methods generally have the problem of neglecting the difference of bad behavior. The article proposes a trusted routing and forwarding mechanism based on Dirichlet distribution. Firstly, the message passing process is used to judge the credibility of the node, and then the routing and forwarding mechanism for dealing with interference is proposed. Experiment shows that the mechanism can accurately evaluate nodes under the condition of poor node interference, and the transmission success rate is 5% ~ 10% higher than the traditional method while keeping the transmission cost low.

Key words: Dirichlet distribution; opportunistic mobile social network; trusted routing

随着网络边缘侧的高速发展,越来越多的边缘业务通过终端协同实现,如智慧校园、移动自组织网络^[1]等. 在机会移动社群网络中,存在终端受用户主观因素约束而引起不良行为的现象,破坏了机会移动社群网络的公平秩序,成为亟待解决的问题.

规避不良节点逐渐引起学者的关注^[2],一般采用直接与间接的方式进行评估. 其中,Chen 等^[3]提

出了以密钥配对来确认节点身份,以待评估节点历史数据确认节点行为;Yao 等^[4]提出了名为基于社交相似性的可信路由方法 (TRSS, the trust routing scheme based on social similarity),利用社交相似性加快身份认证,通过交互评估结果完成间接评估. 但是,上述方法均存在忽略不良行为差异性的问题,导致评估可能出现错误. 基于狄利克雷分布的评估

收稿日期: 2019-05-25

基金项目: 国家自然科学基金项目(61702048); 国家电网有限公司总部科技项目“电力无线专网演进及 4G、5G 技术应用分析”(5700-201941235A-0-0-00)

作者简介: 杜聪(1994—),男,硕士生, E-mail: ducong@bupt.edu.cn; 孟洛明(1955—),男,教授,博士生导师.

方法由 Josang 等^[5]在社交网络中首次提出. 随后, Li 等^[6]类比应用到移动自组网中, 但并未对数据获取进行更深入地研究. Denko 等^[7]提出了记录服务情况, 但未完全解决忽略不良行为差异性的问题.

笔者针对终端破坏机会移动社群网络公平秩序的问题, 提出了基于狄利克雷分布的可信路由转发机制 (TRFDD, trusted routing and forwarding mechanism based on Dirichlet distribution), 其中包含关注不良行为差异性的直接与间接可信评估流程以及基于评估结果的路由转发算法, 最后通过仿真对算法效果进行比对验证.

1 数学模型

1.1 问题描述

在机会移动社群网络中, 内容资源共享通过节点间机会接触实现, 如图 1 所示. 不良节点的存在制约着机会移动社群网络正常秩序的建立. 由于自私节点拒绝服务, 易造成网络资源分配不公平. 恶意节点丢弃数据包, 诋毁其他节点导致通信质量下降, 同时加大了网络负载, 降低了通信效率. 为避免自私与恶意行为, 需采取评估方法进行应对.

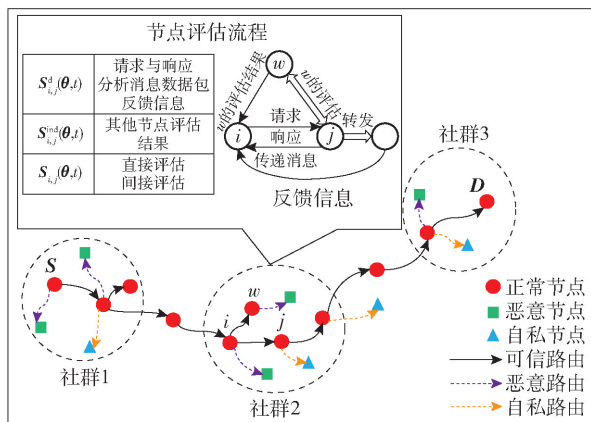


图 1 机会移动社群网络路由选择示意图

以图 1 中 3 个社群为例, 源节点 S 处于社群 1 中, 通过评估选择正常节点实现消息转发, 最终传递到社群 3 中的目标 D . 如何设计可信节点评估方法和相应的路由转发算法成为研究的核心内容.

本研究旨在利用消息传递过程中获取的信息评估节点的可信程度. 为此, 定义每个节点通过分析请求与响应、消息数据包与反馈信息得到的节点 i 对节点 j 的直接评估结果向量为 $S_{i,j}^d(\theta, t)$, 通过获取邻居节点 w 的评估结果计算处理得到的间接评估结果向量, 记为 $S_{i,j}^{\text{ind}}(\theta, t)$, 二者相加得到描述节点

最终可信程度的向量 $S_{i,j}(\theta, t)$, 选择 $\arg \max S_{i,j}(\theta, t)$ 为正常的节点作为转发的候选节点. 对于自私节点, 将其记录于观察名单中, 并以 flag 位标记社交型自私节点. 对于恶意节点, 将其记录于黑名单中, 根据评估结果以时间窗的方式定期更新 2 个名单.

1.2 问题模型

节点 i 为选取可信节点, 需要通过对候选节点 j 的直接评价 $S_{i,j}^d(\theta, t)$ 与其他节点 w 对 j 节点的间接评价 $S_{i,j}^{\text{ind}}(\theta, t)$ 综合计算最终评价 $S_{i,j}(\theta, t)$. 其中, t 为当前所处时间窗; 向量 $\theta = [\theta_1, \theta_2, \theta_3]$ 为节点的可信程度, 并将其划分为正常、自私和恶意 3 类, 分别用 θ_1 、 θ_2 和 θ_3 表示. 通过基于狄利克雷的概率分布模型计算, 最终评估结果表示为

$$S_{i,j}(\theta, t) = S_{i,j}^d(\theta, t) + S_{i,j}^{\text{ind}}(\theta, t) \quad (1)$$

狄利克雷概率密度函数如下:

$$f(p_j(\theta, t) | \alpha_{i,j}(\theta, t)) = \frac{\Gamma\left(\sum_{k=1}^3 \alpha_{i,j}(\theta_k, t)\right)}{\prod_{k=1}^3 \Gamma(\alpha_{i,j}(\theta_k, t))} \prod_{k=1}^3 p_j(\theta_k, t)^{\alpha_{i,j}(\theta_k, t) - 1}$$

$$\text{s. t. } \begin{cases} p_j(\theta_1, t), p_j(\theta_2, t), p_j(\theta_3, t) \geq 0 \\ \sum_{k=1}^3 p_j(\theta_k, t) = 1 \\ \alpha_{i,j}(\theta_1, t), \alpha_{i,j}(\theta_2, t), \alpha_{i,j}(\theta_3, t) > 0 \end{cases} \quad (2)$$

直接评估利用通信过程获取的数据, 计算狄利克雷概率期望:

$$S_{i,j}^d(\theta_k, t) = E(p_j(\theta_k, t) | \alpha_{i,j}(\theta, t)) = \frac{\alpha_{i,j}(\theta_k, t)}{\sum_{k=1}^3 \alpha_{i,j}(\theta_k, t)}, \quad k=1, 2, 3 \quad (3)$$

其中: 向量 $p_j(\theta, t) = [p_j(\theta_1, t), p_j(\theta_2, t), p_j(\theta_3, t)]$ 为节点 j 在当前时间窗内 3 种可信程度的概率; $\alpha_{i,j}(\theta, t) = [\alpha_{i,j}(\theta_1, t), \alpha_{i,j}(\theta_2, t), \alpha_{i,j}(\theta_3, t)]$ 为节点 i 在当前时间窗内观测到的节点 j 出现 3 种类别行为的次数, $\alpha_{i,j}(\theta_k, t)$ 表示为

$$\alpha_{i,j}(\theta_k, t) = \varphi_{i,j}(\theta_k, t) + \sum_{m=1}^3 v_m \varepsilon_j^{v_m}(\theta_k, t), \quad k=1, 2, 3 \quad (4)$$

其中: $\varphi_{i,j}(\theta, t) = [\varphi_{i,j}(\theta_1, t), \varphi_{i,j}(\theta_2, t), \varphi_{i,j}(\theta_3, t)]$ 为描述当前时间窗初始时刻待评估节点可信程度的基础概率, 满足 $\sum_{k=1}^3 \varphi_{i,j}(\theta_k, t) = 1$.

在 $t=0$ 时, 不同社交关系的节点具有不同的初

始基础概率:

$$\varphi_{i,j}(\boldsymbol{\theta}, 0) = \begin{cases} \left(\frac{2}{3}, \frac{1}{6}, \frac{1}{6}\right), & \text{rel}(i, j) = \text{Friends} \\ \left(\frac{1}{2}, \frac{1}{4}, \frac{1}{4}\right), & \text{rel}(i, j) = \text{Strangers} \\ \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right), & \text{rel}(i, j) = \text{Others} \end{cases} \quad (5)$$

其中 $\text{rel}(i, j) = \begin{cases} \text{Friends, Match}(i, j) \geq \text{th} \\ \text{Strangers, Match}(i, j) < \text{th} \\ \text{Others, indirect contact} \end{cases}$ 用于衡量

节点间的社交关系。借鉴社交接触网络的思想,具有更高社交相似性的节点会发生更频繁的接触,更有可能成为可信节点,将不同社交关系的节点进行信任等级的划分:

$$\text{Match}(i, j) = \frac{|\mathbf{F}_i \cap \mathbf{F}_j|}{N} \quad (6)$$

其中:向量 $\mathbf{F} = [f_1, f_2, \dots, f_N]$ 为节点的 N 个社会属性,用于计算节点间的社交相似性,为相同属性数量与所有属性数量的比值。满足阈值条件 th 的节点记为 Friends,不满足阈值条件的节点记为 Strangers。对于间接接触到的节点记为 Others。

基础概率随时间的更新如下,上一时间窗评估结果作为新时间窗的基础概率。

$$\varphi_{i,j}(\boldsymbol{\theta}, t + \tau) = \mathbf{S}_{i,j}^d(\boldsymbol{\theta}, t) \quad (7)$$

根据行为对评估的影响程度将对应行为的增长速率划分为半速、基本速率和二倍速,用向量 $\mathbf{v}_m = (v_1, v_2, v_3)$ 表示, m 代表速率等级; $\varepsilon_j^m(\theta_k, t)$ 表示节点 j 在当前时间窗内的可信程度为 θ_k 、增长速率为 \mathbf{v}_m 的行为出现频数。直接评估的结果为

$$\mathbf{S}_{i,j}^d(\theta_k, t) = E(p_j(\theta_k, t) | \boldsymbol{\alpha}_{i,j}(\boldsymbol{\theta}, t)) = \frac{\varphi_{i,j}(\theta_k, t) + \sum_{m=1}^3 \mathbf{v}_m \varepsilon_j^m(\theta_k, t)}{1 + \sum_{k=1}^3 \sum_{m=1}^3 \mathbf{v}_m \varepsilon_j^m(\theta_k, t)}, k = 1, 2, 3 \quad (8)$$

间接评估利用其他节点 w 的直接评估信息,即

$$\mathbf{S}_{i,j}^{\text{ind}}(\boldsymbol{\theta}, t) = \sum_{w=1}^W \omega(\mathbf{S}_{i,j}^d(\boldsymbol{\theta}, t), \mathbf{S}_{w,j}^d(\boldsymbol{\theta}, t)) \gamma(i, w) \mathbf{S}_{w,j}^d(\boldsymbol{\theta}, t) \quad (9)$$

其中: w 代表与节点 i, j 均接触过的第三方节点, W 为该类型节点的个数; $\omega(\mathbf{S}_{i,j}^d(\boldsymbol{\theta}, t), \mathbf{S}_{w,j}^d(\boldsymbol{\theta}, t))$ 为直接评估结果的相似性,若低于阈值,则忽略,并以基本速率记录该节点恶意行为。相似性采用复杂度较低

的 Tanimoto 方法计算:

$$\omega(\mathbf{S}_{i,j}^d(\boldsymbol{\theta}, t), \mathbf{S}_{w,j}^d(\boldsymbol{\theta}, t)) = A \frac{\mathbf{S}_{i,j}^d(\boldsymbol{\theta}, t) \mathbf{S}_{w,j}^d(\boldsymbol{\theta}, t)}{\mathbf{S}_{i,j}^d(\boldsymbol{\theta}, t) \mathbf{S}_{i,j}^d(\boldsymbol{\theta}, t) + \mathbf{S}_{w,j}^d(\boldsymbol{\theta}, t) \mathbf{S}_{w,j}^d(\boldsymbol{\theta}, t) - \mathbf{S}_{i,j}^d(\boldsymbol{\theta}, t) \mathbf{S}_{w,j}^d(\boldsymbol{\theta}, t)} \quad (10)$$

其中 A 为评价结果相似性的最高采纳权重。

$$\gamma(i, w) = \begin{cases} \frac{2}{3}, & \text{rel}(i, w) = \text{Friends} \\ \frac{1}{3}, & \text{rel}(i, w) = \text{Strangers} \end{cases} \quad (11)$$

式(11)表示对于不同社交关系的节点 w , 节点 i 将采取不同信任权重。

选取最高概率的可信程度,节点 i 得到对于节点 j 的最终评估结果为

$$E_{i,j} = \arg \max_{\theta_k} \mathbf{S}_{i,j}(\boldsymbol{\theta}, t) \quad (12)$$

2 基于狄利克雷分布的可信路由算法

如图 2 所示,算法流程包括节点的可信评估和路由转发策略 2 部分。

2.1 节点评估流程

2.1.1 直接评估流程

1) 请求与响应

请求方检查响应数据包的响应标记位 (ACK, acknowledge), 如果为 1, 表示同意接收。继续检查序号标记位 (SEQ, sequence), 若该值与之前发送值相差 1, 表示响应方表现正常, 以基本速率记录正常行为; 如果 SEQ 没有变化, 以二倍速记录恶意行为。若 ACK 位为 0, 表示响应方拒绝服务, 以二倍速记录自私行为。超过请求数据包生存时间后, 仍未收到响应数据包, 以基本速率记录响应方自私行为。如果请求节点在观察名单中, 但不是起始节点, 则认定其为社交型自私节点, 令其 $\text{flag} = 1$ 。

2) 消息数据包

从消息数据包中获取路由记录, 奖励所有参与中继的节点, 以半速记录正常行为。若出现观察名单中的节点, 则判定其为社交型自私节点, 令其 $\text{flag} = 1$ 。

3) 反馈确认

根据反馈信息的节点是否为目标节点, 将反馈确认过程分为以下 2 种情况。

① 2 跳反馈。非目标节点将接收的消息的哈希值 MSG_{10} 发送给 2 跳前的节点。

如果 MSG_{10} 存储于接收反馈消息的节点中, 则对

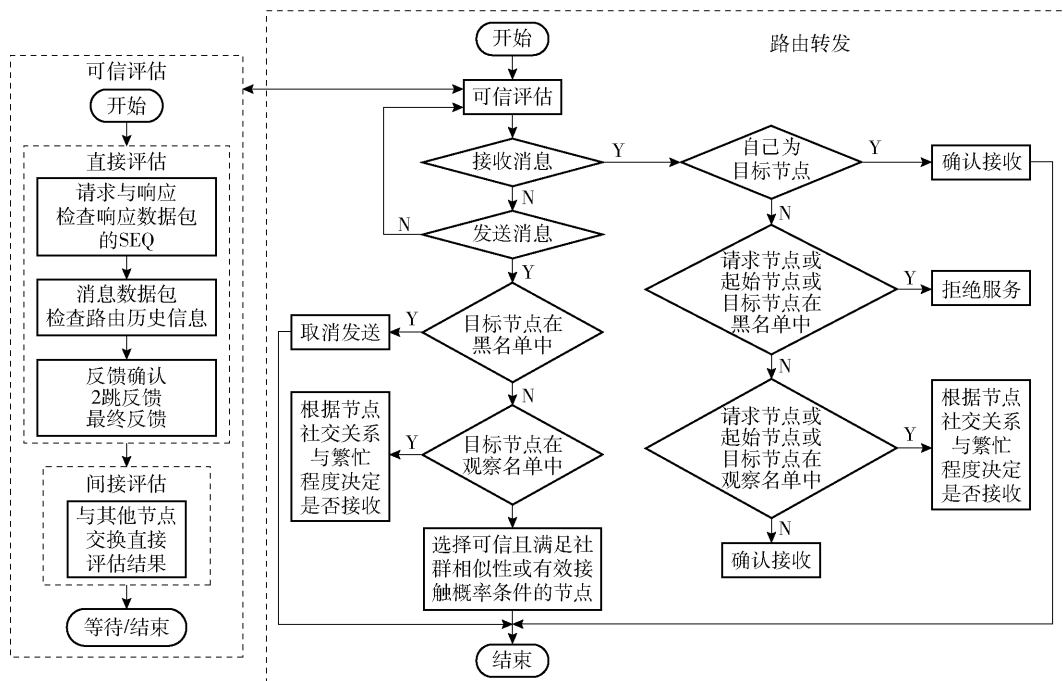


图2 算法流程示意图

反馈信息中包含的中继节点以二倍速记录正常行为。

对于反馈信息的来源,如果来自黑名单中的节点,说明该节点在接收到消息数据包后并未直接丢弃,以基本速率记录正常行为;如果来自观察名单中的节点,说明其为社交型自私节点,令其 $\text{flag} = 1$ 。

如果不存在对应 MSG_{id} ,则直接丢弃该反馈数据包。

② 最终反馈。目标节点将反馈发送给路径中出现的的所有节点。

确认 MSG_{id} 存在本地后,对路径中的其他节点以二倍速记录一次正常行为;否则,忽略该反馈信息。

直接评估结果如式(8)所示。

2.1.2 间接评估流程

节点间定期交换自身的直接评估结果,作为建议信息。间接评估结果如式(9)所示。

间接评估对于直接评估的补充:当由式(10)计算的相似性不满足阈值时,以基本速率记录来源节点的恶意行为;当接收到观察名单中节点的评估结果时,表明该节点参与到了网络通信过程中,以二倍速记录正常行为。

根据式(1)和式(12),获得节点的可信程度。

2.2 路由转发流程

路由转发包括面对请求时如何响应以及发送消息时如何选择中继2种情况。设定可信程度较高节

点的消息数据具有更高的处理优先级。

情况1 面对中继请求的响应

第1步 如果自己为目标节点,一律接收;否则,跳转到第2步。

第2步 如果请求节点、起始节点或目标节点为恶意节点(在黑名单中),则直接反馈表示该次请求不合格,并拒绝服务;否则,跳转到第3步。

第3步 如果请求节点、起始节点或目标节点为自私节点(在观察名单中),若 $\text{flag} = 1$,则跳转到第4步。根据资源空闲情况与设定阈值(朋友关系时,采取较低阈值)的比较结果,利用响应数据包回复同意或拒绝服务;否则,跳转到第4步。

第4步 确认接收。

情况2 选择中继节点向目标节点发送数据包

第1步 如果目标节点为恶意节点(在黑名单中),则取消发送计划;否则,跳转到第2步。

第2步 如果目标节点为自私节点(在观察名单中),若 $\text{flag} = 1$,则跳转到第3步。根据资源空闲情况与设定阈值(朋友关系时,采取较低阈值)的比较结果来判定是否执行发送计划;否则,跳转到第3步。

第3步 在经过狄利克雷评估获得的可信节点基础上,选择满足社群相似性或有效接触概率的节点作为中继节点。

① 社群相似性。描述中继节点与目标节点同属一个社群的可能性。令 tar 代表目标节点, c 代表

候选节点,则社群相似性表示为

$$\text{Sim}(\mathbf{R}_c, \mathbf{F}_{\text{tar}}) = 1 - \sqrt{\frac{\sum_{n=1}^N (\mathbf{R}_c(f_{\text{tar}}^n) - 1)^2}{N}} \quad (13)$$

其中: \mathbf{R}_c 以表格的形式将候选节点 c 存储在本地社群中的所有属性及其记录值中, \mathbf{F}_{tar} 为目标节点 tar 的社会属性。

$\mathbf{R}_c(f_{\text{tar}}^n) = \frac{\text{nums}(f_{\text{tar}}^n)}{\text{sum}(\mathbf{R}_c)}$ 表示在该社群中目标节点 tar 的第 n 个社会属性值 f_n 出现次数的比例。

② 有效接触概率. 描述两节点间传递数据包的历史概率,近似为指数分布,通过分析路由信息可得到. 发生直接传递的事件次数为 1,而间接传递的事件次数随路由距离的增大而衰减. 当前时间窗 τ 内发生有效接触事件 X 的概率为

$$q_{c,\text{tar}}(X \leq \tau) = 1 - q_{c,\text{tar}}(X > \tau) = 1 - e^{-\lambda_{c,\text{tar}}(t)\tau} \quad (14)$$

其中 $\lambda_{c,\text{tar}}(t)$ 为当前单位时间内有效接触事件 X 的平均次数,则

$$\lambda_{c,\text{tar}}(t + \tau) = \beta \lambda_{c,\text{tar}}(t) + (1 - \beta) \sum_{r=1}^{P(t,t+\tau)} e^{-\mu(d_r(c,\text{tar}) - 1)} \quad (15)$$

其中: μ 为受路由距离影响的衰减因子, $d_r(c, \text{tar})$ 为节点 c 与 tar 之间的路由距离, $P(t, t + \tau)$ 为新时间窗内接收的消息数据包数, $\sum_{r=1}^{P(t,t+\tau)} e^{-\mu(d_r(c,\text{tar}) - 1)}$ 为新时间窗内获得的有效接触信息, β 为历史因素的权重。

在可信的基础上,节点选择需要进一步满足下列条件:

$$\text{Sim}(\mathbf{R}_c, \mathbf{F}_{\text{tar}}) > \text{Sim}(\mathbf{R}_{\text{cur}}, \mathbf{F}_{\text{tar}}) \cup q_{c,\text{tar}}(X \leq \tau) > q_{\text{cur},\text{tar}}(X \leq \tau) \quad (16)$$

其中 cur 代表当前节点. 式(16)表示候选节点需要满足社交相似性大于当前节点或者有效接触概率大于当前节点。

3 仿真实现

3.1 仿真环境

仿真环境选择机会网络环境仿真器,从 Info-com06 的真实数据筛选出 78 位用户 4 d 的接触信息,采用国籍、国家、城市、语言、公司和职位信息描述节点. 参数如下: 20 次, 300 000 s, 传输速率为

54 Mbit/s, 传输范围为 30 m, 存储空间为 100 MB, 数据生存时间为 12 h, 用户为 78 个, 不良节点变化比例为 0 ~ 80%.

3.2 结果分析

将所提出的 TRFDD 与 Epidemic^[8]、Prophet^[9]、TRSS^[4] 进行对比, 并采用传输成功率、传输成本、传输时延和丢包数量 4 个评价指标。

3.2.1 传输成功率

传输成功率是指成功传输的次数与所有发送事件数的比值. 如图 3 所示, 所有算法的传输成功率均随着不良节点的增多而下降, 但 TRFDD 始终保持较高的成功率, 很快超过 Epidemic 和 Prophet. 当不良节点比例达到 80% 时, TRFDD 的传输成功率比 TRSS 高出 5%, 比 Epidemic 高出 9%, 比 Prophet 高出 11%.

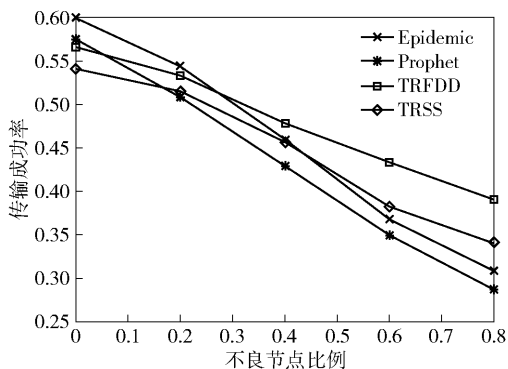


图 3 传输成功率对比

3.2.2 传输成本

传输成本是指为实现单个消息数据包成功接收所需复制转发的次数, 采用对数表示. 如图 4 所示, Epidemic 和 Prophet 的传输成本急速升高, 随后保持稳定; TRFDD 和 TRSS 的传输成本始终处于较低的水平. TRFDD 的传输成本虽然略高于 TRSS, 但传输成功率高出 5%, 效率较高。

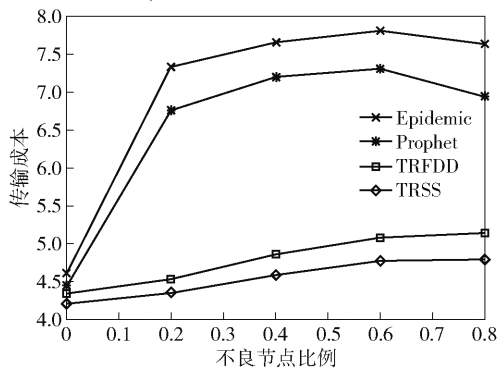


图 4 传输成本对比

3.2.3 传输时延

传输时延是指消息数据包成功接收与生成时刻的时间差. 如图 5 所示, Epidemic 和 Prophet 算法的传输时延增长速率逐渐加快, 在 80% 不良节点比例下达到 5.5 h, 接近数据生存时间; 而 TRFDD 和 TRSS 的传输时延相近始终保持在 4 h 内.

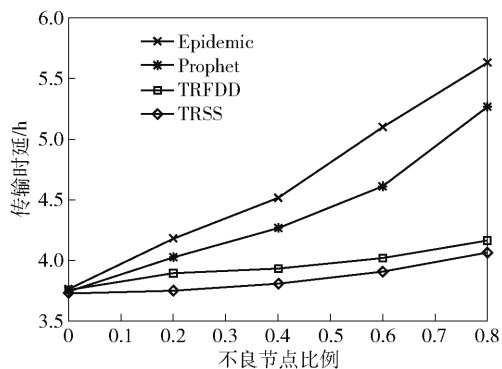


图 5 传输时延对比

3.2.4 丢包数量

丢包数量描述在传输过程中因生存时间超时、不良节点丢弃等原因所造成的数据包丢失, 用以衡量网络资源的浪费情况, 采用对数表示. 如图 6 所示, Epidemic 和 Prophet 的丢包数量提高了 2~3 个数量级, 而 TRFDD 和 TRSS 的丢包数量相近, 且仅在小范围内增长.

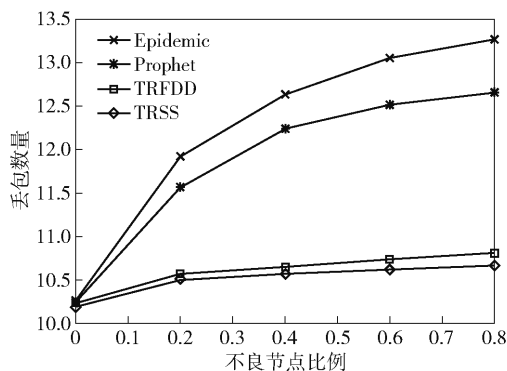


图 6 丢包数量对比

4 结束语

为解决机会移动社群网络中由于节点的不良行为所导致的内容资源共享效率和质量下降的问题, 提出了 TRFDD 以维护网络的正常通信过程. 首先利用消息传递过程中获取的信息从多个维度判断节

点的可信程度, 进而提出了正常节点对不良节点的应对算法, 采取了尽量与自私节点合作, 拒绝与恶意节点合作的策略. 与目前主流的相关算法进行对比实验, 结果显示所提出的算法能够有效地避免不良节点的干扰, 具有较强的鲁棒性. 通过准确评估节点的可信程度、充分挖掘社交型自私节点能力等方式, 高效地维持了较高的传输成功率, 实现了数据包快速转发, 有效地避免了不良行为所引起的网络失衡现象.

参考文献:

- [1] 程伟明. 无线移动自组网及其关键技术[J]. 数据通信, 2002(3): 56-58.
Cheng Weiming. Wireless mobile Ad hoc network and its key technologies[J]. Data Communication, 2002(3): 56-58.
- [2] Mukherjee P, Sen S. Comparing reputation schemes for detecting malicious nodes in sensor networks[J]. The Computer Journal, 2011, 54(3): 482-489.
- [3] Chen Xi, Sun Liang, Ma Jianfeng, et al. A trust management scheme based on behavior feedback for opportunistic networks[J]. Network Technology and Application, 2015, 12(4): 117-129.
- [4] Yao Lin, Man Yanmao, Huang Zhong, et al. Secure routing based on social similarity in opportunistic networks[J]. IEEE Transactions on Wireless Communications, 2015, 15(1): 594-605.
- [5] Josang A, Haller J. Dirichlet reputation systems[C]// International Conference on Availability, Reliability and Security. Vienna: IEEE Press, 2007: 112-119.
- [6] Li Yang, Kizza J M, Alma-Cemerlic, et al. Fine-grained reputation-based routing in wireless Ad hoc networks[C]// Intelligence and Security Informatics. New Brunswick: IEEE Press, 2007: 75-78.
- [7] Denko M K, Sun Tao, Woungang I. Trust management in ubiquitous computing: a Bayesian approach[J]. Computer Communications, 2011, 34(3): 398-406.
- [8] Vahdat A, Becker D. Epidemic routing for partially-connected Ad hoc networks[J]. Master Thesis, 2000, 20(4): 106-119.
- [9] Zhou Hongbo, Ni L M, Mutka M W. Prophet address allocation for large scale MANETs[J]. Ad Hoc Networks, 2003, 1(4): 423-434.