容迟网络中基于社会网络的可靠路由

于海征[1,2]，马建峰[1]，边红[3]

（1. 西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071；
2. 新疆大学 数学与系统科学学院，新疆 乌鲁木齐 830046; 3. 新疆师范大学 数学科学学院，新疆 乌鲁木齐 830054）

摘 要：针对容迟网络中存在较多自私节点的问题，提出了一种基于社会网络的可靠路由方法，以确保消息有效可靠地传递到目的节点。利用社会网络中节点间的关系评估方法，计算出团队间的关系强度矩阵。消息源节点的团队依据关系强度矩阵选择适合的成员节点作为中继节点向目的节点传递消息，避免了网络中自私节点抛弃所转交消息的可能。同时，结合容迟网络间断性连通的特点，在消息转交过程中采用基于身份的密码体制方法，保证了消息转交的安全性。实验表明，所提出的方法在自私节点较多的容迟网络里能保证消息高效、安全地传递到目的节点。

关键词：容迟网络；路由；社会网络；团队

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2010)12-0020-07

Social network-based trustworthy routing in delay tolerant networks

YU Hai-zheng[1,2], MA Jian-feng[1], BIAN Hong[3]

(1. Key Laboratory of Computer Networks and Information Security (Ministry of Education), Xidian University, Xi'an 710071, China;
2. College of Mathematics and System Sciences, Xinjiang University, Urumqi 830046, China;
3. School of Mathematical Sciences, Xinjiang Normal University, Urumqi 830054, China)

Abstract: A trustworthy routing protocol was proposed based on social networks for delay tolerant networks (DTN), which ensured the messages to be sent to the destination node efficiently and reliably against more selfness nodes. With a method of relation evaluation among nodes in social networks, the relation intensity matrix between the groups was figured out. The source node chose proper member nodes as next intermediate node to forward the messages according to the relation intensity matrix, which avoided the messages to be sent to the selfness nodes and reduced the probability of dropping the messages. At the same time, due to intermittent connectivity of DTN, a method of identity-based cryptography was introduced during the process of messages forwarding, it ensured the security of messages forwarding. The experiments show that our method can ensure the security and efficiency of messages to the destination.

Key words: delay tolerant networks; routing; social networks; group

---

收稿日期：2010-05-17；**修回日期**：2010-11-01

基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（2007AA01Z429）；国家自然科学基金资助项目（60702059, 60872041, 60963624, 11061035）

Foundation Items: The National High Technology Research and Development Program of China (863 Program) (2007AA01Z429); The National Natural Science Foundation of China (60702059, 60872041, 60963624, 11061035)

1 引言

容迟网络(DTN, delay tolerant networks)[1, 2]具有间断性连通的特性，所使用的路由协议与其他无线网络有很多的差异。由于节点的稀疏性或者节点的移动性，在 DTN 中很难维持端到端的连通。消息从源节点传递到目的节点，通常需要中继节点的存储、运载和转交才能完成消息的传送。近年来，提出的很多路由协议[3~6]都是要求中继节点必须无条件转交所接到的消息。无论转交的消息是否与自己相关，中继节点必须存储、运载和转交。Epidemic[3] 路由是基于泛洪传递的协议，当节点相遇时，相互交换消息，直到消息被传递到目的节点，大量的消息冗余消耗了大量的网络资源。Spray and wait [4]路由协议提出每条消息产生固定的副本数量，网络中的副本数量被控制，一定程度上减少了冗余的消息。PROPHET[5]是一种概率转交路由协议，利用节点相遇和转交的历史经验来增强传递的性能。MaxProp[6]路由协议依据历史数据，结合数据包转交到其他节点的列表和放弃转交的节点列表的顺序，确定下一跳转交节点的优先次序。

但是，在挑战环境中，节点的资源有限，如能量、存储和带宽受限，许多节点为了自身的利益很有可能放弃转交过来的与自己无关的消息。在现实社会里，大部分节点都具有自私的特性，对于那些没有利益关系的消息可能不愿意去转交，不接收或者接收后扔掉[7, 8]。PeopeNet[7]协议利用社会网络架构了一个无线虚拟社会网络，用来模仿人类搜索信息的方式，使用具体地理位置上的基础设施传递查询给利益相关的用户，与用户相邻的节点通过对等链接通信直到发现一个匹配的查询。文献[8]提出了借助人类移动和局部/全局连通在移动用户设备之间传输数据的方法，实验测试了人的移动模式，发现在同一个社区里的用户交流较为活跃。

针对网络中存在自私节点，一些激励机制被提出[9,10], 用来刺激自私节点转交消息。事实上，自私节点不是不愿意转交消息，而是通常愿意帮助与自己有关系的节点(亲属、好友和同事等)。文献[9]提出一个防欺骗基于信用的系统，在自私节点中对合作和诚实报告行为动态给予奖励。文献[10]提出了一种分布式自适应信誉机制，避免了节点被错误地当作自私节点而遭到报复，从而快速恢复合作关系。根据社会关系的强弱，自私节点根据意愿选择转交的顺序，文献[11]提出感知社会自私性的路由算法，依据节点的转交意愿和接触机会选择下一个转交节点。文献[12]在车辆网络中提出了一种基于社会关系的隐私保护消息转交协议，根据节点的社会等级信息，设置路侧基站 (RSU, roadside unit)具有较高的社会等级，更大程度上提供了临时存储空间同时协助转交消息，从而获得更高的传递率。但是，如果网络中存在较多的自私节点，消息就很难被传递到目的节点。

为了避免把消息转交给自私节点，本文提出一种基于社会网络的可靠路由方法，克服了网络存在较多自私节点的问题。利用源节点和目的节点的社会团队来传递数据。源节点通过自己的社会关系建立了一个自己可以信赖的团队，团队中的节点保证所接收的消息安全可靠地转交出去。同样的，目的节点也有自己一个可信赖的团队，消息只要经过团队中的任一节点都会保证最终传递到目的节点。一个节点的团队成员会尽其所能为自己服务，当消息源节点需要传递消息到目的节点时，源节点考察其每个成员对目的节点整个团队的关系强度，计算并获得关系强度矩阵，选择合适的成员节点转交消息。负责转交消息的节点携带消息传递到目的节点所在团队的成员节点，最后目的节点的团队成员节点转交消息到目的节点。

针对容迟网络中消息转交的安全性，文献[13]总结了 DTN 安全状况，并指出对 DTN 的主要威胁是消息篡改、未授权使用 DTN 的稀缺资源和拒绝服务攻击。文献[14]给出了一种合理的 DTN 安全设计选择方案，把 IPSec 类型安全报头增加到消息(另称为 bundles)里提供不同的安全服务。文献[15,16]提出利用基于身份的密码体制(IBC, identity-based cryptography)[17]解决容迟网络中的一些安全问题。文献[18]提出了一种基于 IBC 的匿名认证协议和安全架构，提高了消息的安全通信。为了保证节点间消息的安全传递，防止私有消息内容被泄露，结合容迟网络的间断性连通的特点，本文也采用了基于身份的密码体制(IBC)的安全机制，在网络连通性较低的情况下，提高消息的保密性，确保消息安全可靠地传递到目的节点，并且降低了服务器端的工作负载。

在本文所提出的方法中，关系强度的评估是建立在源节点成员到目的节点的整个团队的基础上，一个源节点团队的成员可能和目的节点的团队中多个成员有联系，由此得出关系强度团队间的评估，

而在其他文献中只考虑节点间的关系评估研究。

本文结构安排如下，第2节给出了可靠路由的基本原理、社会关系评估及安全考虑，第3节对所提出的方法进行了性能分析与比较，第4节是结束语。

2 可靠路由机制

2.1 基本原理

当一条消息由一个节点（源节点）产生，需要传递消息到目的节点时，如果不能直接传递到目的节点，就需要中间的一些节点利用自身的移动和存储帮助源节点转交消息。但是，在实际网络中并不是所有的节点都愿意转交消息。由于DTN网络中资源受限，很多的节点为了自身相关的通信需求，而保留存储空间、带宽和能量等资源，便于将来的消息传递。在社会网络中，节点间的消息转交依靠它们之间的社会关系，如果2个节点间不存在社会关系，或者关系很差，很显然2个节点相互之间不愿意为对方提供转交服务。

本文所提出的路由方案是依据社会网络中社会关系所建立的社会团队来选择负责消息转交的下一跳节点。如图1所示，消息源节点 S 生成消息 msg，需要传递到目的节点 D，如果 S 不能直接转交到 D，则需要通过一些中间节点。为了消息能安全可靠地传递到目的节点，依赖自身的社会团队（图1中的虚线内），源节点 S 首先在自己的团队成员中寻找合适的中继节点 S_i，转交消息（图1中的步骤1）。节点 S_i 携带着消息 msg，通过移动，遇见目的节点 D 的团队成员 D_j，转交消息（图1中的步骤2）。D_j 通过自己和 D 的社会关系，转交消息到 D（图1中的步骤3）。如果 S_i 直接遇见的是目的节点 D，递交成功，不需要步骤3。虚线外的节点是与源节点团队及目的节点团队不相关的节点，也就是说，这些节点和2个团队的社会关系很弱，或者是没有关系的节点，这些节点中往往包含有自私节点，甚至有一些恶意节点，不能当作中继节点来转交消息。

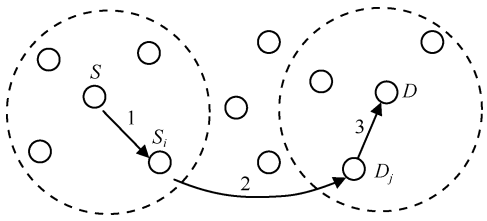

图1 消息传递方式

消息转交的具体过程如算法1，消息源节点 S 的团队 $\hat{S}=\{S_i \mid 1\leqslant i\leqslant m\}$，不失一般性，$\hat{S}$ 包含源节点 S，源节点被记为 S_1，同样的，目的节点 D 的团队 $\hat{D}=\{D_j \mid 1\leqslant j\leqslant n\}$ 也包含 D，记为 D_1（此记号为了在下一节社会关系强度评估中便于计算和分析）。针对一条消息，源节点 S 的团队中与目的节点 D 的团队相关的节点集合记为 S_D，从中 S 选择合适的中继节点转交消息。

在算法1中，提到了根据关系强度来选择合适的转交节点，关系强度的具体计算见下一节。由于DTN网络的特点，本文采用多副本的路由方式，所以在选择转交节点的时候，多个节点充当消息的中继节点。当源节点的团队无法转交时，将会求助于相邻的其他团队，相邻团队的转交过程和源节点方式一致。

算法1 消息转交策略

消息 msg 的源节点 S 询问自身的团队所有成员 $\hat{S}$，收集能传递 msg 到目的节点 D 的团队 $\hat{D}$ 的节点集合 S_D；

if $S_D\neq\phi$

比较集合 S_D 中节点与 S 和 D 的关系强度 $T_{S\to S_i}$ 和 $T_{S_i\to D}$，选择关系强度较大的节点作为消息 msg 的转交节点；

else

自身团队中没有合适的选择，S 寻找相邻的团队核心节点 A，发送请求，A 询问自身的团队成员 $\hat{A}=\{A_i\}$，收集能传递 msg 到目的节点 D 及 D 的团队成员的节点集合 A_D；

if $A_D\neq\phi$

源节点 S 转交 msg 给 A，A 比较 A_D 中 $T_{A\to A_i}$ 和 $T_{A_i\to D}$，选择关系强度较大的节点作为消息 msg 的转交节点；

else

S 寻找其他相邻的团队核心节点，直到找到合适的转交节点为止。

2.2 社会关系评估

源节点必须评估对所有的成员节点的关系强度，而且还要考察成员节点对目的节点团队的关系强度，从而具体确定消息转交的中继节点。

根据算法1，在选择转交节点时，要先考虑节点之间的关系强度，由于节点间的关系是不对称的，因此得到如图2所示的加权有向社会图，消息源节点 S 的社会团队成员为 $\{S_i \mid 1\leqslant i\leqslant m\}$，目的节点 D 的社

会团队成员为$\{D_j \mid 1 \leqslant j \leqslant n\}$，$S$ 对其成员 S_i 的关系值为 p_i，设 $p^{\mathrm{T}}=(p_1,\cdots,p_i,\cdots,p_m)$，为节点 S 对所有成员的关系向量。设 $q^{\mathrm{T}}=(q_1,\cdots,q_j,\cdots,q_n)$，为 D 的社会团队成员对 D 的关系向量。注：这里所指节点间的关系可表达为相遇概率、信任程度及优先转交级别等，或者是这几个量的组合。

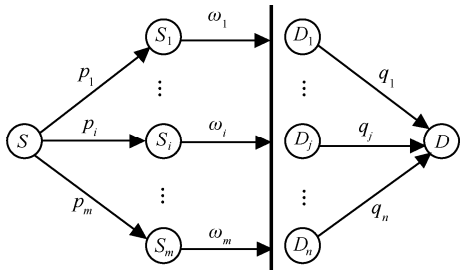

图 2　加权有向社会图

算法 1 中提到转交时要考虑节点 S 的社会团队成员 $S_i(1 \leqslant i \leqslant m)$ 对 D 的团队的关系强度（包括对自身的评估，S_1 为源节点），在图 2 中，ω_i 表示节点 S_i 对 D 的所有成员的关系评估，记为 $\omega_i=(\omega_{i1},\cdots,\omega_{ij},\cdots,\omega_{in})$，$\omega_{ij}$ 表示节点 S_i 对节点 D_j 的关系评估。此时，得到 S 的所有成员节点对 D 的所有成员节点的关系评估矩阵为 $\boldsymbol{W}_{m\times n}$：

$$\boldsymbol{W}=\begin{bmatrix} \omega_{11} & \cdots & \omega_{1j} & \cdots & \omega_{1n} \\ \vdots & \ddots & \vdots & & \vdots \\ \omega_{i1} & \cdots & \omega_{ij} & \cdots & \omega_{in} \\ \vdots & & \vdots & \ddots & \vdots \\ \omega_{m1} & \cdots & \omega_{mj} & \cdots & \omega_{mn} \end{bmatrix}$$

为了便于计算，把向量 $\boldsymbol{p}$ 扩充为对角矩阵 $\boldsymbol{P}$：

$$\boldsymbol{p}=\begin{bmatrix} p_1 \\ \vdots \\ p_i \\ \vdots \\ p_m \end{bmatrix} \rightarrow \boldsymbol{P}=\begin{bmatrix} p_1 & & & & \\ & \ddots & & & \\ & & p_i & & \\ & & & \ddots & \\ & & & & p_m \end{bmatrix}$$

通过计算得到节点 S 关于关系强度的转交向量 $\boldsymbol{T}$，$\boldsymbol{T}^{\mathrm{T}}=[T_1,\cdots,T_i,\cdots,T_m]$，其中：

$$\boldsymbol{T}=\boldsymbol{PWq}=\begin{bmatrix} p_1 & & & & \\ & \ddots & & & \\ & & p_i & & \\ & & & \ddots & \\ & & & & p_m \end{bmatrix}\cdot \begin{bmatrix} \omega_{11} & \cdots & \omega_{1j} & \cdots & \omega_{1n} \\ \vdots & \ddots & \vdots & & \vdots \\ \omega_{i1} & \cdots & \omega_{ij} & \cdots & \omega_{in} \\ \vdots & & \vdots & \ddots & \vdots \\ \omega_{m1} & \cdots & \omega_{mj} & \cdots & \omega_{mn} \end{bmatrix}\begin{bmatrix} q_1 \\ \vdots \\ q_j \\ \vdots \\ q_m \end{bmatrix}$$

$$=\begin{bmatrix} \sum_{j=1}^{n} p_1\omega_{1j}q_j \\ \vdots \\ \sum_{j=1}^{n} p_i\omega_{ij}q_j \\ \vdots \\ \sum_{j=1}^{n} p_m\omega_{mj}q_j \end{bmatrix}$$

比较向量 T 的分量，选择分量值不小于 T_1，也就是关系强度要优于源节点的所有成员节点作为转交节点，S_I 为转交节点集合：

$$S_I=\{S_i \mid i \in I\},\ I=\{i \mid T_i \geqslant T_1,\ 1 \leqslant i \leqslant m\}$$

注：若考虑单副本路由转交方式，则选择最大的关系强度 $\max\limits_{1\leqslant i\leqslant m}(T_i)$ 所对应的节点 S_i 作为转交节点。

2.3　消息安全性考虑

2.3.1　基于身份的密码体制的使用

在 DTN 网络中，由于间断性连通的特性，所采用的安全机制有其独特的地方[13~16, 18]。为了提高转交过程中消息的保密性，根据容迟网络的特点，基于身份的密码体制(IBC, identity-based cryptography)[17]被采用。DTN 网络中端到端的路径常常不存在，实时得到私钥生成中心(PKG, private key generator)提供的私钥是不现实的，因此，采用 IBC 的方法可以使得消息接收者在收到消息之前就可以获得 PKG 生成的私钥，如图 3 中的步骤 5 和步骤 6，可以先于其他步骤进行。为了表述和理解的方便，这里用 *Alice* 和 *Bob* 分别表示消息的源节点 S 和目的节点 D，

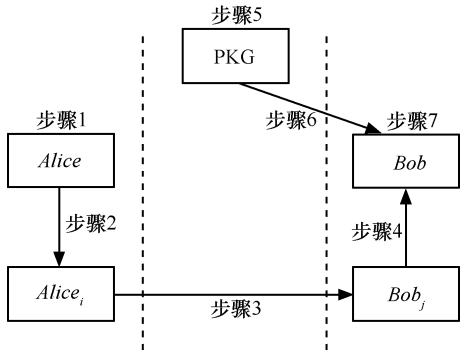

图 3　基于 IBC 的安全机制

$Alice_i$ 和 Bob_j 分别表示其所在团队的成员。步骤 2 是源节点对其成员的传递，步骤 4 是目的节点成员对目的节点的传递，步骤 3 是不同团队的成员之间的传递。

密钥生成中心 PKG 的公私钥对 $(P_{\mathrm{PKG}}, S_{\mathrm{PKG}})$，*Alice* 和 *Bob* 的 ID 分别为 id_{Alice} 和 id_{Bob}（公钥字符串）。

1) *Alice* 计算消息 *msg* 的散列值：$Hash(msg) \to h$；从密钥生成中心 PKG 得到私钥 s_{Alice}，$G(P_{\mathrm{PKG}}, S_{\mathrm{PKG}}, id_{Alice}) \to s_{Alice}$；对 h 签名：$Sign(P_{\mathrm{PKG}}, s_{Alice}, h) \to sig$；利用对称密钥 sk_{AB}，对称加密 $E(sk_{AB}, msg, sig) \to c$（密文）；基于身份的非对称加密 $E_{\mathrm{IBC}}(P_{\mathrm{PKG}}, id_{Bob}, sk_{AB}) \to t$（信封）。

2) *Alice* 发送密文 c 和信封 t 到 *Alice* 的团队成员 $Alice_i$。

3) $Alice_i$ 遇见消息目的节点 *Bob* 的团队成员 Bob_j，转交密文 c 和信封 t 给 Bob_j。

4) Bob_j 转交密文 c 和信封 t 到目的节点 *Bob*。

5) 密钥生成中心 PKG 生成 *Bob* 的 IBC 私钥 s_{Bob}，$G(P_{\mathrm{PKG}}, S_{\mathrm{PKG}}, id_{Bob}) \to s_{Bob}$，对称加密 $E(sk_{PB}, s_{Bob}) \to t'$。

6) PKG 传递 t' 到目的节点 *Bob*。

7) 对称解密 $D(sk_{PB}, t') \to s_{Bob}$；基于身份的非对称解密 $D_{\mathrm{IBC}}(s_{Bob}, t) \to sk_{AB}$；对称解密 $D(sk_{AB}, msg, sig) \to msg, sig$；验证 *Alice* 的签名 $D_{\mathrm{IBC}}(P_{\mathrm{PKG}}, id_{Alice}, sig) \to h$，比较 $Hash(msg)$ 和 h。

利用对称密码对所传递的消息进行加密和解密，利用 IBC 非对称密码把对称密钥加密封装成电子信封 t，保证了对称密钥的安全传输，同时减少了加解密的运算工作量。

2.3.2 基于身份的密码体制与基于 PKI 的密码体制比较

基于身份的密码体制与基于 PKI(public key infrastructure)的密码体制都是公钥密码体制，IBC 中 PKG 的充当者和 PKI 中的 CA(certification authority)也可以是一样的。但是在 DTN 网络环境下，IBC 方法的优点主要表现在 2 个方面：一是对消息接收方的网络连接性有较低的要求；二是合理地降低了 PKG 服务器的工作负载。如果采用 PKI 的方法，*Bob* 接收到 *Alice* 的加密消息和电子信封后无法解密，必须把电子信封发送到密钥服务器，密钥服务器解密后重新封装再发送给 *Bob*，此时，*Bob* 解开信封，获得对称密钥并且解密消息。这种情况下需要密钥服务器到 *Bob* 一个来回的通信，对这两者之间的连接有较高的要求。但是在 IBC 方法中，如图 3 中的步骤 6，IBC 方法只需要从 PKG 到 *Bob* 的一次通信，而且此次通信可以先于步骤 1、步骤 2、步骤 3、步骤 4，对于 DTN 网络这种机会性连接的特征，IBC 方法比较适合。

在相同的 DTN 环境下比较了 IBC 方法和 PKI 方法在三方的计算量。假设类似 *Alice* 的发送方有 m 个，类似 *Bob* 的接收方有 n 个。对于发送方来说，平均每个发送方分别发送 r_1 个消息到 n_1 个接收方；对于接收方来说，平均每个接收方收到 r_2 个消息。得到的计算量见表 1。

表 1 计算量比较

工作方	IBC 方法	PKI 方法
Alice	IBC 加密次数 r_1n_1， 对称加密次数 r_1	公钥加密次数 r_1， 对称加密次数 r_1
Bob	IBC 解密次数 r_2， 对称解密次数 r_2+1	对称解密次数 $2r_2$
Server	IBC 密钥生成次数 n， 对称加密次数 n	私钥解密次数 mr_1， 对称加密次数 mr_1n_1

对于 PKI 方法，在服务器端的计算量较大，但是对于 IBC 方法发送方也需要较多的工作。一般来说 IBC 方法相比于 PKI 方法并没有绝对的优势，但是在 DTN 这种机会转交的环境里，使用 IBC 的方法更能适应间断性连通的特性，降低服务器的负载，提高消息的保密性。

3 性能分析

实验采用仿真工具 The ONE 1.4.0[19]，是一种适合于 DTN 网络的机会网络环境仿真工具[20]，利用工具里设计的场景针对本文所提的路由方案进行评估。采用真实城市街区图，126 个节点，2 种速度，一种是步行速度：0.5~1.5m/s；另一种是汽车速度：3~10m/s。节点间的通信范围半径为 10m。消息源节点和目的节点的团队成员数均为 20。节点缓存区大小为 5MB。

如果不考虑节点的缓存受限制，Epidemic 路由递交率最高。这是因为 Epidemic 路由采用的是泛洪式转交方法，复制消息并转交给所遇到的所有节点，中间节点若不存在自私节点的问题，负责转交的中继节点能及时把消息转交给下一个中继节点，最大程度上传递消息，所以消息递交率最高且延迟

最小。但是 Epidemic 路由产生了大量的冗余副本，牺牲了大量的存储、带宽和能量等网络资源。PROPHET 路由是基于转交概率而选择下一跳的中继节点，因此消息副本数量有所控制，负责转交的节点减少，延迟有所增大。但是，图 4 中 Epidemic 路由递交率低于 PROPHET 路由，这是因为节点缓存区有限制，过多的消息副本会导致缓存区没有空间，删除较早的消息，或者消息排队导致没有及时转交，消息延迟增加，如图 5 所示。在 DTN 这种资源受限的网络环境中，消耗过多的资源很大程度上会影响消息的传递。本文所提出的基于社会团队的路由，如图 4 和图 5 中的 Group，由于消息传递的中继节点在消息所在的社会团队中，因此递交率和延迟都比较平稳，在自私节点不多的情况下，效果不是很好，但在自私节点逐渐增多的情况下能够保持平稳的递交率和延迟，优于 Epidemic 和 PROPHET 路由。

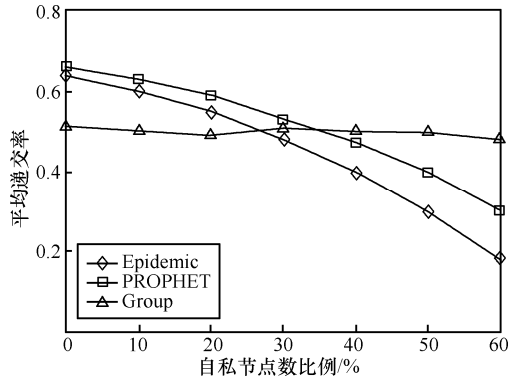

图 4　消息成功传递率

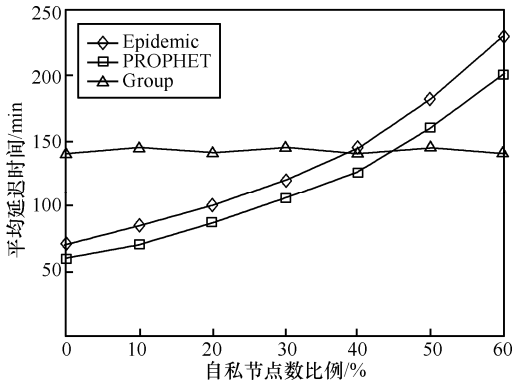

图 5　消息延迟时间

在图 6 中比较了 3 种路由方法产生的消息冗余数，在自私节点占 20%的情况下，Epidemic 路由在网络中产生的消息随时间增加而迅速增加，对节点的存储和能量产生巨大负担。而 Group 方法用于转交的消息很少，不宜对网络产生负担，尤其在 DTN 网络资源有限的环境下，能节省大量的资源。

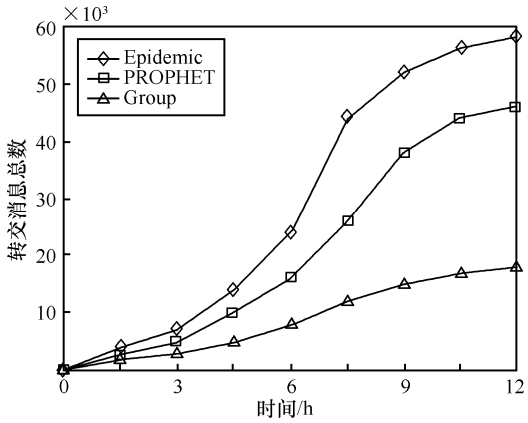

图 6　消息冗余数

4　结束语

本文提出了一种基于社会网络的容迟网络路由方案，解决了网络中存在较多自私节点而导致消息无法传递的问题。利用社会网络中节点间的关系评估方法，得到源节点团队到目的节点团队的社会关系强度矩阵，比较关系强度的大小确定转交消息的节点，能够保证消息有效可靠地传递到目的节点，避免了自私节点抛弃转交消息的情况。同时，结合容迟网络间断性连通的特点，在节点转交消息过程中采用基于身份的密码体制方法，确保转交的消息安全高效地传递到目的节点。虽然在自私节点较少的情况下，本文所提的方法效果不太理想，但是在自私节点较多的情况下，相比较其他的算法优势明显。

参考文献：

[1] FALL K. A delay-tolerant network architecture for challenged internets[A]. Proceedings of ACM SIGCOMM[C]. Karlsruhe, Germany, 2003.27-34.

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

[3] VAHDAT A, BECKER D. Epidemic Routing for Partially Connected Ad Hoc Networks[R]. Technical Report CS-200006. Duke University, 2000.

[4] SPYROPOULOS T, PSOUNIS K, RAGHAVENDRA C S. Spray and wait: an efficient routing scheme for intermittently connected mobile networks[A]. Proceedings of ACM SIGCOMM Workshop on Delay-tolerant Networking[C]. Philadelphia, New York, 2005. 252-259.

[5] LINDGREN A, DORIA A, SCHELEN O. Probabilistic routing in intermittently connected networks[J]. Lecture Notes in Computer Sci-

ence, 2004, 3126: 239-254.

[6] BURGESS J, GALLAGHER B, JENSEN D, *et al*. MaxProp: routing for vehicle-based disruption tolerant networks[A]. Proceedings of IEEE INFOCOM[C].Barcelona, Spain, 2006.1-11.

[7] MOTANI M, SRINIVASAN V, NUGGEHALLI P. PeopleNet: engineering a wireless virtual social network[A]. Proceedings of MobiCom[C]. Cologne, Germany, 2005. 243-257.

[8] HUI P, CHAINTREAU A, SCOTT J, *et al*. Pocket switched networks and human mobility in conference environments[A]. Proceedings of SIGCOMM[C]. Philadelphia, USA, 2005. 244-251.

[9] ZHONG S, CHEN J, YANG Y R. Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks[A]. Proceedings of IEEE INFOCOM[C]. San Francisco, USA, 2003. 1987-1997.

[10] JARAMILLO J J, SRIKANT R. Darwin: distributed and adaptive reputation mechanism for wireless ad-hoc networks[A]. Proceedings of MobiCom[C]. Montreal, Canada, 2007. 87-98.

[11] LI Q, ZHU S, CAO G. Routing in socially selfish delay tolerant networks[A]. Proceedings of INFOCOM 2010[C]. San Diego, USA, 2010. 857-865.

[12] LU R, LIN X, SHEN X. SPRING: a social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks[A]. Proceedings of INFOCOM 2010[C]. San Diego, USA, 2010. 632-640.

[13] FARRELL S, CAHILL V. Security considerations in space and delay tolerant networks[A]. Proceedings of the 2nd IEEE International Conference on Space Mission Challenges for Information Technology[C]. Pasadena, USA, 2006. 29-38.

[14] SYMINGTON S, FARRELL S, WEISS H. Bundle Security Protocol Specification[S]. IRTF, DTN Research Group, 2010.

[15] ASOKAN N, KOSTIAINEN K, GINZBOORG P, *et al*. Towards Securing Disruption-tolerant Networking[R]. NRC-TR-2007-007, Nokia Research Center, 2007.

[16] ASOKAN N, KOSTIAINEN K, GINZBOORG P. Applicability of identity-based cryptography for disruption-tolerant networking[A]. Proceedings of the 1st International MobiSys Workshop on Mobile Opportunistic Networking (MobiOpp 07)[C]. San Juan, Puerto Rico, 2007. 52-56.

[17] SHAMIR A. Identity-based cryptosystems and signature schemes[A]. Proceedings of CRYPTO[C]. Santa Barbara, USA, 1984. 47-53.

[18] KATE A, ZAVERUCHA G, HENGARTNER U. Anonymity and security in delay tolerant networks[A]. Proceedings of 3rd International Conference on Security and Privacy in Communication Networks (SecureComm 2007)[C]. Nice, France, 2007. 504-513.

[19] The ONE 1.4.0[EB/OL]. http://www.netlab.tkk.fi/tutkimus/dtn/theone/. Nokia Research Center (Finland), 2010.

[20] KER NEN A, OTT J, K RKK INEN T. The ONE simulator for DTN protocol evaluation[A]. Proceedings of the 2nd International Conference on Simulation Tools and Techniques (Simutools09)[C]. Rome, Italy, 2009. 1-10.

作者简介：

于海征（1976-），男，新疆哈密人，西安电子科技大学博士生，主要研究方向为移动网络、无线网络安全等。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为网络与信息安全、密码学等。

边红（1976-），女，新疆奎屯人，博士，新疆师范大学副教授，主要研究方向为图论与网络优化等。