doi:10.3969/j.issn.1000-436x.2012.12.010

基于信誉的延迟容忍网络双重 Spray and Wait 增强方案

张希，王晓飞，张权，唐朝京
（国防科学技术大学 电子科学与工程学院，湖南 长沙 410073）

摘 要：引入转发证据的概念，设计了节点行为观测协议，提出一种基于信誉的双重 Spray and Wait 增强方案。通过对原始协议直接传输阶段的建模，使得信誉门限的确定建立在概率计算的基础上。仿真结果表明，在自私节点存在的环境中，与原始方案相比，增强方案能够减少自私行为对网络的危害，提高网络性能。

关键词：信誉；延迟容忍网络；激励方案；路由
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2012)12-0079-06

Enhanced binary Spray and Wait scheme based on reputation for DTN

ZHANG Xi, WANG Xiao-fei, ZHANG Quan, TANG Chao-jing
(School of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China)

Abstract: A concept of forwarding credential was introduced, and a detection protocol of behavior was designed. A novel scheme which enhanced the prevalent binary Spray and Wait routing scheme was integrated with reputation to resist the impairment of selfishness. According to the model of bundle transferring, the determination of reputation threshold was based on probability computation. The simulation results suggest that the enhanced scheme gain an advantage over original one under selfish misbehavior.

Key words: reputation; DTN; incentive schemes; routing

1 引言

在各种无线网络应用中，节点移动特性、稀疏分布、无线设备射频关闭或障碍物造成的信号衰减等因素都可能导致网络的间歇性连通或长时间延迟。这类环境中，网络报文传输所需的端到端路径难以得到保证。为了有效解决受限环境中网络连通性的难题，延迟容忍网络（DTN, delay tolerant network）的研究[1,2]日益受到重视，并在军事战术网络、野生物种追踪、深空通信等领域初步展现了其应用价值。

为了提高 DTN 的传输效率，Spyropoulos 等人提出 Spray and Wait(SW)多副本路由方案[3]，缓解了资源消耗和传输延迟的矛盾。SW 路由方案包含 Spray 和 Wait 2 个阶段。在 S 阶段，每个报文都会生成相应的副本，并分发至多个不同的转发节点。在 W 阶段，如果报文转发过程中始终没有发现目的节点，则多个持有报文副本的节点切换至直接发送状态，仅仅将报文转发给目的节点。双重 Spray and Wait（BSW）是 SW 路由协议族中的一种运行模式。该模式下，如果节点持有多份报文副本，即处于 S 阶段，将每次转发持有的副本数量的一半给其他转发者。当仅持有一份副本时，即处于 W 阶段，节点等待目的节点的出现，并通过直接传输方

收稿日期：2011-10-17；**修回日期**：2012-09-19
基金项目：国家自然科学基金资助项目(61101073)
Foundation Item: The National Natural Science Foundation of China (61101073)

式完成转发。该方案提供了一种有效的多副本路由方式，在间歇连接的环境中得到较为广泛的应用。

这类多副本路由方案需要每个节点能够共享其资源实现整个网络的互联互通，并承担报文转发的工作。很多研究表明，如果缺乏合适的激励方案，网络节点因自身传输带宽、存储空间和能耗等因素的限制，难于克服自私的天性，分享有效资源[4,5]。伴随着自私节点数量的增多和自私行为的频繁发生，网络性能将受到严重影响，甚至妨碍整个网络的运行。DTN 本身所特有的网络割裂和间歇中断特性将使得这种危害进一步加剧[6,7]。信誉为抑制自私行为的发生提供了一种有效的解决办法。通过对用户行为的收集分析，提供信誉评分，作为节点行为的参考依据，判断节点是否存在自私行为[8~10]。

然而，现有的针对无线自组织网络和 P2P 网络的信誉方案并不适用于 DTN 环境。首先，现有方案都假设在源节点到目的节点之间存在一条端到端路径。这种假设因为 DTN 的网络割裂和间歇链接的特性而不能成立。其次，现有方案大多基于单副本路由方式，而 DTN 中为提高网络性能和传输可靠性，一般采用多副本路由方式。这使得现有方案不能应用于 DTN 环境。

本文将信誉与 BSW 相结合，以解决 DTN 环境中自私节点带来的网络性能下降甚至不可用的问题。首先，引入传输证据的概念，设计了观测协议以解决 DTN 环境下对节点行为的观测问题，实现对节点行为的数据统计。其次，依据节点行为的统计数据对节点进行信誉评分，实现对自私节点的辨识，改变原有 BSW 的路由选择过程；为 BSW 路由过程建模，通过概率计算确定信誉门限，避免了对门限的主观性、经验型的选择。最后，建立仿真实验平台，验证了该方案能够减少自私行为对 DTN 性能的负面影响，提高网络性能。

2 提出的方案

为实现信誉与 BSW 的融合，本方案设计了两大模块，即观测处理模块和信誉路由模块。在观测处理模块中，设计了一种应用于节点通信过程的观测协议，协议提供了对邻居节点行为监测的方法，取代原有信誉方案对混杂监听模式的依赖。该模块负责对统计数据的收集，以用于后续的信誉处理。在信誉路由模块中，通过处理节点交互统计数据以计算评分，从而判断节点是否有自私行为发生，优化原有的 BSW 路由选择。信誉与路由的结合，使得节点可以根据表征节点自私程度的评分判断自私节点，避免了自私节点对网络运行的危害。在方案的详细表述之前，首先对系统配置进行说明。

2.1 系统配置

本方案设计中需要配置离线的私钥生成器（OKG, offline key generator）负责节点注册阶段的密钥生成。系统应用了双线性对技术，采用 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 分别表示 q 阶的加法循环群和乘法循环群，用 P 表示加法循环群的生成元。双线性对 $\hat{e}:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$ 能够满足双线性、非退化性和可计算性。OKG 选择一个 $s\in\mathbb{Z}_q^*$ 作为私钥，计算其公钥 $P_{\text{pub}}=sP$，并选取一个散列函数 $H:\{0,1\}^*\to\mathbb{G}_1$。OKG 采用 $\{\mathbb{G}_1,\mathbb{G}_2,\hat{e},P,P_{\text{pub}},H\}$ 作为系统参数，在注册过程中配置到 DTN 节点中。同时，OKG 验证节点身份信息，并根据其身份信息计算节点私钥 $sk=sH(ID)$，并以 $pk=H(ID)$ 作为节点公钥。

当一个节点 i 需要转发一个报文 B 的时候，节点需要配置附属消息 Ai，由以下部分组成：BI 包含报文基础信息，其中有源节点、目的节点的身份信息，报文会话号等；FI，表示报文转发相关信息，其中，包括报文转发请求节点、接收节点以及下一跳的转发节点的身份信息。TS 和 Sig 分别表示时间戳和对报文的签名。

2.2 观测处理模块

观测处理模块的设计主要解决 DTN 环境下对节点行为观测和统计的问题。节点行为的观测方式是基础信誉数据采集的关键，也是信誉在 DTN 环境下应用的瓶颈。频繁的网络割裂和机会链路的特性导致经典的观测方式——混杂监听模式和源路由模式难于应用。混杂监听模式下，节点缓存发送给邻居节点的报文，截获并比对所有通过的报文与原始报文的差异，以未发生伪造和篡改来确定邻居节点的正常转发行为。然而，网络的间歇链接特性难以保证对无线链路的持续观测。总是存在一条端到端路径的假设同样不适用于 DTN，因而导致源路由相关方案的应用困难。

本方案引入转发证据的概念，设计了对节点行为的观测协议，将转发证据的生成与传播融入观测协议中，且转发证据的传输可以通过报文进行捎带，减少了网络资源的消耗。

以 $m\to n\to p$ 的报文传输过程为例描述观测

协议。节点 m 确定下一个节点之后，随机选择 $r\in\mathbb{Z}_q^*$，计算 $\sigma_1=sk_m+rH(B\|BI\|FI\|TS)$ 和 $\sigma_2=rP$，得到对报文签名 $Sig=(\sigma_1\|\sigma_2)$。这里选择 Sakai-Ohgishi-Kasahara 方案实现协议支持的签名[11]。

1) $m\to n$: B,Ai_m，其中，$Ai_m=(BI\|FI\|TS\|Sig)$；

当节点 n 接收报文和附属信息后，将执行以下步骤验证。

①验证报文基本信息的正确性，包括时间戳和 TTL 信息；

②验证 Ai_m 时间戳正确性；

③通过检查下式以便于确定签名的正确性。

$$\hat{e}(pk_m,P_{\text{pub}})\hat{e}(H(B\|BI\|FI\|TS),\sigma_2)=\hat{e}(\sigma_1,P) \quad (1)$$

2) $n\to m$: Fe_n，其中，$Fe_n=(BI\|Set_{\text{id}}\|TS\|Sig)$；

$n\to p$: B,Ai_n，其中，$Ai_n=(BI\|FI\|TS\|Sig)$；

验证通过之后，节点 n 发送转发证据 Fe 给节点 m 作为其成功转发报文的响应。Set_{id} 包括 3 个部分的身份信息，即报文转发节点、接收节点以及需要提供传输证据的节点。

节点 n 选择下一跳节点，重新计算附属信息，继续分发过程。

3) $p\to n$: Fe_p，其中，$Fe_p=(BI\|Set_{\text{id}}\|TS\|Sig)$；

节点 p 执行同样验证过程。验证通过后，发送传输证据 Fe 给节点 n，其中，Set_{id} 包含了节点 m,n 和 p 的身份信息。

4) $n\to m$: Fe_p，其中，$Fe_p=(BI\|Set_{\text{id}}\|TS\|Sig)$；

节点 m 确认 Fe 签名的正确性之后，确认节点 n 的转发行为。该模块将激活报文确认计数器，对相关统计数据进行操作。

针对 BSW 路由的两个阶段，模块配置两组统计量 $(t_{\text{sf}},c_{\text{sf}})$ 和 $(t_{\text{dt}},c_{\text{dt}})$ 分别对其进行统计。在节点 i 成功完成报文转发之后，如果接收节点 j 获得的报文副本数量大于 1，则节点 i 对节点 j 配置的计数器 t_{sf} 将增加，否则计数器 t_{dt} 增加。在节点 i 验证 Fe 成功后，如果节点 j 执行了扩散传输，则记录 S 阶段的确认报文数量的计数器 c_{sf} 将增加 1；如果其执行直接传输，则计数器 c_{dt} 增加。

按照观测协议设计，报文和传输证据 Fe 的成功传输都会激活该模块对相关统计数据执行操作。该模块的状态机模型以及观测协议的处理如图 1 所示。节点处于空闲状态，将根据报文转发、接收以及传输证据接收等行为而进入相关处理状态；处理完毕将恢复空闲状态。

2.3　信誉路由模块

信誉路由模块的设计主要解决信誉与 BSW 结合的问题。信誉提供了一种建立节点之间信任关系的有效方式，一种对节点合作性(或自私性)的度量方式。信誉的引入使得节点能够有效分辨自私节点并给予惩罚，甚至将其排除网络。信誉与路由的结合旨在提高网络对自私行为的鉴别度和适应度，从而提高网络性能。

很多信誉方案的研究工作都集中在对复杂的数学表达式的探索，以期带来的对节点自私行为更为精确、快速的评分，然而，却采用经验型的信誉门限进行判断[10, 12]。DTN 信誉的应用环境与 P2P 文件共享网络存在较大差异。后者的场景中存在大量的报文交互。而 DTN 一般配置在一个很大区域之中，2 个特定节点的交互次数相对较小。因此，本方案的信誉设计应用判别准则取代复杂的计算公式，可以表示为

$$\begin{cases} c_{\text{sf}}/t_{\text{sf}}\geqslant\eta_1\wedge c_{\text{dt}}/t_{\text{dt}}\geqslant\eta_2 & \Rightarrow\text{Honest}\\ c_{\text{sf}}/t_{\text{sf}}\leqslant\eta_1\vee c_{\text{dt}}/t_{\text{dt}}\leqslant\eta_2 & \Rightarrow\text{Selfish}\end{cases} \quad (2)$$

节点执行报文转发之前，都会按照判别准则对转发节点进行判定。如果节点 i 对节点 j 的两组统计数据都超过了设定门限值，那么认为该节点是诚实理性的，将按照源 BSW 方案执行路由；如果两组数据中有一组低于设定门限，则认为节点 j 在转发过程有不良行为发生。如果节点 j 被判定为自私节点，节点 i 将其加入黑名单，并拒绝节点 j 的所有转发请求。同时，生成针对节点 j 的控告消息，在报文转发的过程中进行捎带，以提醒其他节点。如果针对节点 j 的控告节点数目超过一个特定门限值，则该节点将直接被加入黑名单。因此，在转发过程中有不良表现的节点将最终被排除出网络。

门限设定与路由两个阶段的情况直接相关。S 阶段要求节点将多余的报文副本尽快散发。节点可以轻易将报文副本分发完毕。$c_{\text{sf}}/t_{\text{sf}}$ 近似于 Fe 的传输概率，可以表示为

$$\eta_1=\alpha P_{Fe}\geqslant(1-P_M)P_{Fe} \quad (3)$$

其中，$P_{Fe}\approx\sum c_{\text{sf}}/\sum t_{\text{sf}}$。

其设定为确认自私行为的一种评判标准。α 和 P_M 分别表示容忍参数和网络允许范围内的自私行为比率的上限。保证 $\alpha \geqslant 1-P_M$，以避免允许范围之外的自私节点逃避检测。

在 W 阶段，要求节点通过直接传输的方式将唯一的报文副本转发给目的节点。因此，确认报文的传输概率可以表示为

$$P = P_{Fe} \times P_{\mathrm{dt}}$$

其中，P_{dt} 表示报文从转发节点到目的节点的直接传输概率。当节点配置传输范围为 K 的无线设备时，假设无线设备具有较高的传输速率且忽略信道干扰，则报文的直接传输问题转化为在分布在一定区域内的 2 个节点移动到直线距离小于 K 的范围内的问题。那么，该问题进一步映射为 2 个节点之间距离小于 K 的模型。因此，直接传输的概率问题最终被转化为在一个广大区域 2 个节点之间的距离小于 K 的问题。参考 Bettstetter 等在随机路点移动模型(RWP, random waypoint)方面的研究[13]，得到了 RWP 模型的空间分布函数，且该分布与速度无关，该函数可以表示为

$$f(x,y) \approx \frac{36}{a^6}\left(x^2-\frac{a^2}{4}\right)\left(y^2-\frac{b^2}{4}\right) \tag{4}$$

以近似节点在 $a\times a$ 的正方形范围之内的分布。其中，$-a/2 \leqslant x \leqslant a/2$ 且 $-a/2 \leqslant y \leqslant a/2$。这个表达式非常接近真实仿真里的分布。根据前述的建模，在同样的移动模型下，直接传输的概率可以结合仿真场景得到

$$\begin{aligned} P_{\mathrm{dt}} &\approx \iint_{|\boldsymbol{X}_1-\boldsymbol{X}_2|<K} \iint f(x_1,y_1)f(x_2,y_2)\mathrm{d}x_1\mathrm{d}y_1\mathrm{d}x_2\mathrm{d}y_2 \\ &= \iint_{\substack{-a/2\leqslant x_1\leqslant a/2\\ -a/2\leqslant y_1\leqslant a/2}} f(x_1,y_1)\mathrm{d}x_1\mathrm{d}y_1 \cdot \\ &\quad \iint_{\substack{x_1-K/2\leqslant x_2\leqslant x_1-K\\ y_1-\sqrt{K^2-(x_2-x_1)^2}\leqslant y_2\leqslant y_1+\sqrt{K^2-(x_2-x_1)^2}}} f(x_2,y_2)\mathrm{d}x_2\mathrm{d}y_2 \end{aligned} \tag{5}$$

根据仿真场景的参数得到积分结果，则门限可以表述为

$$\eta_2 = \alpha P_{Fe} P_{\mathrm{dt}} \geqslant (1-P_M) P_{Fe} P_{\mathrm{dt}} \tag{6}$$

3 性能仿真

为了验证增强方案的有效性，基于 ONE 仿真平台[14]，建立 4 000m×4 000m 的正方形仿真区域。按照 RWP 移动模型，配置 250 个移动节点，并设定其速度为 10~50km/h，通信范围为 200m。按照一定比例选择节点执行自私行为，随机丢弃转发报

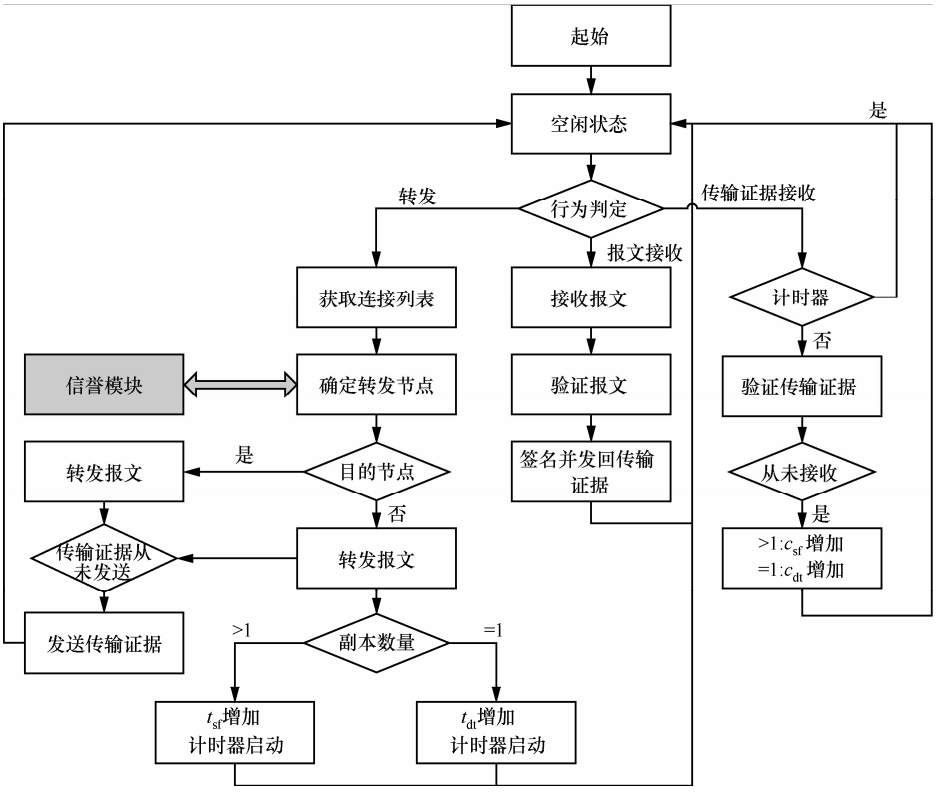

图 1 观测处理模块的状态机模型

文。在此环境下，与原始 BSW 方案进行对比试验，验证提出的方案对节点自私行为的有效性。

通过配置报文副本数目为 4 和 16，仿真结果显示了伴随自私节点比率增加，分别应用两种方案的网络性能变化。如图 2(a)所示，当自私节点的比率由 0%上升为 30%时，原始方案的传输率由 0.86 下降为 0.59，传输效率降低接近 27%。由此可知，自私行为严重影响了 DTN 网络的性能。两条虚线之间的差异同样值得关注。低副本数目 BSW 方案因为较低的网络消耗而在自私节点比率较低时，相对于高副本数目配置有一定优势。然而，伴随自私节点数目的增加，高副本数目的 BSW 方案因自私行为对报文的丢弃反而有着更优的传输效率。增强方案的下降趋于缓慢，两种方案之间的差距随着自私节点比率的增加而不断扩大。在恶意节点的比率达到30%的时候，增强方案的传输效率仍然接近75%。不同于 BSW 方案，高副本数目的配置对于有自私行为检测的增强方案而言，其网络消耗一直都是一种浪费和负担，因此其性能始终较低。

自私节点比率的增加使得网络中的报文丢弃行为更加频繁，从而影响到网络中存在的副本数目。而增强方案因为对自私节点的辨识，一定程度上抑制了对报文的丢弃，反而使得网络中副本数目较多，因而其消耗比率一直比同样副本数目配置的原始方案高，如图 2(b)所示。对于 DTN 网络的平均延迟和平均缓存时间而言，因为自私节点对报文的丢弃，使得网络实际报文副本数目较少，因而增大了网络成功传输的时间以及报文的缓存时间，使得其相对于增强方案有着更高的延迟和缓存时间。然而，高副本配置的方案允许更多的网络副本能够尽快散播，大大降低了网络整体的报文传输时间和缓存时间，因此，高副本配置的方案在平均延迟和缓存时间上有着更多优势，如图 2(c)和 2(d)所示。

综上所述，与原有的 BSW 方案相比，本文提

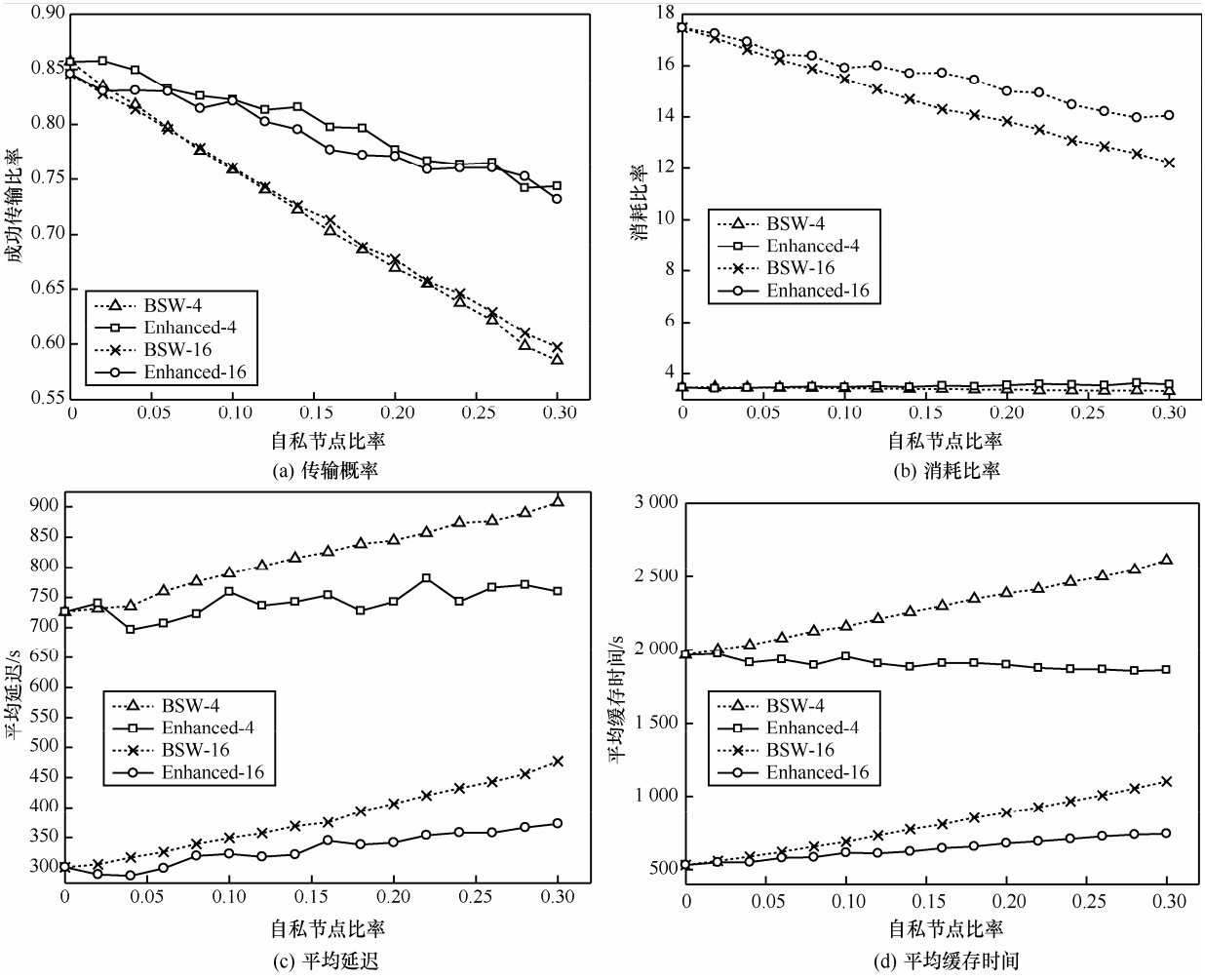

图 2　伴随自私节点比率增加，网络各项性能指标变化情况

出的增强方案能够有效的区分和隔离自私节点，并且可以更好地容忍节点的自私行为，实现更佳的网络性能。

4　结束语

信誉与 BSW 方案的结合使得增强方案能够在自私节点存在的环境中有效的提高 DTN 的性能，并且可以有效的激励节点进行正常的网络行为，培养节点之间的信任关系。节点的自私行为会导致网络的排斥，在一定程度上抑制了自私行为的发生。

延迟容忍网络的自私行为模型和信誉应用是下一步研究的重点。信誉在 DTN 中的应用仍然是该领域一个开放性问题，值得更多研究者的关注。

参考文献：

[1] FALL K. A delay-tolerant network architecture for challenged Internets[A]. Computer Communication Review[C]. Karlsruhe, Germany, 2003.

[2] FALL K, FARRELL S. DTN: an architectural retrospective[J]. IEEE Journal on Selected Areas in Communications, 2008, 26(5): 828-836..

[3] SPYROPOULOS T, PSOUNIS K, PAGHAVENDRA C S, *et al.* Spray and Wait: an efficient routing scheme for intermittently connected mobile networks[A]. ACM SIGCOMM Workshop on Delay-Tolerant Networking(WDTN)[C]. USA, 2005.252-259.

[4] YOO Y, AGRAWAL D P, Why does it pay,to be selfish in a MANET[J]. IEEE Wireless Communications, 2006, 13(6): 87-97.

[5] MARIAS G F, GEORGIADIS P, FLITZANISD, *et al.* Cooperation enforcement schemes for MANETs: a survey, Wireless Communications & Mobile Computing, 2006,6(3):319-332.

[6] LU R, LIN X D, AHU H J, *et al.* Pi:a practical incentive protocol for delay tolerant networks[J]. IEEE Transactions on Wireless Communications, 2010, 9(4):1483-1493.

[7] ZHU H J, LIN X D, LU R X, *et al.* SMART: a secure multilayer credit-based incentive scheme for delay-tolerant networks[J]. IEEE Transactions on Vehicular Technology, 2009, 58(8):4628-4639.

[8] ZHOU Y, ZHAN H W. An incentive-based reputation mechanism for mobile ad hoc networks[A]. 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing[C]. Dalian, China, 2008. 1-4

[9] ZHOU R F, HWANG K. PowerTrust: A robust and scalable reputation system for trusted peer-to-peer computing[J]. IEEE Transactions on Parallel and Distributed Systems, 2007,18(4): 460-473.

[10] ZHANG H, PUAN H X, LIU W. RRM: an incentive reputation model for promoting good behaviors in distributed systems[J]. Science in China Series F-Information Sciences, 2008, 51(11): 1871-1882.

[11] SAKAI R, OHGISHI K, KASAHARA M. Cryptosysytems based on pairing[A]. Symposium on Cryptography and Information Security (SCIS)[C].Okinawa, Japan 2000.

[12] GANERIWAL S, BALZANO L K, SRVASTAVA M B. Reputation-based framework for high integrity sensor networks[J]. Acm Transactions on Sensor Networks, 2008,4(3): 1-37.

[13] BETTSTETTER C, WAGNER C. The spatial node distribution of the random waypoint mobility model[A]. German Workshop on Mobile Ad Hoc Networks (WMAN)[C]. Ulm, Germany, 2002.

[14] The one simulator. [EB/OL]. http://www.netlab.tkk.fi/tutkimus/dtn/theone/.

作者简介：

张希（1983-），男，山东济南人，博士，国防科学技术大学工程师，主要研究方向为延迟容忍网络路由算法、信誉方案和移动模型等。

王晓飞（1981-），男，河北承德人，博士，主要研究方向为频谱管理、协议设计和信息安全等。

张权（1974-），男，上海人，博士，国防科学技术大学副教授、硕士生导师，主要研究方向为信息安全、无线网络安全和量子通信等。

唐朝京（1962-），男，江苏武进人，博士，国防科学技术大学电子科学与工程学院院长、教授、博士生导师，主要研究方向为信息安全、空间通信和量子通信等。