doi:10.11959/j.issn.1000-436x.2016047

可靠的机会网络自私节点检测算法

任智，谭永银，李季碧，陈前斌
（重庆邮电大学移动通信技术重庆市重点实验室，重庆 400065）

摘 要：针对现有机会网络自私节点检测算法没有考虑节点收到错帧和节点脱离通信范围监听失败的情况而影响检测准确性的问题，提出一种可靠的自私节点检测新算法——RSND。采用基于跨层监听机制的错帧解析、基于节点相遇的信息挖掘和基于 RSSI 的节点距离估计 3 种新机制消除错帧和节点脱离通信范围监听失败对节点自私性检测的影响，提升检测可靠性。理论分析证明了 RSND 算法的有效性，仿真结果显示，相对于现有的基于 2-ACK 的自私节点检测算法和 Watchdog 检测算法，新算法的自私节点检测准确率和网络吞吐量至少提高了 6%和 4%。

关键词：机会网络；自私节点；检测算法；监听；误判
中图分类号：TP393.04 **文献标识码：**A

Reliable selfish node detection algorithm for opportunistic networks

REN Zhi, TAN Yong-yin, LI Ji-bi, CHEN Qian-bin
(Chongqing Key Laboratory of Mobile Communication Technolo y, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: To address the problem of detection accuracy affected by situations like the omission of node receiving wrong frame and failure of monitoring beyond nodes' communication range during the consideration of the ex ing selfish node detection algorithms in opportunistic networks, a novel and reliable selfish node detection algorithm——RSND algorithm for opportunistic networks was proposed. It employs wrong frame analysis based on cross-layer monitoring mechanism, information excavation based on node encounter and node distance estimation based on RSSI three new mechanisms to eliminate the influence of node's selfishness detection due to wrong frame and failure of monitoring beyond nodes' communication range, improving the reliability of detection. Theoretical analysis verifies the effectiveness of RSND, and simulation results show that RSND can improve selfish node detection accuracy ratio and network throughput at least 6% and 4%, as compared to the existing selfish node detection algorithm based on 2-ACK and watchdog detection algorithm.

Key words: opportunistic networks, selfish node, detection algorithm, monitor, misjudgment

1 引言

机会网络[1,2]是一种不需要源节点和目的节点之间存在完整链路，利用节点移动带来的相遇机会实现通信的时延和分裂可容忍的无线自组织网络。目前，机会网络路由协议均假设网络中的节点具有良好的协作性。然而，由于机会网络中节点的资源（包括能量和缓存等）有限，为了节约资源，节点会拒绝帮助其他节点转发消息。这种自私行为使现有的路由机制无法正常工作，从而导致网络性能退化[3,4]。机会网络中不为系统作贡献，只享受信息资源服务的节点称为自私节点。自私节点并不想要损害其他节点，从而造成信息传递的失败，主要是在使用网络资源的同时，拒绝消耗自身有限的能量为其他节点提供信息转发服务，即不协作参与网络中的信息转发服务[5]。自私节点的存在会严重影响网

收稿日期：2015-06-19；修回日期：2015-11-16
通信作者：谭永银，tyy0805@126.com
基金项目：国家自然科学基金资助项目（No.61379159）；长江学者和创新团队发展计划基金资助项目（No.IRT1299）；重庆市自然科学基金资助项目（No.cstc2012jjA40051）；重庆市教委基金资助项目（No.Kizh11206）
Foundation Items: The National Natural Science Foundation of China (No.61379159), The Program for Changjiang Schnolars and Innovative Research Team in University (No.IRT1299), The Natural Science Foundation of Chongqing (No.cstc2012jjA40051), The Special Fund of Chongqing Municipal Education Commission (No.Kizh11206)

络性能以及网络服务的可靠性，甚至会破坏网络的正常运行。因此如何设计有效的自私节点检测算法，促使数据能够成功转发到目的节点成为当前机会网络中亟待解决的问题。

目前，可用于机会网络的自私节点检测算法主要有 IRONMAN[6]、CORE [7]、CONFIDANT [8]、Watchdog[9]和 2-ACK[10]等。IRONMAN 是一种基于喷雾式路由的自私节点自主检测机制，节点通过相遇并交换历史记录来判断中间节点的自私性。由于机会网络中节点是自由移动的，任意 2 个节点相遇周期具有不确定性，这就使 IRONMAN 检测算法对自私节点的检测难以满足实时性要求。CORE 算法通过信誉值来判断节点的自私性，信誉值包括主观信誉值、间接信誉值和功能信誉值，最后的信誉评价是这 3 者的综合。其中，间接信誉值来自社区中的其他节点，由于机会网络中的节点移动性较强，邻居节点不固定，社区划分不明显，因此 CORE 机制的准确性得不到保证。CONFIDANT 机制也是根据信誉来判断节点的自私性，但信誉值维护、传播及节点信任机制复杂且不可靠，容易导致信誉不一致的问题。Watchdog 检测算法的主要思想是利用广播信道的特征，侦听下一跳节点是否转发了该消息。若在规定的时间内下一跳节点无更改地转发了此消息，则说明下一跳节点行为良好；反之则说明下一跳节点出现了不合作行为。该算法在普通移动自组织网络中效果良好，但在机会网络中，由于节点随机移动，节点可能脱离通信范围，数据分组之间可能发生碰撞，造成检测不准确；当节点没监听到数据分组时，认为节点没参与转发，判断过于严格。基于 2-ACK 的自私节点检测算法的主要思想是当一个节点成功转发数据分组后，其下一跳节点会向其上一跳节点发送一个 2 跳应答数据分组，指示成功接收到数据。相对于 Watchdog 检测算法，基于 2-ACK 的自私节点检测算法在部分情况下能够提高自私节点检测的准确率，但它要求存在 2 跳的路径，而且引入了大量 2-ACK 应答分组，增加了控制开销，容易引起网络拥塞，进而影响网络性能以及检测准确性。

综上所述，在机会网络中应用 Watchdog 算法是一种较为可行的选择，但本文在研究中发现当机会网络节点收到错帧和节点脱离通信范围监听失败时，Watchdog 算法因未考虑应对之策而会出现误判，影响检测准确性。为解决此问题，提出了一种可靠的机会网络自私节点检测算法。

2 假设与问题描述

2.1 假设

为准确界定问题，做出如下假设。网络节点分为自私和不自私 2 种类型。自私节点只发送自己的数据分组，不为其他节点转发数据分组。节点都是使用全向天线，通信范围相等[11,12]，无线链路为双向链路。

2.2 问题描述

由于机会网络中存在无线信道质量、干扰以及信号碰撞等不稳定因素，造成帧的长度、内容等发生变化，节点收到的帧未能通过校验，也就是所谓的“收到错帧”，容易造成误判，从而导致检测不准确。

由于节点的随机移动，携带数据分组的中间节点在移动的过程中可能脱离节点的通信范围，造成节点难以监听中间节点是否转发了数据分组，导致检测困难。

前面提到的检测算法中均没有考虑到上述问题，会造成部分行为良好（转发了数据帧）的节点因为监听节点没有侦听到其转发操作而被误判为自私节点，导致它们受到不必要的惩罚（数据分组不能被转发），从而降低网络吞吐量。

3 RSND 算法

为解决上述问题，本文提出一种更可靠的自私节点检测算法——RSND（reliable selfish node detection），它可在机会网络相关路由协议中灵活使用。

3.1 RSND 算法包含的新机制

RSND 算法包含 3 种新机制，具体如下。

3.1.1 错帧解析

当前节点在监听中间节点的行为时，收到未通过校验的帧后，不直接丢弃此帧，而是通过跨层提取帧中数据分组的头部与中间节点保存的已发数据分组的头部进行比对，若二者相同，则说明中间节点转发了该数据分组；若二者不同，则提取一定长度（缺省值建议为 64 bit）的数据分组尾部信息和缓存分组进行比对；如果相同，说明中间节点进行了数据分组转发，不是自私节点；若不同，则将中间节点归入难以确定的类型。

3.1.2 基于节点相遇的信息挖掘

当 2 个相遇节点交换数据分组时，收到数据分组后的节点提取分组头部信息，判断分组的源节点是否为对方节点；如果不是，说明对方节点在为其他节点转发数据分组，因此判定其不是自私节点；

否则，对方节点便存在自私嫌疑，节点根据网络中自私节点的比例，估计对方节点的自私性。

在节点存储空间允许的情况下，节点建立一张与 SV（summary vector）对应的表，存储每个数据分组的下一跳节点地址以及该数据分组的目的节点地址。数据分组的源节点如果发现相遇节点是目的节点且已收到该数据分组，则判定该数据分组的下一跳节点进行了转发，不是自私节点。

3.1.3　脱离判断

节点采用跨层协作的方式判断邻居节点是否脱离通信范围，具体思路为：节点通过在 MAC 层多次接收来自邻居节点的帧（ACK 帧、Hello 帧等）并记录收帧时间，采用 RSSI[13]机制测收帧时节点间的间距，由记录的时间和测得的间距计算节点运动的平均速度并确定运动方向，判断邻居节点是否已脱离通信范围。如果在 MAC 层判断邻居节点已脱离通信范围，则通过“跨层信息共享”的方式将该信息报告给网络层；网络层在未监听到邻居节点发送数据分组的情况下不将其判定为自私节点。

3.2　算法操作

RSND 算法的具体操作步骤如下。

step1　节点 B 周期性地广播 Hello 消息进行邻居发现。在一个 Hello 周期内，如果 B 没有收到任何一个邻居节点 C 回复的 SV_C，则在该周期结束后，启动下一周期的邻居发现过程；否则，进入下一步。

step2　如果节点 B 是源节点，则节点 B、C 均建立一张与 SV 对应的表，存储每个数据分组的下一跳节点地址以及该数据分组的目的节点地址。B 收到 SV_C 后，比较 SV_C 和 SV_B，若 B 在 SV_C 中发现其中包含自己的数据分组且 C 正好是该数据分组的目的节点，则 B 的下一跳节点不是自私节点。

step3　如果不确定节点 B、C 中是否存在源节点，则 B 收到 SV_C 后，比较 SV_C 和 SV_B，获取 C 缓存中有而自己没有的数据分组信息并向 C 发送 Request 请求消息，C 收到 Request 后，根据请求消息向 B 发送数据分组，B 收到数据分组后，回复 ACK 给 C 并更新自己的 SV_B，节点 B 通过提取分组头部消息，判断分组的源节点是否为 C，若不是，则 C 不是自私节点，否则 C 存在自私嫌疑，B 根据网络中自私节点比例估计 C 的自私性。

step4　节点 C 收到来自节点 B 的 ACK 时，记录收到 ACK 的时间 t_0，并采用 RSSI 机制测量节点 B、C 间的间距 d_0。

step5　当节点 C 收到 B 广播的 Hello 消息时，记录收到时间 t_1、测量 B、C 间的间距 d_1。由 t_0、t_1、d_0 和 d_1 计算 B 的平均速度 v_1，并比较 d_0 和 d_1 的大小，若 $d_0 \geq d_1$ 且 v_1 不大，则 B、C 相互靠近且未脱离彼此的通信范围，C 通过监听 B 收帧，判断 B 的自私性。若 $d_0 < d_1$ 且 v_1 较大，则 B、C 可能脱离彼此的通信范围，若 C 未监听 B 发送数据分组，则不将节点 B 判定为自私节点。如果 C 收到的帧通过了帧校验，则判定 B 不是自私节点；否则，进入下一步。平均速度 v_1 的计算公式如下

$$v_1 = \left| \frac{d_1 - d_0}{t_1 - t_0} \right| \tag{1}$$

其中，d_1、d_0、t_1 和 t_0 分别表示 C 收到 B 的 Hello、ACK 消息时它们之间的间距和收到消息的时间。

step6　C 收到未通过校验的帧后，不直接丢弃该帧，而是提取帧中数据分组的头部并与 B 保存的已发数据分组的头部进行比对，若二者相同，则说明 B 转发了数据分组，B 不是自私节点；若二者不同，则提取一定长度（缺省值建议为 64 bit）的数据分组尾部信息和缓存分组进行比对，如果相同，则 B 不是自私节点，否则，将 B 归入难以确定类型。

3.3　性能分析

关于 RSND 算法的性能，本文进行了如下的理论分析。

引理 1　在相同的网络条件下，RSND 算法的自私节点检测准确率高于现有相关自私节点检测算法。

证明　假设网络中每条无线信道出现干扰以及数据分组发生碰撞的概率分别为 p_a 和 p_b。如图 1 所示，在均不考虑节点脱离通信范围的情况下，假设基于 2-ACK 的自私节点检测算法出现误判的概率为 P_0，则

$$P_0 = 2p_a + p_a^2 + 2p_b + p_b^2 \tag{2}$$

其中，$0 < p_a < 1$，$0 < p_b < 1$。假设 RSND 算法出现误判的概率为 P_1，则

$$P_1 = p_a + p_b + p_b^2 \tag{3}$$

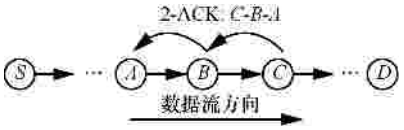

图 1　2-ACK 节点行为检测

比较式(2)和式(3)，显然 $P_0 > P_1$，即相对于基于 2-ACK 的自私节点检测算法，RSND 检测算法出现

误判的概率更低。

假设网络中因数据分组发生碰撞而出现误判的概率为 $p(0<p<1)$，在均不考虑节点脱离通信范围的情况下，假设 Watchdog 检测算法检测准确的概率和 RSND 算法检测准确的概率分别为 P_W 和 P_R，则

$$P_W = 1-p \tag{4}$$

$$P_R = 2p(1-p)+(1-p)^2 \tag{5}$$

将式(5)化简可得

$$P_R = 1-p^2 \tag{6}$$

比较式(4)和式(6)，可知 RSND 检测算法检测准确的概率高于 Watchdog 检测算法。

在相同的网络条件下，由于 RSND 检测算法考虑了节点收到错帧和节点脱离通信范围监听失败这 2 种情况，并采用了有效的机制进行了合理的处理，因此相对于其他检测算法，RSND 检测算法的自私节点检测准确率更高。

引理 2 在相同的网络条件下，RSND 算法的控制开销低于现有自私节点检测相关算法。

证明 假设节点发送消息的控制开销为 d，携带消息的平均控制开销为 e，网络中产生的消息总量为 m，消息到达目的节点平均跳数为 ETX。

基于 2-ACK 的自私节点监测算法中消息完成传输需要的总的控制开销为

$$T_2 = m(5d+e)(ETX-1) \tag{7}$$

RSND 算法中消息完成传输需要的总的控制开销为

$$T_R = m(4d+e)(ETX-1) \tag{8}$$

比较式(7)和式(8)可知，$T_R < T_2$，得证。

4 仿真分析

由于现实条件（如成本、时间等）的原因，同时考虑到专业网络仿真软件 OPNET 在网络通信协议/算法性能比较方面的准确性和接近网络实际测量结果的可信度，本文选择了业内流行的 OPNET 软件作为仿真平台，对所提 RSND 算法的有效性进行定量验证。

4.1 参数设置

在基于 Epidemic[14~17]机制的路由算法上加载 RSND 算法、基于 2-ACK 的自私节点检测算法和 Watchdog 检测算法，分别将它们表示为 R-Epidemic、A-Epidemic 和 W-Epidemic。加载这些自私节点检测算法的方法是在路由时避开自私节点，不向这些节点发送数据分组。主要仿真参数设置如表 1 所示。

表 1 主要仿真参数设置

参数	数值
仿真时间/s	3 000
模拟区域大小	1 000 m×1 000 m
节点数量	100
节点移动速率/(m·s^{-1})	1~3
节点通信方式	bluetooth
节点通信半径/m	10
节点移动模型	restrict random waypoint
数据传输速率/(kbit·s^{-1})	100
数据分组大小/KB	100
节点缓存大小/MB	30

4.2 仿真结果及分析

4.2.1 自私节点检测准确率

从图 2 中可以看出，随着自私节点比例的上升，RSND 算法能维持较高的自私节点检测准确率，与基于 2-ACK 的自私节点检测算法相比，RSND 算法检测准确率提高了 6%以上，主要原因在于提出的“错帧解析”、“信息挖掘”和“脱离判断”3 种新机制发挥了作用，使自私节点检测的准确率得到提高。

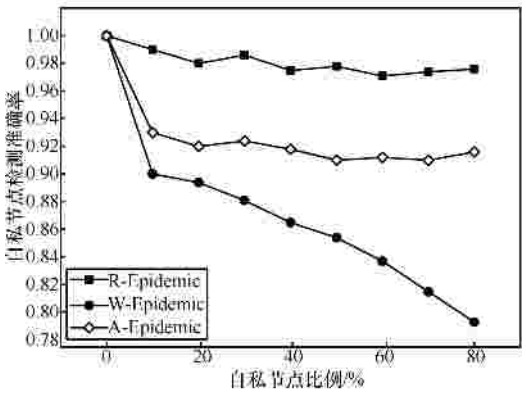

图 2 自私节点检测准确率

4.2.2 网络吞吐量

网络吞吐量是在单位时间内成功到达目的节点消息的比特数。吞吐量受网络的带宽与网络的额定速率的限制，计算公式为

$$p = \frac{P_D}{T_i} \tag{9}$$

其中，P_D 表示成功到达目的节点消息的比特数，T_i 表示网络运行时间。

如图 3 所示，相比与基于 2-ACK 的自私节点检测算法，RSND 算法能至少提高网络吞吐量 4%，主要原因是自私节点检测准确率高，被不合理惩罚的节点减少，因而有更多数据分组被转发到目的节点。

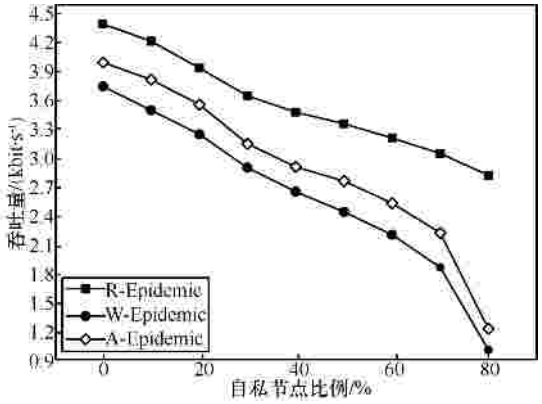

图 3　网络吞吐量比较

4.2.3　投递成功率

投递成功率是指成功到达目的节点的消息数与源节点创建的消息数的比值。计算公式为

$$D_{\text{rate}} = \frac{\sum_{i=1} D_i}{\sum_{j=1} S_j} \tag{10}$$

其中，D_i 表示已到达目的节点的消息个数，S_j 表示源节点所创建的消息个数。

如图 4 所示，相比于基于 2-ACK 的自私节点检测算法和 Watchdog 检测算法，RSND 算法的投递成功率更高，主要原因是自私节点检测准确率提高后，更多行为良好节点发出的数据分组被转发，从而到达目的节点的数据分组增加。

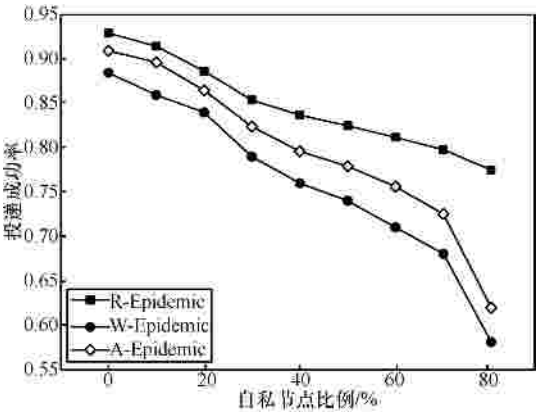

图 4　投递成功率

4.2.4　平均端到端时延

平均端到端时延是指所有消息到达目的节点时的平均时延，计算公式为

$$\overline{T} = \frac{\sum_{i=1} T_i}{\sum_{j=1} D_j} \tag{11}$$

其中，T_i 表示第 i 个到达目的节点的消息时延，D_j 表示已到达目的节点的消息个数。

如图 5 所示，相比于基于 2-ACK 的自私节点检测算法和 Watchdog 检测算法，RSND 算法能够减少分组的端到端时延，其原因估计在于自私性检测准确性提高后，数据分组被传送的概率在整体上有所增加，因而有利于它们更快地到达目的节点。

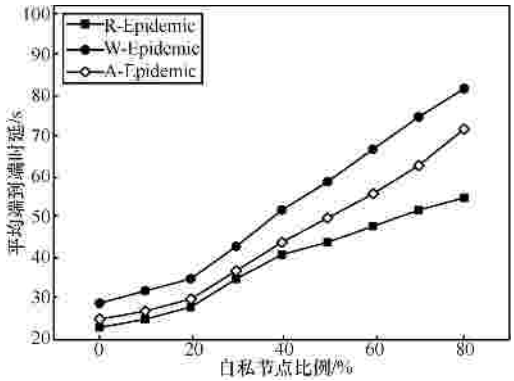

图 5　平均端到端时延

4.2.5　归一化控制开销

归一化控制开销是累加所有节点发出的控制消息的比特数与到达目的节点消息的比特数的比值，计算公式为

$$C = \frac{P_{\text{C}}}{P_{\text{C}} + P_{\text{D}}} \tag{12}$$

其中，P_{C} 表示全网发出的控制消息包含的比特数，P_{D} 表示所有到达目的节点消息的比特数。

如图 6 所示，相比 Watchdog 检测算法，RSND 算法能够降低归一化控制开销 15%以上，因而具有

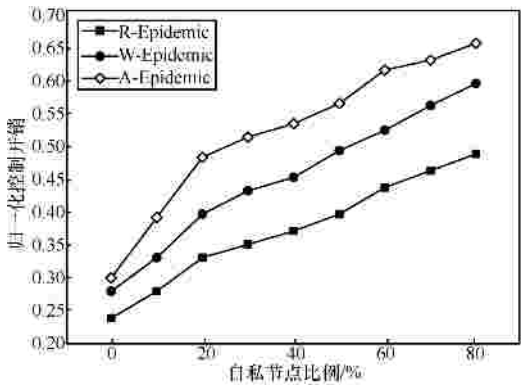

图 6　归一化控制开销

更高的效率，分析其主要原因在于自私节点检测准确率提高后，更多数据分组被送达它们的目的节点，使 Request 控制消息的数量在整体上会趋于减少，因而控制开销有所降低。

5 结束语

机会网络中节点的自私行为对网络吞吐量、投递成功率和网络开销等性能造成不良影响，本文为解决机会网络现有典型自私性检测算法在节点收到错帧和脱离通信范围时自私检测的准确性降低的问题，提出了一种可靠的机会网络自私节点检测算法并通过理论分析和仿真验证了其有效性。未来研究工作将围绕节点相遇信息的更深度挖掘展开。

参考文献：

[1] 熊永平, 孙利民, 牛建伟, 等. 机会网络[J]. 软件学报, 2009, 20(1): 124-137.
XIONG Y P, SUN L M, NIU J W, et al. Opportunistic networks[J]. Journal of Software, 2009, 20(1): 124-137.

[2] STAVROULAKI V, TSAGKARIS K, LOGOTHETIS M, et al. Opportunistic networks[J]. IEEE Vehicular Technology Magazine, 2011, 6(3): 52-59.

[3] 刘乔寿, 周建二, 张普宁. 机会网络中基于消息副本数量的自适应缓存管理策略[J]. 重庆邮电大学学报(自然科学版), 2012,23(4): 394-399.
LIU Q S, ZHOU J E, ZHANG P N. Adaptive cache management method for opportunistic network based on number of message copies[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2012,23(4): 394-399.

[4] RESTA G, SANTI G. A framework for routing performance analysis in delay tolerant networks with application to non-cooperative networks[J]. IEEE Transactions on Parallel and Distributed System, 2011, 23(1): 2-10.

[5] 张程, 刘慧君, 陈自郁, 等. 基于信用的重复博弈模型在节点转发中的应用[J]. 解放军理工大学学报, 2012, 13(2): 152-158.
ZHANG C, LIU H J, CHEN Z Y, et al. Credit-based repeated game model applied in transfer decision of opportunistic network[J]. Journal of PLA University of Science and Technology(Natural Sc nce Edition), 2012, 13(2): 152-158.

[6] BIGWOOD G, HENDERSON T. IRONMAN: Using social networks to add incentives and reputation to opportunistic networks[C]//2011 IEEE International Conference on Privacy, Security, Ri and Trust, and IEEE International Conference on Social Computing. IEEE, c2011: 65-72.

[7] MICHIARDI P, MOLVA R. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks[C]//IFIPTC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security. Portoroz, Slovenia, c2002: 107-121.

[8] BUCHEGGER S, BOUDEC J L. Performance analysis of the confidant protocol[C]//ACM International Symposium on Mobile Ad Hoc Networking Computing. Lausanne, Switzerland, c2002: 226-236.

[9] MARTI S, GIULI T J, LAI K, et al. Mitigating routing misbehavior in mobile ad hoc networks[C]//International Conference on Mobile Computing and Networking. Boston, USA, c2000: 255-265.

[10] 唐作用, 袁艺嘉, 董永强, 等. 基于信誉值维护的机会网络自私节点检测机制[J]. 通信学报, 2012,33 (z2): 217-221.
TANG Z Y, YUAN Y J, DONG Y Q, et al. Detection of selfish nodes based on credit mechanism in opportunistic networks[J]. Journal on Communications, 2012, 33(z2): 217-221.

[11] 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[J]. 软件学报, 2013, 24(4): 887-899.
QU D P, WANG X W, HUANG M. Selifish node detection and incentive mechanism in mobile P2P networks[J]. Journal of Software, 2013, 24(4): 887-899.

[12] 王立, 吴蒙, 常莉. 移动 ad hoc 网络基于信誉系统的节点协作方案[J]. 计算机技术与发展, 2010, 20(3): 32-35.
WANG L, WU M, CHANG L. A scheme to node cooperation based on reputation system in mobile ad hoc networks[J]. Computer Technology and Development, 2010, 20(3): 32-35.

[13] VIANI F, LIZZI L, ROCCA P, et al. Object tracking thro gh RSSI measurements in wireless senor networks [J]. Electronics Letters, 2008, 44(10): 653-654.

[14] BECKER V D. Epidemic routing for partially connected ad hoc networks[R]. USA: Duke University, CS-2000-06, 2000.

[15] 赵广松, 陈鸣. 自私性机会网络中激励感知的内容分发的研究[J]. 通信学报, 2013, 34(2): 73-84.
ZHAO G S, CHEN M. Research of incentive-aware data dissemination in selfish opportunistic networks[J]. Journal on mmunications, 2013, 34(2): 73-84.

[16] 任智, 黄勇, 曹建玲, 等. 基于邻居信息交换的机会网络低时延路由算法[J]. 华中科技大学学报(自然科学版), 2011, 39(2): 94-97.
REN Z, HUANG Y, CAO J L, et al. Low-delay routing algorithm for opportunistic networks by exchanging the neighborhood nformation[J]. Journal of Huangzhong University of Science and Technology (Natural Science Edition), 2011, 39(2):94-97.

[17] 王汝言, 金勇, 吴大鹏, 等. 面向机会网络的自适应冗余副本删除机制[J]. 重庆邮电大学报学报(自然科学版), 2013, 25(1): 59-63,74.
WNAG R Y, JIN Y, WU D P, et al. Adaptive redundant message deletion mechanism for opportunistic networks[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Sc nce Edition), 2013, 25(1): 59-63,74.

作者简介：

任智（1971-），男，四川内江人，重庆邮电大学教授，主要研究方向为宽带无线通信网络理论与技术。

谭永银（1989-），男，湖南常宁人，重庆邮电大学硕士生，主要研究方向为机会网络路由算法。

李季碧（1975-），女，四川开江人，重庆邮电大学讲师，主要研究方向为无线通信网络。

陈前斌（1967-），男，四川南充人，重庆邮电大学教授、博士生导师，主要研究方向为无线通信与网络。