

## 中断容忍网络中一种激励相容的两跳路由协议

文 鼎<sup>1</sup>, 蔡 英<sup>1,2\*</sup>, 李 卓<sup>1,2</sup>

(1. 北京信息科技大学 计算机学院, 北京 100101; 2. 北京信息科技大学 网络文化与数字传播研究北京市重点实验室, 北京 100101)

(\* 通信作者电子邮箱 ycai@bistu.edu.cn)

**摘 要:** 针对中断容忍网络(DTN)中节点自私造成通信性能下降等问题, 提出了一种激励相容的两跳(TIC)路由协议, 以选择最优中继节点, 在综合考虑节点间的相遇概率及传输消耗的情况下, 保证节点在诚实汇报相遇情况及传输消耗时利益最大化。同时引入基于双线性映射的签名技术, 有效地防止恶意节点篡改信息且确保参与转发的中继节点安全地获取报酬。

**关键词:** 中断容忍网络; 路由协议; 激励相容; 自私; 安全

**中图分类号:** TP393 **文献标志码:** A

### Two-hop incentive compatible routing protocol in disruption-tolerant networks

WEN Ding<sup>1</sup>, CAI Ying<sup>1,2\*</sup>, LI Zhuo<sup>1,2</sup>

(1. Computer School, Beijing Information Science and Technology University, Beijing 100101, China;

2. Beijing Key Laboratory of Internet Culture and Digital Dissemination Research,  
Beijing Information Science and Technology University, Beijing 100101, China)

**Abstract:** A Two-hop Incentive Compatible (TIC) routing protocol was proposed for Disruption-Tolerant Networks (DTN) to defend the degradation of communication performance caused by selfish nodes. TIC selected the optimal relay node, which took both the encounter probability and transmission cost into account and ensured that nodes could maximize their profit when they reported their encounter probability and transmission cost honestly. At the same time, a signature technology based on bilinear map was introduced to ensure the selected relay nodes to get the payment securely, which can effectively prevent the malicious nodes from tampering the messages.

**Key words:** Disruption-Tolerant Networks (DTN); routing protocol; incentive compatible; selfish; security

## 0 引言

中断容忍网络(Disruption-Tolerant Networks, DTN)节点间在有传输机会出现时进行信息传递, 可降低无线骨干网络(3G等)上的负载。在文件共享、数据批量传输领域<sup>[1-3]</sup>, DTN已得到实际应用。由于节点的频繁移动、节点稀疏性、无线传输范围的限制等因素, DTN中两个节点间并不能保证任意时刻均有一条连接的通路。为保持网络中的正常通信, 需要节点间相互合作。

DTN中节点采用“存储-携带-转发”的方式来传递信息, 由于通信资源的有限性易造成自私行为的产生: 节点更倾向于让其他节点为自己传输信息, 而自己则尽可能少地提供中继服务。在数据中继过程中, 自私节点可能通过谎报自己同其他节点的相遇概率、传输开销等手段来避免被选做中继节点, 这样会造成数据被拒绝接收、拒绝转发等现象, 从而严重影响网络的性能, 更有甚者会造成网络的瘫痪。因此, 必须针对节点这类自私行为设计有效的防御机制。

基于算法博弈论, 本文提出了一种激励相容的两跳(Two-hop Incentive Compatible, TIC)路由协议, 其中源节点为每一报文传输确定一个报酬值, 源节点选择中继节点时基于一种新分配算法: 选择效益最大的节点, 由证明可知该算法下节点只有在汇报真实的同其他节点相遇概率、传输开销时其利益值才可最大, 由此可保证节点诚实地参与中继节点的选择过程。

同时, 引入虚拟银行(Virtual Bank, VB)概念, 通过VB来奖励参与转发的中继节点。当一个节点拒绝为其他节点转发报文时, 那么该节点将无法得到报酬, 即无法享受其他节点为其提供服务, 从而避免了节点丢弃、拒绝转发报文的自私行为。为防止恶意节点通过欺骗手段得到更多的报酬或者不传递数据仍能得到报酬, 利用双线性映射的特点来防止信息的伪造和篡改。

## 1 相关工作

早期, DTN的研究主要集中在如何基于机会传输设计高效的传输机制上, 多数假设每个节点会为其他节点转发报文, 即不存在自私行为, 如文献[4]。之后, 研究者发现实际网络中, 可能存在着大量的自私节点, 并发现自私节点的存在会大幅降低目的节点收到报文的机会, 影响网络的性能<sup>[5-7]</sup>。对于如何防御自私节点攻击, 目前的研究主要分为两类: 基于声望的机制(reputation based schemes)和基于信用的机制(credit based schemes)。基于声望的机制<sup>[8]</sup>主要依赖节点自身去监视周围邻居节点的流量同时记录互相的声望值来发现自私节点, 并将其孤立出网络作为惩罚, 以此来刺激其他节点不要表现出自私行为。在基于信用的机制中<sup>[9-10]</sup>, 节点通过提供中继服务(传递数据包)来获得信用值(如虚拟货币), 并且通过支付信用值来获得其他节点提供的服务(接收需要的数据包), 没有信用值将无法得到其他节点的服务, 而只有参与转

收稿日期: 2012-12-03; 修回日期: 2013-01-05。 基金项目: 北京市教委科技发展计划项目(KM201110772013, KM201311232014); 北京信息科技大学网络文化与数字传播北京市重点实验室开放课题(6ICDD201206, 7ICDD201207, 5026035413)。

作者简介: 文鼎(1987-), 男, 河北邢台人, 硕士研究生, 主要研究方向: 无线网络安全; 蔡英(1966-), 女, 四川绵阳人, 副教授, 主要研究方向: 无线网络、计算机安全; 李卓(1983-), 男, 河南南阳人, 讲师, CCF会员, 主要研究方向: 无线网络、移动计算。

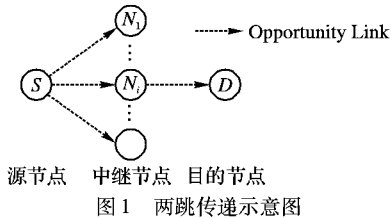
发信息才有机会获得信用值,以此来鼓励节点去参与传递。

与文献[8]不同,本文采用激励机制来刺激自私节点传递信息,而不是单纯地移除或者孤立自私节点,这是因为DTN本身连接受限、传输机会宝贵,节点的不断减少只会加剧网络服务质量的降低。与文献[9-10]工作不同,本文考虑了自私节点谎报相遇信息、传输开销这一恶意行为,并针对此设计了一套激励机制;同时,针对中继节点在获取报酬过程中可能受到的恶意攻击,本文提出了一套基于双线性映射的安全机制。

## 2 系统模型和设计目标

### 2.1 网络模型

本文的DTN模型用一个有向图 $G=(V,E)$ 来表示, $V$ 代表网络中的节点, $E$ 代表网络中节点的概率连接。网络中数据传输采用两跳(Two hop)方式,即每个源节点 $S$ 发送信息副本给中继节点,中继节点将数据传递到目的节点 $D$ ,不再经由其余节点中继,如图1所示。



网络中节点(比如智能手机等)同时具备3G上网、WiFi通信能力;为降低3G骨干网络负载,节点只能在传递控制信息(注册、支付、获取报酬等)时接入3G网络,在传递数据内容时,通过基于WiFi的节点间机会传输实现。假设存在一个离线安全管理器(Offline Security Manager, OSM)和一个虚拟银行VB, OSM负责密钥管理,在一个节点加入DTN前,都要在OSM处注册,注册后每个节点会获得自己的公钥证书。VB负责存储源节点的报酬即虚拟货币,并支付给满足条件的中继节点。假设DTN中的任一节点随时都可以通过3G网络连接到VB,并且利用目的节点返回的Ack领取相应的报酬。虚拟货币可以用来支付为其提供数据转发服务的中继节点,如果节点不参与转发包,那么就得不到虚拟货币,从而无法得到其他节点的服务。本文假设任意节点只要被选作中继节点,为了获得利益就一定会去转发包。

### 2.2 节点模型

在DTN中,每个节点 $i$ 都有自身的参数值 $\theta_i$ ,其包括节点 $i$ 与节点 $j$ 的相遇概率 $p_{ij} \in [0,1]$ ,及传递信息的非负开销 $c_{ij}$ ,  $\theta_i = (p_i, c_i)$ ,其中 $p_i = (p_{i1}, p_{i2}, p_{i3}, \dots)$ ,  $c_i = (c_{i1}, c_{i2}, c_{i3}, \dots)$ 。这些参数信息是每个节点非公开的私有信息。当源节点想要发送一个数据时,其他节点将向其汇报自己的参数值 $\hat{\theta}_i$ ,以竞拍得到数据转发的机会。节点为了能赢得转发机会,可能不会报价自己真实的参数值,本文通过设计激励机制来鼓励节点报价自己真实的参数值,第3章会证明只有这样节点才能实现自身利益最大化。

### 2.3 移动模型

DTN中的节点通常由人所携带的一些移动设备构成,因此它们的移动模型通常是由人的移动行为来确定。人在社会环境中的移动行为具有一定的规律性,比如在校学生经常出现在宿舍、教室和食堂等学校建筑物中,而工作中的人经常出现在家和工作单位之间。因此,可以认为DTN中的节点

在不同建筑物间运动,当节点运动到同一建筑物内时相互之间可以直接进行数据交换,而不同建筑之间的节点不能直接进行数据交换。如图2所示,以学校为例,在宿舍中的节点 $S$ 想给在食堂中的 $D$ 节点发送一个报文,那么 $S$ 可以从宿舍中的其余节点间选择一个最优的节点作为中继并发给其报文,当该中继节点移动到食堂后即可将报文转发给 $D$ 。

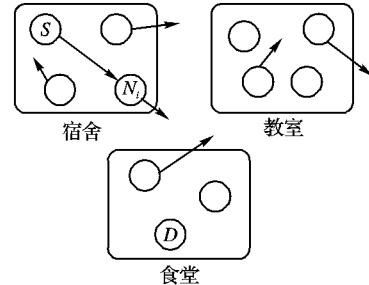


图2 节点移动模型示意图

### 2.4 攻击模型

把DTN中不合作节点分为两种类型:自私节点和恶意节点。自私节点只有在获得或追求自身利益最大化时才会为其他节点传递数据包。恶意节点会破坏网络的正常运行,它们试图通过欺骗手段得到更多的虚拟货币或者不传递数据但仍能得到报酬。因此归纳为如下两种攻击方式:

- 1) 拒绝服务攻击。节点不参与转发或者故意报高价获得转发机会,但故意不去转发,并将报文丢掉。
- 2) 伪造攻击。节点可能伪造一个假的Ack以此到VB处领取报酬,而实际上该节点并没有完成传送。

### 2.5 设计目标

一个好的激励系统应有能力防御自私节点和恶意节点,可鼓励自私节点来传递数据,也能防范恶意节点通过伪造记录来骗取报酬,即要实现如下目标:

- 1) 激励相容(Incentive Compatible, IC)。每个节点报价自己真实的参数值对它们来说是一个优势策略,即当节点报价 $\theta_i$ 时,节点 $i$ 的期望净利润 $u_i$ ,报价 $\hat{\theta}_i$ 时期望净利润 $\hat{u}_i$ ,总存在 $u_i \geq \hat{u}_i$ 。
- 2) 个体理性(Individual Rational, IR)。每个节点能有一个非负期望净利润,即 $u_i \geq 0$ 。
- 3) 安全(Security)。协议应该能抵御节点的伪造攻击。

## 3 TIC路由协议

本章介绍中断网络中一种新型的激励相容两跳路由协议TIC。先给出相关的背景知识,然后描述协议的过程,并给出相关证明。

### 3.1 双线性映射

在TIC中,利用双线性的特点来防止信息的伪造和篡改。设 $G_1, G_2$ 分别为加法循环群和乘法循环群,阶都为 $q$ ,设 $P$ 为 $G_1$ 的生成元,定义双线性映射为 $e: G_1 \times G_1 \rightarrow G_2$ ,该映射满足如下特性:

- 1) 双映射性。对 $\forall a, b \in \mathbb{Z}_q^*, P \in G_1$ ,有 $e(aP, bP) = e(P, P)^{ab}$ 。
- 2) 非退化性(Non-Degenerate)。不存在 $p \in G_1$ 使得 $e(P, P) = 1$ 。
- 3) 可计算性。存在有效的算法,对于 $P, Q \in G_1$ ,可计算 $e(P, Q)$ 。

### 3.2 协议过程

当源节点 $S$ 想发送一个报文给目的节点时, $S$ 附近想做中

继的节点会向  $S$  发送自己的参数  $\theta_i$ ,  $S$  根据中继选择算法从中选取一个最优节点作为中继节点,如图3所示,当  $S$  把报文发给中继节点后,会把相应的报酬和中继节点的身份信息发给 VB。当中继节点成功完成报文的传递时,凭借目的节点的反馈信息 Ack 可到 VB 处领取报酬,VB 验证身份信息无误后会将报酬发给该中继节点。如果在规定时间内中继节点没有转发成功,即没有节点凭 Ack 去 VB 处领取报酬,那么 VB 会将报酬返回给  $S$  节点。

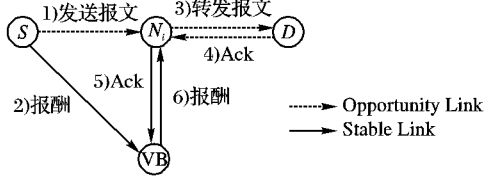


图3 协议流程

### 3.3 协议实现

1) 系统初始化。OSM 将双线性对的参数  $(q, G_1, G_2, e, P)$  引进作为系统参数,再加入哈希函数:  $H: \{0, 1\}^* \rightarrow G$ 。这些系统参数  $(q, G_1, G_2, e, P, H)$  预加载到每个 DTN 节点中。对每个即将加入到 DTN 中的节点,随机选择  $SK_N \in \mathbf{Z}_q^*$  作为自己的私钥,相应的公钥为  $PK_N = SK_N P$ ,然后 OSM 发给其相应的公钥证书。

2) Bundle 的生成。数据在节点间以 Bundle 的形式传递,当  $S$  节点选择好中继节点  $N_i$  后, $S$  需要对发送的 Bundle 进行签名:  $Sig_S = SK_S H(B \parallel S \parallel D \parallel TS \parallel TTL \parallel N_i)$ ,其中  $TS$  为 Bundle 的生成时间,  $TTL$  为 Bundle 的失效时间。然后发送  $B, S, D, TS, TTL, Sig_S$  和  $Cert_S$  给选定的中继节点  $N_i$ 。

3) Bundle 的转发。中继节点  $N_i$  收到后首先检查 Bundle 的时间是否失效,若失效则丢弃该 Bundle,否则在 Bundle 中加入  $Cert_{N_i}$ ,然后在其遇到目的节点时将其发给  $D$ 。

目的节点  $D$  收到信息后,首先检查 Bundle 时间是否失效,验证  $Cert_S$  和  $Cert_{N_i}$  之后,验证  $S$  的签名,计算  $e(P, Sig_S) = e \cdot (PK_S, H(B \parallel S \parallel D \parallel TS \parallel TTL \parallel N_i))$  是否成立。如果  $B, S, D, TS, TTL, Sig_S, Cert_S$  之中被修改,那么上述等式中哈希函数的值将改变,整个等式将不成立,节点  $D$  将丢掉该报文;如果成立将向中继节点  $N_i$  回馈一个加密的 Ack(用  $D$  的私钥进行加密),以此证明  $N_i$  确实完成了信息的传递任务,  $N_i$  凭此 Ack 可到 VB 处领取报酬。

### 3.4 中继节点的选择

当节点  $S$  收到各个节点的报价信息后采用如下算法来确定中继节点。

算法 中继节点选择算法。

输入 节点的报价参数  $\hat{\theta}_i$ ;

输出 被选中中继的节点身份和应得的报酬值。

1) 通过计算比较节点利益最大的节点。

Let  $i \leftarrow \arg \max_k (\hat{p}_k \cdot V - \hat{c}_k)$

2) 确定中继节点。

$f_i(\hat{\theta}) = \{1\}$

3) 计算中继节点的报酬值。

$r_i(\hat{\theta}, \mu) = V \cdot \mu - \max_{k \neq i} (\hat{p}_k \cdot V - \hat{c}_k)$

4) 对所有满足  $j \neq i$ , 执行 5)。

5) 对没有选上的节点,其利益为 0。

$f_i(\hat{\theta}) = \emptyset$

$r_j(\hat{\theta}, \mu) = 0$

6) 返回  $i, r_i(\hat{\theta}, \mu)$ 。

其中  $V$  表示源节点报文发送到目的节点后的利润值;  $f_i(\hat{\theta})$  表示节点  $i$  根据其报价参数  $\hat{\theta}$  是否赢得竞争;  $r_i(\hat{\theta}, \mu)$  表示  $i$  的报酬值,  $\mu$  表示传递完成情况,与  $\hat{\theta}$  独立,其中  $\mu = 0$  表示传递失败,  $\mu = 1$  表示传递成功。对于报价失败的节点  $i$ ,将不予报酬。随后继续通过该算法选择下一节点进行转发信息。

现在证明该机制满足个体理性 IR, 激励相容 IC, 然后给出安全性证明。其中假设节点  $i$  的真实参数为  $\theta_i = (p_i, c_i)$ , 报价参数为  $\hat{\theta}_i = (\hat{p}_i, \hat{c}_i)$ ,  $i$  的期望净利润分别为  $u_i$  和  $\hat{u}_i$ 。

证明

1) 个体理性 IR。

① 若  $i$  以真实参数报价赢得竞争,假设除节点  $i$  外利益最高的节点为  $j$ ,其报价  $\theta_j = (p_j, c_j)$ 。若节点  $i$  传递成功,由中继节点选择算法可知节点  $i$  成功转发后的报酬值为  $V - (p_j \cdot V - c_j)$ ;若  $i$  传递失败,则其报酬值为  $-(p_j \cdot V - c_j)$ ,则此时  $i$  的期望净利润可由式(1)推出:

$$u_i = p_i [V - (p_j \cdot V - c_j)] - (1 - p_i)(p_j \cdot V - c_j) - c_i = (p_i - p_j) \cdot V + c_j - c_i \quad (1)$$

因  $i$  赢得竞争,故

$$(p_i \cdot V - c_i) > (p_j \cdot V - c_j) \rightarrow$$

$$(p_i - p_j) \cdot V + c_j - c_i > 0$$

可得  $u_i > 0$ ;

若  $i$  以真实参数报价没有赢得竞争,则  $u_i = 0$ 。

因此,当  $i$  以真实参数报价时,期望净利润  $u_i \geq 0$ 。

② 若  $i$  以  $\theta_i = (p_i, c_i)$  报价没有赢得竞争,而以  $\hat{\theta}_i = (\hat{p}_i, \hat{c}_i)$  报价赢得竞争,即

$$(\hat{p}_i \cdot V - \hat{c}_i) > (p_j \cdot V - c_j) > (p_i \cdot V - c_i) \rightarrow$$

$$(p_i - p_j) \cdot V + c_j - c_i < 0$$

虽然报价  $\hat{\theta}_i = (\hat{p}_i, \hat{c}_i)$  赢得竞争,但  $i$  的实际期望净利润值仍需按照其真实参数  $\theta_i = (p_i, c_i)$  来计算的,如式(2)所示:

$$\hat{u}_i = p_i [V - (p_j \cdot V - c_j)] - (1 - p_i)(p_j \cdot V - c_j) - c_i = (p_i - p_j) \cdot V + c_j - c_i < 0 \quad (2)$$

若  $i$  以  $\hat{\theta}_i = (\hat{p}_i, \hat{c}_i)$  报价没有赢得竞争,则  $u_i = 0$ 。

因此报价  $\hat{\theta}_i$  时,  $\hat{u}_i \leq 0$ 。

综上所述,只有  $i$  以真实参数报价时,才能保证其期望净利润非负,该机制鼓励每个节点报价其真实的信息。

2) 激励相容 IC。

① 若以  $\theta_i$  和  $\hat{\theta}_i$  都赢得竞争,则此时  $i$  的期望净利润都是按照真实参数值来计算的,此时  $u_i = \hat{u}_i$ 。

② 若以  $\theta_i$  报价赢得竞争,则  $u_i > 0$ ,而以  $\hat{\theta}_i$  报价没有赢得竞争,则  $\hat{u}_i = 0$ ,此时  $u_i > \hat{u}_i$ 。

③ 若以  $\theta_i$  报价没有赢得竞争,而以  $\hat{\theta}_i$  报价赢得竞争,则  $u_i = 0, \hat{u}_i$  按真实参数计算,如式(3)所示:

$$\hat{u}_i = p_i [V - (p_j \cdot V - c_j)] - (1 - p_i)(p_j \cdot V - c_j) - c_i = (p_i - p_j) \cdot V + c_j - c_i < 0 \quad (3)$$

此时  $u_i > \hat{u}_i$ 。

④ 若以  $\theta_i$  和  $\hat{\theta}_i$  报价都没有赢得竞争,则此时  $u_i = \hat{u}_i$ 。

综上所述,无论  $i$  能否赢得竞争,只有以真实参数报价才

是最优选择。

下面给出一个例子来说明: 源节点  $S$  想要传递一个报文给  $D$ , 利润  $V = 210$ , 接收到三个节点的参考报价, 如表 1 所示。

表 1 节点参数信息

节点	$c_i$	$p_i$
1	35	0.5
2	100	1.0
3	60	0.9

假设三个节点报价真实, 那么节点 3 会以最大利益  $0.9 \times 210 - 60 = 129$  赢得竞争。如果节点 3 不参加, 那么节点 2 会赢得竞争, 则应付节点 2 的报酬值为  $210 \times 1.0 - 100 = 110$ 。由此, 如果节点 3 完成传递会得到报酬  $210 - 110 = 100$ ; 如果失败, 则相当于损失 110。因此节点 3 的期望净利润为  $100 \times 0.9 - 110 \times 0.1 - 60 = 19 > 0$ 。如果节点 3 的报价夸大, 假设其真实报价为  $(70, 0.8)$ , 那么此时节点 3 的期望净利润  $100 \times 0.8 - 110 \times 0.2 - 70 = -12$ 。

### 3) 安全性。

目的节点利用节点  $S$  的公钥对收到的信息进行验证, 通过验证式 (4) 是否成立来检查信息是否被篡改:

$$\begin{aligned} e(P, \text{Sig}_S) &= e(P, SK_S H(B \| S \| D \| TS \| TTL \| N_i)) = \\ &= e(P, H(B \| S \| D \| TS \| TTL \| N_i))^{SK_S} = \\ &= e(SK_S P, H(B \| S \| D \| TS \| TTL \| N_i)) = \\ &= e(PK_S, H(B \| S \| D \| TS \| TTL \| N_i)) \quad (4) \end{aligned}$$

由式 (4) 可知, 若任意参数被篡改, 则等式不成立, 节点  $D$  将删除接收的信息。 $D$  只有在确认信息无误的情况下, 才会向中继节点发送 Ack 信息。同时 VB 对接收到的 Ack 进行解密验证, 若有误则删除, 从而进一步确保相应报酬的安全支付。

## 4 性能分析

实验采用仿真工具 The One 1.4.1<sup>[11]</sup>, 该工具适合于对 DTN 网络进行仿真<sup>[12]</sup>, 利用工具里设计的场景对本文所提的方案进行评估。

### 4.1 场景设置

具体场景如表 2 所示。

表 2 仿真场景设置

类别	参数	值
场景特征	仿真时间	12 h
	仿真区域范围	4500 m × 3400 m
	仿真背景城市	Helsinki
节点特征	节点数目	126
	移动速度	0.5 ~ 1.5 m/s
	数据包生存期	5 h
	通信范围半径	10 m
	缓存区大小	5 MB

### 4.2 实验结果分析

在实验结果中, 主要考虑三个参数: 传递成功率、平均延迟和网络开销比率 (overhead\_ratio)。其中网络开销比率计算公式为:

$$\text{overhead\_ratio} = \frac{(\text{relayed} - \text{delivered})}{\text{delivered}} \quad (5)$$

其中: relayed 为实际完成的总转发数, delivered 为成功到达目

的节点包的数目, 因此网络开销比率由包转发总数和包成功到达数二者决定, 转发总数越大, 网络开销比率越大, 成功到达数目越大, 网络开销比率越小。

本实验与三个著名的协议 Epidemic、PROPHET 和 Spray and Wait 进行对比分析, 其中在实现 Spray and Wait 时设置其包的副本数为 2, 即源节点会将一个副本传递给相遇的第一个节点, 然后这两个节点直到遇到目的节点才会进行传递, 转化成一种两跳传递。从图 4 和图 5 可以明显看出, 当自私节点不断增加的情况下, 三种协议的传递成功率大幅下滑, 平均延迟不断增大, 性能受到极大影响。而本文提出的 TIC 协议, 不再盲目地选择中继节点, 而是选择最优的节点作为中继, 并且刺激节点去传递包, 可以看出在自私节点不断增大时, 传递成功率和平均延迟表现平稳。

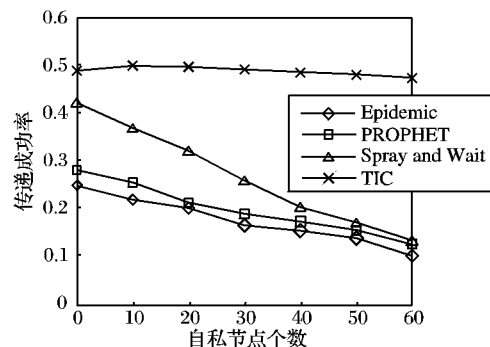


图 4 消息传递成功率

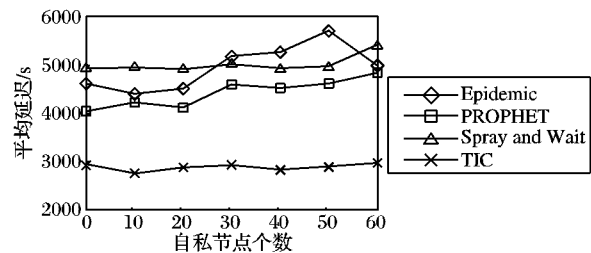


图 5 消息延迟时间

图 6 中 Epidemic 和 PROPHET 的传递次数比较多, 因此网络开销比率较大, 当自私节点数目增多时, 传递次数下降, 传递成功率下降, 相应的网络开销比率也有所下降, 而 Spray and Wait 由于只有两个副本, 当自私节点增加时, 传递出去的副本可能被丢掉, 因此等同于变成直接传递 (Direct Delivery), 网络开销比率最小。TIC 算法转交的消息少, 在网络产生的负担少, 在 DTN 这样的受限环境下, 能节省大量的网络资源。

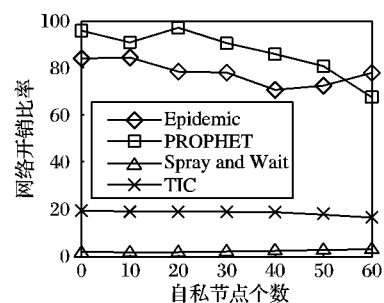


图 6 网络开销比率

## 5 结语

激励相容原理是博弈论中非常具有实用价值的原理, 判断算法是否合理、是否能有效防止自私问题的标准, 在实际系统中有很大的实用价值。本文提出了一种两跳的激励相容路

由协议,以解决 DTN 中因自私节点而导致的消息传递成功率降低、通信性能下降等问题。

通过采用激励机制,给予参与转发的中继节点一定的利益,从而刺激节点来积极参与转发消息,同时在传递的消息中加入认证机制,确保消息的准确性,并且保证参与转发的中继节点能收到源节点给予的利益。最终实验结果表明,TIC 算法能有效地防止节点的自私行为,刺激节点传递消息,并且确保了消息传递的正确率和成功率。

#### 参考文献:

- [1] CROWCROFT J, YONEKI E, HUI P, *et al.* Promoting tolerance for delay tolerant network research[J]. SIGCOMM Computer Communication Review, 2008, 38(5):63-68.
- [2] LINDGREN A, HUI P. The quest for a killer app for opportunistic and delay tolerant networks[C] // Proceedings of the 4th ACM Workshop on Challenged Networks. New York: ACM, 2009: 59-66.
- [3] TOURNOUX P, LOCHIN E, LEGUAY J, *et al.* Robust streaming in delay tolerant networks[C]// Proceedings of the International Communications Conference. Piscataway: IEEE, 2010:1-5.
- [4] SPYROPOULOS T, PSOUNIS K, RAGHAVENDRA C S. Efficient routing in intermittently connected mobile networks: the multiple-copy cast[J]. IEEE/ACM Transactions on Networking, 2008, 16(1):77-90.
- [5] PANAGAKIS A, VAIOS A, STAVRAKAKIS I. On the effects of cooperation in DTNs[C]// Proceedings of the 2nd International

Conference on Communication System Software and Middleware and Workshops COMSWARE. Piscataway: IEEE, 2007:1-6.

- [6] KARALIPOULOS M. Assessing the vulnerability of DTN data relaying schemes to node selfishness[J]. IEEE Communications Letters, 2009, 13(12):923-925.
- [7] LI Y, SU G, WU D, *et al.* The impact of node selfishness on multicasting in delay tolerant networks[J]. IEEE Transactions on Vehicular Technology, 2011, 60(5):2224-2238.
- [8] HE Q, WU D, KHOSLA P. SORI: A secure and objective reputation-based incentive scheme for Ad Hoc networks[C] // Proceedings of Wireless Communications and Networking Conference 2004. Piscataway: IEEE, 2004:825-830.
- [9] ZHU H, LIN X, LU R, *et al.* SMART: A secure multilayer credit-based incentive scheme for delay-tolerant networks[J]. IEEE Transactions on Vehicular Technology, 2009, 58(8):828-836.
- [10] LEE S B, PAN G, PARK J S, *et al.* Secure incentives for commercial ad dissemination in vehicular networks[C] // Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing. New York: ACM, 2007:150-159.
- [11] The ONE 1.4.1[EB/OL]. [2012-06-20]. <http://www.net-lab.kk.fi/tutkimus/dtn/theone/>Tietover-kko laboratorio.
- [12] KERANEN A, OTT J, KARKKAINEN T. The ONE simulator for DTN protocol evaluation[C]// Proceedings of the 2nd International Conference on Simulation Tools and Techniques. New York: ACM, 2009:5674.

(上接第1499页)

两种切换流程与 NBS 方案切换流程的时延对比。从图 8 可以看出,当  $P_f$  分别取值 0.1 和 0.5 时,本文所提方案的切换流程的时延都要优于 NBS 方案,其中快速切换流程时延最小,且随着  $D_p$  和  $P_f$  取值的增大而时延优势愈加明显。

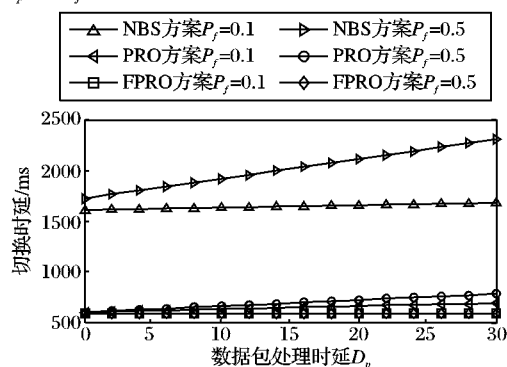


图8 本文方案切换流程与 NBS 方案切换流程时延对比

## 4 结语

随着 NEMO 网络在众多军事及民用领域的快速普及,如何提高 NEMO 网络的可靠性及稳定性逐渐成为研究热点。本文通过分析 NBS 方案以及 PMIPv6 网络协议,在前人研究的基础上,提出了 NEMO 网络在 PMIPv6 中的实现方案及其快速切换流程。方案结合了 NEMO 网络和 PMIPv6 网络的特点,通过减少空中链路信令的数量等方法,显著减少了切换时延。数据分析表明,本文移动网络实现方案的性能要优于 NBS 方案。

#### 参考文献:

- [1] DEVARAPALLI V, WAKIKAWA R, PETRESCU A, *et al.* Network Mobility (NEMO) basic support protocol, IETF RFC 3963

[S]. Fremont: IETF, 2005.

- [2] PERKINS C, JOHNSON D, ARKKO J. Mobility support in IPv6, IETF RFC 6275[S]. Fremont: IETF, 2011.
- [3] GUNDAVELLI S, LEUNG K, DEVARAPALLI V, *et al.* Proxy mobile IPv6, IETF RFC 5213[S]. Fremont: IETF, 2008.
- [4] LEE J H, HAN Y H, GUNDAVELLI S, *et al.* A comparative performance analysis on hierarchical mobile IPv6 and proxy mobile IPv6[J]. Telecommunication Systems, 2009, 41(4):279-292.
- [5] LEE J H, ERNST T, CHUNG T M. Cost analysis of IP mobility management protocols for consumer mobile devices[J]. IEEE Transactions on Consumer Electronics, 2010, 56(2):1010-1017.
- [6] SOLIMAN H, CASTELLUCCIA C, ELMALKI K, *et al.* Hierarchical mobile IPv6 (HMIPv6) mobility management, IETF RFC 5380[S]. Fremont: IETF, 2008.
- [7] KOODLI R. Mobile IPv6 fast handovers[S]. IETF RFC 5568, 2009.
- [8] DROMS R, THUBERT P, DUPONT F. DHCPv6 prefix delegation for Network Mobility (NEMO), IETF RFC 6276[S]. Fremont: IETF, 2011.
- [9] FATHI H, CHAKRABORTY S, PRASAD R. Mobility management for VoIP: evaluation of mobile IP-based protocols[C]// International Conference on Communications. Piscataway: IEEE, 2005:3230-3235.
- [10] GIUSTO D, IERA A, MORABITO G, *et al.* The Internet of things[M]. Berlin: Springer, 2010:102-105.
- [11] NARTEN T, NORDMARK E, SIMPSON W. Neighbor discovery for IP version 6 (IPv6), IETF RFC 2461[S]. Fremont: IETF, 1998.
- [12] YOKOTA H, CHOWDHURY K, KOODLI R. Fast handovers for proxy mobile IPv6[S]. IETF RFC 5949, 2010.
- [13] ATZORI L, IERA A, MORABITO G. The internet of thing: a survey[J]. Computer Networks, 2010, 54(15):2787-2805.