

一种用于信息隐蔽传输的高效 DTN 路由算法

刘美华¹, 田茂¹, 陈小莉¹, 张新晨^{2†}

(1. 武汉大学 电子信息学院, 湖北 武汉 430072;
2. 华中师范大学 物理科学与技术学院, 湖北 武汉 430079)

摘要:作为一种间歇性连接的网络,延迟容忍网络(DTN)中的消息通过节点间的机会性相遇完成投递,这种多跳、随机的传递方式使得消息难以被追踪,因此 DTN 非常适合实现信息的隐蔽传输.然而在 DTN 中节点之间的连接频繁断开限制了传输效率,且现有的 DTN 路由并未针对隐蔽传输的安全性进行相关研究.为保证隐蔽传输的通信质量和安全性,提出一种路由算法,首先利用节点的静态社会特征和实时相遇情况设计一种高效的转发策略以提高消息的投递效率;其次考虑到过多的消息副本在增加投递概率的同时也会增加暴露的风险,根据网络连通情况对副本数进行了动态设置.最后,将提出的算法与 DTN 经典算法进行仿真对比,结果显示本算法能够提高 DTN 的消息投递率,减少网络开销,同时提高消息的安全性.

关键词:延迟容忍网络;传输隐藏;路由算法;副本数控制;转发策略

中图分类号: TN915

文献标志码: A

An Efficient DTN Routing Algorithm for Covert Transmission of Information

LIU Meihua¹, TIAN Mao¹, CHEN Xiaoli¹, ZHANG Xinchen^{2†}

(1. Electronic Information School, Wuhan University, Wuhan 430072, China;
2. School of Physical Science and Technology, Central China Normal University, Wuhan 430079, China)

Abstract: The Delay Tolerant Network (DTN), as an intermittently connected network, transfers messages through opportunistic encounters between nodes. It is difficult to intercept messages because of the multi-hop and random delivery method, which shows that DTN is very suitable for covert transmission of information. However, it also limits transmission efficiency. In order to develop transmission efficiency and to guarantee the security of covert transmission, a routing algorithm was proposed. Firstly, an efficient message forwarding strategy was designed to improve the delivery efficiency of messages by utilizing the static social characteristics and real-time encounters of nodes. Secondly, because massive copies of message lead to high probability of delivery but also reduce the security of covert transmission, the number of copies was dynamically set according to the topology of the network. Finally, the proposed algorithm was simulated. Compared with the classical DTN algorithm, the simulating results show that the proposed algorithm can improve the message delivery rate of DTN, reduce network overhead, and increase the security of messages.

Key words: Delay Tolerant Network (DTN); transmission hiding; routing algorithm; control of message copies; forwarding strategy

* 收稿日期:2018-09-05

基金项目:国家自然科学基金资助项目(61661028), National Natural Science Foundation of China(61661028)

作者简介:刘美华(1989—),女,湖北荆州人,武汉大学博士研究生

† 通讯联系人, E-mail: zxc9501@hotmail.com

在延迟容忍网络(Delay Tolerant Network, DTN)中,移动设备之间以自组织的形式通过短距离接口进行数据交换,这种低成本的通信方式与蜂窝系统互补协同,成为物联网领域的一个重要方向^[1-2]。但由于设备的移动导致连接时常断开,消息只能通过节点间的机会性相遇以存储-携带-转发的方式实现投递^[3]。这种多跳、随机的方式与传统网络通信有着本质差异,DTN 中移动节点之间自组织、间歇性的连接使消息传输路径的随机性很大,通信过程很难追溯,因而使消息难以被追踪,因此 DTN 能够用于信息隐藏系统中对消息的传输过程进行保护。信息隐藏系统通常可以分为内容隐藏和传输隐藏,内容隐藏技术包括数字水印、密码学、隐写术^[4]等;传输隐藏主要是利用信道的一些固有特性以实现传输的隐蔽,例如扩频、跳频等^[5],与这些物理层的传输隐藏方法不同,本文提出一种基于 DTN 的从网络层面实现隐蔽传输的方法,其与内容隐藏一起构建信息隐藏系统:经加密或者隐写之后得到的载密信息通过 DTN 进行多跳传输,由于传输路径的不确定性,消息和源节点均难以被追踪,这样就能够实现对传输过程和发送方的保护。

尽管 DTN 能用于信息隐藏,但其间断,随机的特征决定了其在消息投递率和延时可控等可靠性上得不到保障,导致 DTN 难以成为实用的传输信道。针对这个问题,学者们基于“存储-携带-转发”机制提出了许多优化路由协议来提高传输质量^[6],主要分为两种策略,第一种通过消息多副本来得到较好的投递率,比如 Epidemic^[7]以洪泛的方式来转发数据,然而过多的消息副本数增加了网络开销和暴露的风险,影响通信的隐蔽性,因此必须控制副本数量;Spray and Wait^[8]限制副本数为一个定值以提升整体效率,但固定的副本数不能适应网络拓扑结构的变化。文献[9]指出网络连通度能很大程度上决定消息的投递,并提出一种根据网络连通度来动态调整消息副本数的 DA-SW 路由,但是需要提前获取网络历史数据集的分析结果作为参考,不能适用于所有 DTN 网络,因此需要制定一种能够根据实时的网络连通程度来自适应设置消息副本数的方法。

第二种策略通过评估节点的投递效用,为消息选择合适的下一跳使其以更高的概率到达目的节点,比如 Prophet 通过相遇频率来估计再次相遇的概率,选择与目的节点相遇概率高的邻居节点作为下一跳^[10],但忽略了节点的社会性。近年来,许多研究证明合理地利用网络的社会特征可以对消息的转

发效率起到比较显著的提升作用^[11],Bubble Rap, SimBet 等社会路由利用节点的社区性、相似性和中心性来评估节点的转发效用^[12-13]。以二者为代表的大多社会性路由都致力于挖掘节点的潜在社会关系,而忽略了节点与目的节点的直接联系,使得消息中继节点的选择不够精确,因此,在制定中继选择策略时,不仅要考虑社会特征,还需要考虑中继节点与目的节点的直接联系。

针对这些问题,本文提出一种安全高效的路由策略 ER-IHS (Efficient Routing of DTN for Information Hiding Systems),首先考虑到消息副本过多会影响隐蔽传输的安全性,提出用消息的投递时延来评估与量化网络的连通程度,以此来自适应设置消息副本数,兼顾传输质量和隐蔽性;然后提出一种转发效用评估方法,兼顾节点社会特征以及它与目的节点的直接联系,来选择中继节点。在仿真时,采用 DTN 传输效率指标和提出的安全性指标来评估本路由的性能^[14],同时提出安全性指标来评估本路由。仿真对比结果表明该算法可以在保证较高的传输效率的同时取得较好的安全性。

1 信息隐藏系统结构与问题描述

1.1 系统结构

本文选择那些表现出一定的社会功能的容忍延迟网络作为新型信息隐藏应用的信道。信息隐藏系统的结构如图 1 所示,首先对原始消息进行加密或隐写处理,然后在 DTN 的间歇性连接的环境下以多跳的方式传递加密信息,当接收方收到消息时对数据进行解密。由于节点的相遇具有很大的随机性,很难追溯消息的传输路径;由于事先经过高效的密码术或隐写等内容加密技术的处理,即使消息经过多个节点,仍然难以暴露,因此消息、发送者和传输过程都得以“隐藏”。

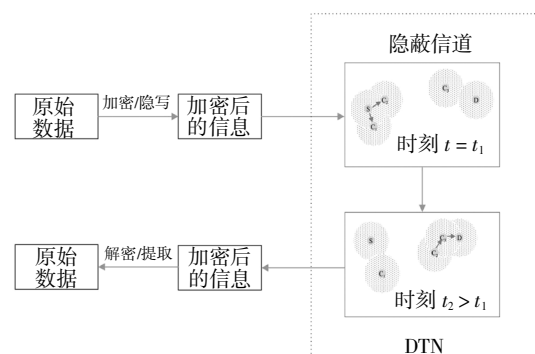


图 1 信息隐藏系统的结构

Fig.1 Block diagram of the system

1.2 问题描述

本文在设计用于信息隐藏系统的 DTN 路由算法时,主要面临下面几个问题:

1)在网络拓扑结构变化的情况下,消息副本数既要保证较高的投递率又要降低信息暴露的风险,就必须实时检测网络连通情况,以此对副本数进行动态的设置,因此单个节点如何估计全局的连通程度,以及如何通过估计的连通程度计算副本数,是需要解决的重要问题.

2)如何在充分利用潜在的社会关系基础上结合与目的节点之间的直接联系来设计投递效用函数,为消息选择最优的载体节点决定着路由的优劣.

2 基于节点社会特征的路由算法 ER-IHS

为了提高 DTN 用于隐蔽传输时的通信质量,本文的 ER-IHS (Efficient Routing for Information Hiding Systems)路由算法在消息多副本的基础上,采用一种消息转发策略,该策略提出一种节点投递效用值的计算方法以更精确地选择下一跳.同时考虑到过多的副本带来的安全性隐患,ER-IHS 对网络的连通程度进行评估与量化,并以此动态设置消息的复制上限,从而在保证消息投递效率的基础上提高安全性.以下将对本算法进行详细阐述.

2.1 相关定义

2.1.1 网络连通程度的评估

整个网络的连通程度取决于网络拓扑结构,且在很大程度上决定了消息成功投递的概率及投递时延^[9],对于单个节点来说,最容易获取的关于网络全局连通程度的信息是当该节点作为目的节点时,成功接收到消息所花费的时延,所以这个时延可以用来反映网络的连通状况,使节点做出更优的决策.本文以节点记录的投递时延来量化网络整体的连通程度,记为 T_{link} .每个节点先在本节点计算 T_{link} ,然后再与邻居节点交互统一更新.计算时以常数 T_{interval} 作为步长量化时间,初始条件为,当某节点没有接收到任何以之为目的节点的消息时, T_{link} 被设置为 ∞ ,一旦接收到第一条消息, $T_{\text{link}} = \text{TTL}_i - \text{RTTL}_i$.第 k 个时刻的 T_{link} 以下面的公式进行计算更新.

1)当前时刻 k ,节点成功接收以之为目的节点的消息时, T_{link} 以式(1)进行更新.

$$T_{\text{link}}(k) = T_{\text{delay}_j} \times \alpha + T_{\text{link}}(k-1) \times (1-\alpha) \quad (1)$$

$$T_{\text{delay}_j} = \text{TTL}_i - \text{RTTL}_i \quad (2)$$

式中: i 表示消息序号; TTL_i 表示消息的生命期; RTTL_i 表示第 i 条消息的剩余生命期; T_{delay_j} 表示第 j 条消息的投递时延.式(1)是利用投递时延来衡量网络的连通程度,计算时考虑数据的时效性,为最新的投递时延附上较大权值 α ,通常在 $(0,1)$ 中取一个较大的值.

2)节点接收完消息之后, T_{link} 以式(3)进行更新.

$$T_{\text{link}}(k) = T_{\text{link}}(l) \times \gamma^n \quad (3)$$

$$n = \frac{k-l}{T_{\text{interval}}} \quad (4)$$

式中: l 表示最近一次接收以该节点为目的节点的消息的时刻; γ 为老化因子, $0 < \gamma < 1$; n 表示 l 时刻到当前时刻的时间步数.式(3)表明,如果该节点长时间不能接收到消息 T_{link} 应该变大,以表示连通状况变差.

3)当前时刻 k ,两个节点 a 与 b 相遇,相互获取彼此的 T_{link} 值(T_{link_a} 和 T_{link_b}) 和 l 值(l_a 和 l_b),然后以统一后的 T_{link} 值替换原来的值.

$$T_{\text{link}}(k) = \frac{k-l}{2k-(l_a+l_b)} \times T_{\text{link}_a}(k-1) + \frac{k-l_b}{2k-(l_a+l_b)} \times T_{\text{link}_b}(k-1) \quad (5)$$

式中: l_a, l_b 分别表示节点 a, b 记录的 l 值.式(5)表示当两节点相遇计算统一的 T_{link} 值时,同样考虑数据的时效性, l 较大的节点应该分配更大的权重.

2.1.2 节点的转发效用值-转发活跃度的计算

节点的社会关系很大程度上决定节点之间的相遇情况,在社交网络中越活跃的节点遇到其他节点的概率越高,因此为消息选择中继节点时,考虑节点的社会特征能够提升消息的投递效率.但是如果只考虑这种整体的活跃性是不够的,因为活跃节点与目的节点的相遇概率不一定很高.针对这个问题,本文同时考虑节点的活跃度和与目的节点的相遇情况,提出转发活跃度的概念来评估节点的投递效用值.

如式(6)所示,本文以节点遇到的其他节点总个数而不是总次数来衡量该节点的活跃度 Activity,因为现实的社交网络中很可能存在与固定的少数节点相遇频繁的节点,这些节点不应被赋予高的活跃度.

$$\text{Activity}_i = \sum_{j=i}^* j \quad (6)$$

式中: j 表示到目前为止与节点 i 有过接触的节点.节点 i 与目的节点 d 的接触概率 P_{id} 按式(7)进行计算.

$$P_{id} = \frac{N_{id}}{N_i^*} \quad (7)$$

式中: N_{id} 表示到目前为止节点*i*与目的节点*d*的相遇次数; N_i^* 表示到目前为止节点*i*与其他节点相遇的总次数.

根据以上两个因素,本文以式(8)定义节点的转发活跃度 Forward_activity.

$$\text{Forward_activity}_i = (1 - e^{-\text{Activity}_i}) \times P_{id} \quad (8)$$

2.2 消息副本数的动态控制

在网络拓扑结构变化的情况下,消息副本数既要保证较高的投递率又要降低信息暴露的风险,就必须实时检测网络连通情况,以此对副本数进行动态设置,以兼顾传输质量和安全性.当生成某条消息时,其源节点根据其估计的网络当前整体连通程度来设置消息的副本数*L*,计算方法见式(9).

$$L = \frac{T_{\text{link}}(k)}{T_{\text{meet_int}}(k)} \quad (9)$$

式中:*k*表示当前时刻,即该条消息生成的时刻; $T_{\text{link}}(k)$ 为生成消息的源节点所估计的当前网络连通程度; $T_{\text{meet_int}}(k)$ 表示与其他节点相遇的平均间隔,也是由本节点进行局部性的估计,并在节点相遇时进行更新统一.更新方法为取均值,如式(10)所示.

$$T_{\text{meet_int}}(k) = \frac{T_{\text{meet_int}_a}(k) + T_{\text{meet_int}_b}(k)}{2} \quad (10)$$

当两节点*a*和*b*相遇时,两个节点的 T_{meet} 更新值是对两节点的本地估计值 $T_{\text{meet_int}_a}$ 和 $T_{\text{meet_int}_b}$ 取均值得到.

2.3 基于社区特征的下一跳选择策略

本文在对网络进行社区划分的基础上,利用节点的活跃度和接触频率来评估邻居节点的消息投递能力,为消息找到合适的下一跳.结合 Bubble Rap 中的社区划分方法^[14]和 2.1 节中所述的转发活跃度 Forward_activity,提出本地转发活跃度和全局转发活跃度的概念.本地转发活跃度是只计算同社区节点相遇情况得到的转发活跃度;而全局转发活跃度是按照整个网络的相遇情况来计算转发活跃度.当邻居节点为非目的节点时,选择下一跳的流程如图 2 所示,主要可以分为 4 种情况.

情况 1:载体节点*a*,邻居节点*b*均与目的节点*d*在同一社区,如果*b*的本地转发活跃度大于*a*的本地转发活跃度则*a*将消息转发给*b*,转发后*a*将剩余副本数减去 1;如果*b*的本地转发活跃度小于*a*,则*a*不转发消息.

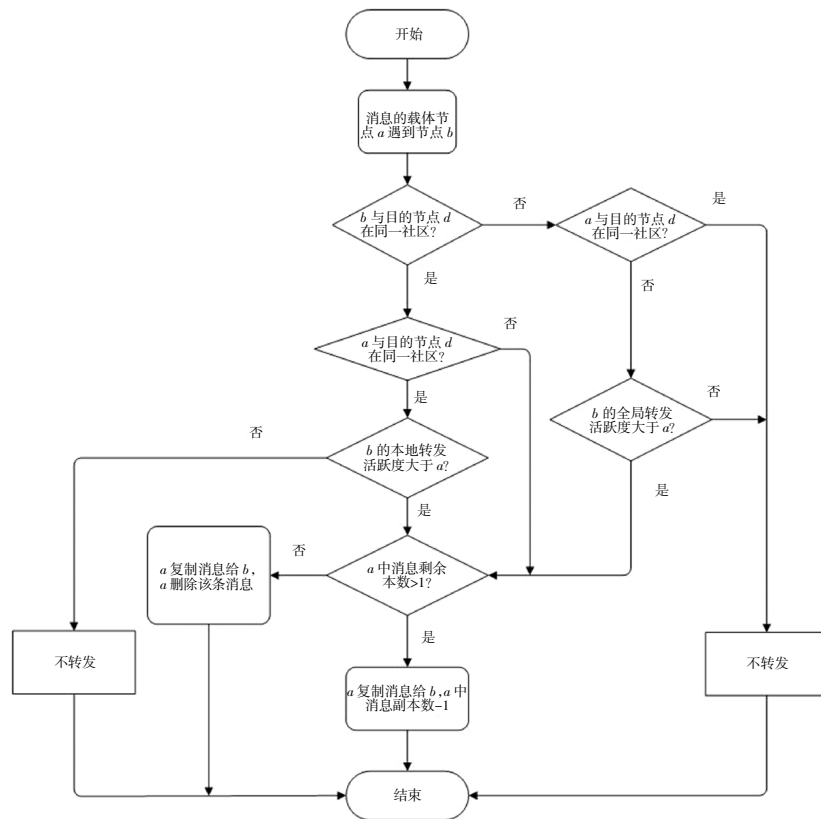


图 2 下一跳选择策略流程图

Fig.2 Flowchart of message forwarding mechanism

情况 2: 载体节点 a 与目的节点 d 不在同一社区, 而邻居节点 b 与 d 在同一社区, 则 a 直接将消息转发给 b , 同样转发后 a 将剩余副本数减去 1.

情况 3: 载体节点 a 与目的节点 d 在同一社区而邻居节点 b 与 d 不在同一社区, 则 a 不转发消息.

情况 4: 载体节点 a , 邻居节点 b 均不与目的节点 d 在同一社区, 此时如果 b 的全局转发活跃度大于 a 的全局转发活跃度, 则 a 将消息转发给 b , 如果 b 的全局转发活跃度小于 a 的全局转发活跃度则 a 不转发消息.

3 仿真结果与分析

3.1 参数设置与性能指标

为了评估所提出的路由算法 ER-IHS 的性能, 本文用真实数据集在 The ONE (Opportunistic Networks Environment) 平台上对其进行仿真, 与 4 种经典算法 (Bubble Rap, SimBet, Epidemic, Prophet) 的仿真结果进行对比, 然后对提出的副本数动态设置方法以及基于转发活跃度的中继选择方法的贡献进行了验证. 仿真参数为: 外部数据集采用 Infocom06; 每条消息间隔 300 s 到 600 s 随机产生, 消息大小在 100 kB 到 300 kB 之间, 其源节点和目的节点随机选择, TTL 设置为 720 min; 每个节点的缓存大小设置为 5 MB, 通信接口的传输速度为 250 kbps.

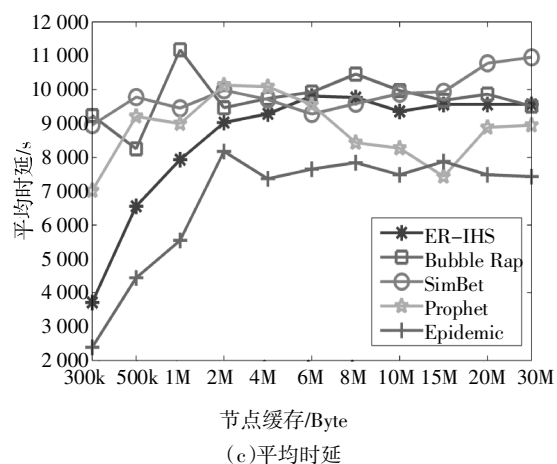
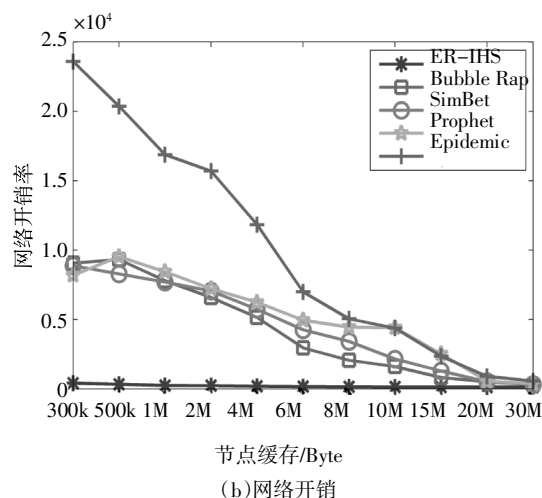
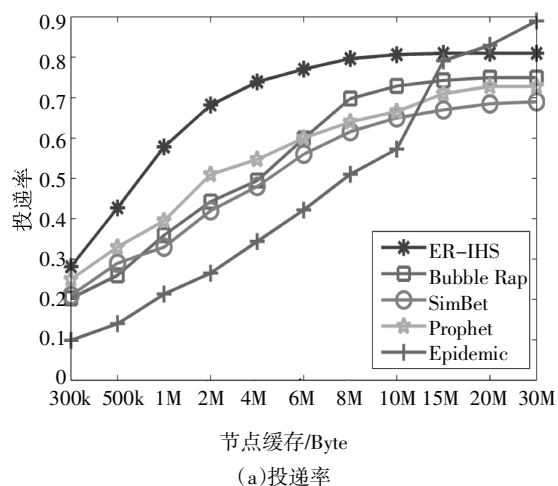
在性能指标上, 主要考虑隐蔽传输的传输效率和安全性: 传输效率指标采用广泛使用的消息投递率, 网络开销和平均投递延时; 在安全性指标上, 由于本文所提出的隐蔽传输方法与传统的物理层隐蔽传输方法有本质区别, 因此本文考虑提出新的指标来衡量算法安全性. 考虑到多副本策略会影响消息成功投递后在网络中残留的平均副本数, 增加消息暴露的风险, 因此本文提出以消息遗留的平均副本数为衡量路由安全性的指标.

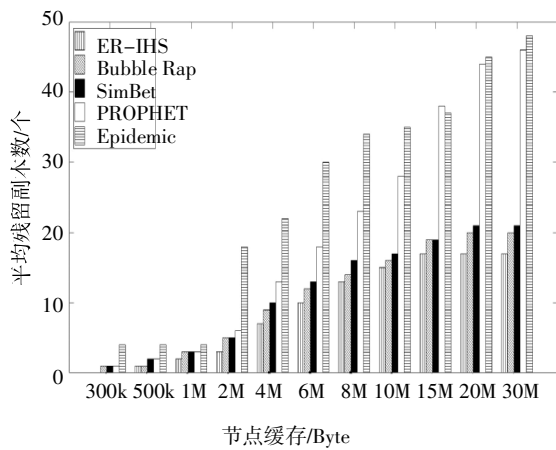
3.2 ER-IHS 路由的性能

本文将 ER-IHS 路由与两种基于节点社会特征的路由 Bubble Rap 和 SimBet, 以及 2 种经典路由 Epidemic, Prophet 进行了对比, 改变节点缓存的大小, 得到的结果如图 3 所示.

在传输效率上, 由图 3(a) 可以看到除 Epidemic 之外, 各路由的投递率随着缓存的增大逐渐增大, 最后趋于稳定. 总体而言本算法 ER-IHS 的投递率比 SimBet, Prophet, Bubble Rap 三种路由都要高, 当缓存为 2 M 时 ER-IHS 投递率比 Bubble Rap 高 54%,

比 SimBet 高 62%, 比 Prophet 高 34%. 图 3(b) 显示各路由的网络开销随着缓存的增大而减小最后趋于稳定, 其中 Epidemic 的开销最大, ER-IHS 的开销最小, 当缓存为 15 M 时 ER-IHS 的开销分别是 Bubble Rap 的 15%, SimBet 的 10%, Prophet 的 5%. 图 3(c) 显示 ER-IHS 的平均投递延时处于中等水平, 当缓存为 20 M 时, ER-IHS 的平均时延比 Bubble Rap 高 3%, 比 SimBet 低 11%, 比 Prophet 高 7%, 而当节点的缓存偏小时, ER-IHS 则表现出明显的优势.





(d)平均残留副本数

图 3 所有路由的性能比较
Fig.3 Comparisons of 5 algorithms

出现以上结果的原因可以归结于:

首先,ER-IHS 路由根据网络的连通状况动态调整消息的副本数量,减少不必要的消息复制,节省了网络资源;选择下一跳时 Bubble Rap 和 SimBet 仅利用了节点的社会关系,Prophet 仅利用了节点与目的节点的相遇概率,而 ER-IHS 将两个因素综合考虑,能够更精确有效地选择下一跳,因此得到更高的投递率。

第二,由于 Epidemic 通过消息大量复制和转发的方式牺牲缓存资源来提升投递率,因此开销是最高的,其余算法均设置了中继节点选择策略,能够减少总消息转发次数,因此网络开销显著低于 Epidemic,在此基础上 ER-IHS 对消息的副本数进行控制,又进一步使网络开销降低。

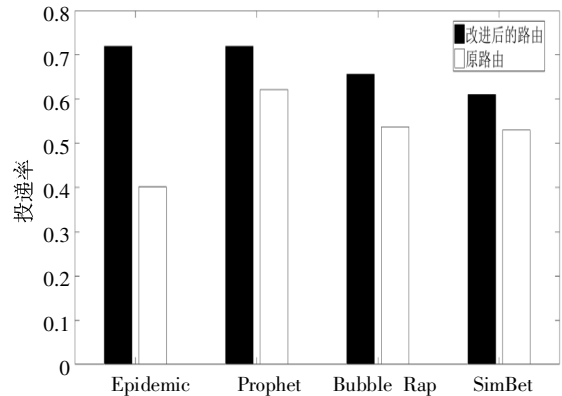
第三,与 Epidemic 相比,ER-IHS 和其他三种路由均对消息的转发设置了条件,使得消息在网络中的平均副本数变少,而 ER-IHS 除了设置了较严格的转发条件之外还对副本数进行了控制,导致消息的投递时延略微增加,但是整体上仍与 Bubble Rap 和 SimBet 的平均时延相近.总的来说,ER-IHS 路由以增加少量的投递时延为代价,获取较高的投递率和较低的网络开销。

在安全性上,图 3(d)显示各个路由的平均残留副本数随着节点缓存的增大而增加,其中 Epidemic 和 Prophet 的增幅明显,另三种增幅较少,其中 ER-IHS 的平均残留副本数最低.当节点缓存为 6 M 时, Bubble Rap 的平均残留副本比 ER-IHS 多 20%, SimBet 比 ER-IHS 多 30%,Prophet 比 ER-IHS 多

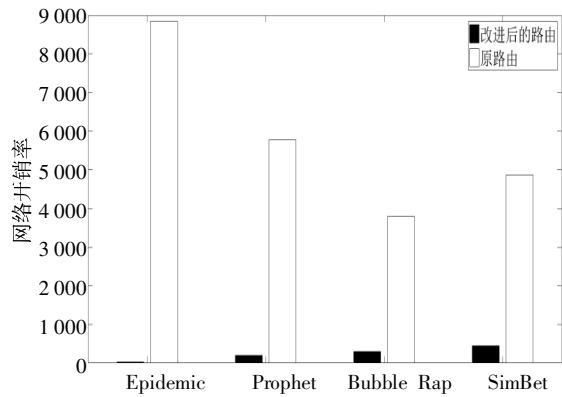
80%,Epidemic 比 ER-IHS 多 200%. 主要原因在于 ER-IHS 对消息副本数自适应设置,因此网络中的残留副本数得到显著降低,减少了消息暴露的风险。

3.3 消息副本数 L 的动态控制方法的性能

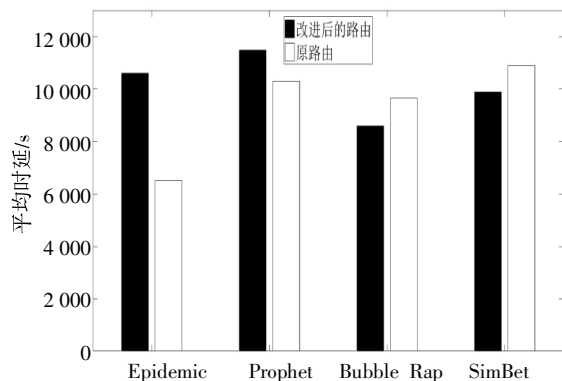
消息副本数的动态控制方法旨在提高消息安全性,为了检测该方法对传输质量是否造成了负面影响,本文将其在 4 种副本复制没有上限的经典路由 Epidemic,Prophet,Bubble Rap,SimBet 上,将传输效率和安全性与原路由进行比较.在本文配置的参数下的结果如图 4 所示,为方便比较,将改进后路由与改进前的差值列出,如表 1 所示,“+”表示增加,“-”表示减少。



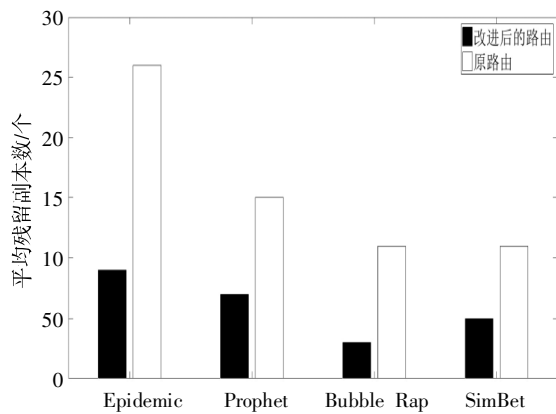
(a)投递率



(b)网络开销



(c)平均时延



(d)平均残留副本数

图4 消息副本数的动态设置方法的性能

Fig.4 Performance of the dynamic setting of copies

表1 结合了动态控制副本数方法的路由性能比较

Tab.1 Performance comparison of routing algorithms with dynamic control to message copies

	投递率/%	网络开销/%	平均时延/%	残留副本/%
Epidemic	+78.6	-99.7	+62.6	-65.4
Prophet	+15.7	-96.5	+10.3	-53.3
Bubble Rap	+22.3	-92.2	-11.1	-72.8
SimBet	+15.1	-91	-9.3	-54.5

在传输效率上,结合了本文的动态控制副本数方法的路由的投递率均得到提高,网络开销得到大幅降低,在投递时延上改进的 Epidemic 和 Prophet 比原路由均有所提高,而基于社会特征的 Bubble Rap 和 SimBet 则比原路由的时延要略低.在安全性上,改进后的路由的平均残留副本数均显著减少.

由以上结果可以看到,本文的动态控制消息副本数的方法能够在保证传输质量的基础上提高消息的传输安全性,对于那些对消息冗余依赖程度较高的路由,虽然增加了一定的消息平均时延,但总体而言改善了传输效率和传输安全.

3.4 转发活跃度的性能

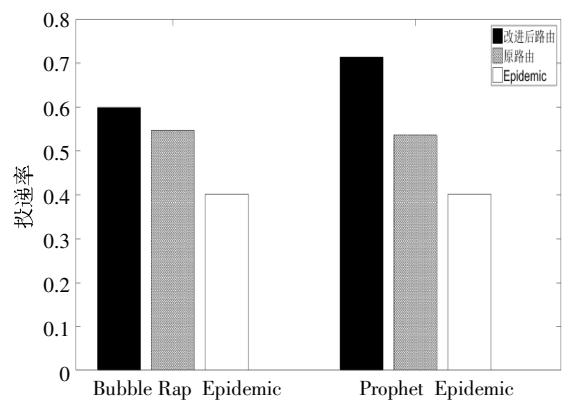
本文考察提出的基于转发活跃度 Forward_activity 的中继节点选择策略对消息投递率,网络开销和平均投递时延的影响.将其应用于同样考虑了社区性和节点活跃程度(中心性)的 Bubble Rap 和利用节点与目的节点之间相遇的概率来选择中继节点的 Prophet,得到 Bubble Rap_FA(以转发活跃度代替中心性)和 Prophet_FA(以转发活跃度代替相遇概率)与原始路由相比较,同时以 Epidemic 的结果作为参考.图5展示了比较结果.为了便于观察,将改进后路由与改进前的差值列出,如表2所示.

表2 结合了动态控制 TTL 方法的路由性能比较

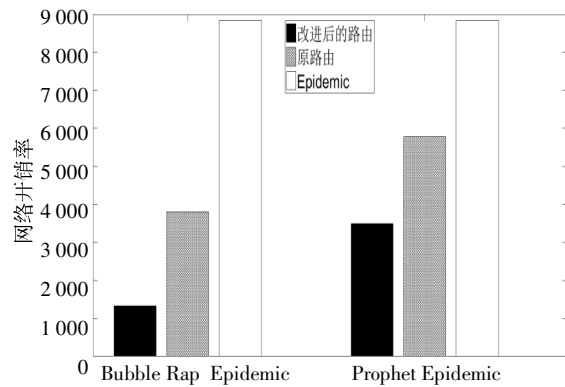
Tab.2 Performance comparison of routing algorithms with dynamic control to message TTL

路由	投递率/%	网络开销/%	平均时延/%
Prophet	+33	-39.4	-9.8
Bubble Rap	+9.3	-65.2	-17

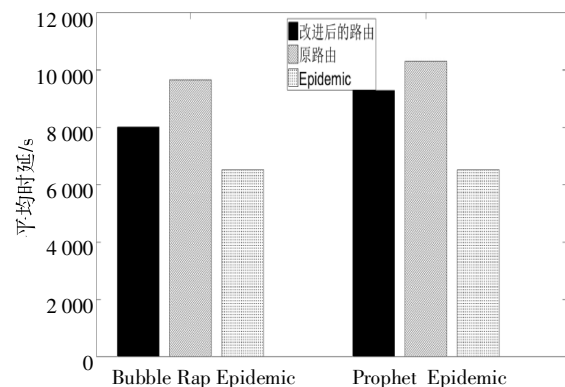
由图5可以看到,基于转发活跃度的路由与原路由相比,提高了消息投递率,降低了网络开销和平均投递时延.这是由于转发活跃度能够更加精确地评估节点的投递效用,从而能够提高消息传输效率.



(a)投递率



(b)网络开销



(c)平均时延

图5 结合了转发活跃度因子的路由性能

Fig.5 Performance of the forwarding mechanism

4 结 论

本文利用 DTN 的多跳随机的传输特点将其用作信息隐藏系统中的隐蔽信道,为了应对 DTN 间歇性连接的不利特性,提出了一种有效的路由策略以提高 DTN 的通信质量,并降低消息暴露风险.该路由提出一种检测网络连通度的方法以动态设置消息的副本数,并利用节点的静态社会特征和实时的相遇信息来评估节点投递效用,选择合适的中继节点.在仿真实验中,本文对提出的路由的传输效率和安全性做出评估和比较,并分别验证了动态设置消息副本和中继选择策略的性能.仿真结果表明,提出的路由算法能提高消息投递率,降低平均延迟和网络开销,并可以减少消息成功投递后在网络中残留的副本数,因此本文的路由能在 DTN 中获得较好的传输质量和安全性,对将 DTN 理论应用于实际信息隐藏系统具有指导意义.

参考文献

- [1] 姚宏,白长敏,胡成玉,等.移动数据分流研究综述[J].计算机科学,2014,41(S2):182—186.
YAO H,BAI C M,HU C Y,*et al.* Survey on mobile data offloading [J]. Computer Science,2014,41(S2):182—186. (In Chinese)
- [2] 中国信息通信研究院.物联网白皮书 [EB/OL]. [2016-12-01]. http://www.caict.ac.cn/kxyj/qwfb/lbps/201612/t20161228_2185496.htm.
China Academy of Telecommunication Research of MIIT. White Paper of IoT[EB/OL].[2016-12-01].
- [3] PENTLAND A,FLETCHER R,HASSON A. DakNet: Rethinking connectivity in developing nations [J]. Computer,2004,37(1):78—83.
- [4] 白迪,田茂,陈小莉,等.基于图像信息熵的随机数可视化表达[J].湖南大学学报(自然科学版),2017,44(4):139—146.
BAI D,TIAN M,CHEN X L,*et al.* Image-entropy-based visual expression of random [J]. Journal of Hunan University (Natural Sciences),2017,44(4):139—146. (In Chinese)
- [5] SODERI S,MUCCHI L,HÄMÄLÄINEN M,*et al.* Physical layer security based on spread spectrum watermarking and jamming receiver [J]. Transactions on Emerging Telecommunications Technologies,2016,28(12):1—13.
- [6] MOTA V F S,CUNHA F D,MACEDO D F,*et al.* Protocols, mobility models and tools in opportunistic networks: A survey [J]. Computer Communications,2014,48(8):5—19.
- [7] VAHDAT A,BECKER D. Epidemic routing for partially-connected Ad Hoc networks[R]. Duke University,2000.
- [8] SPYROPOULOS T,PSOUNIS K,RAGHAVENDRA C S. Spray and wait: an efficient routing scheme for intermittently connected mobile networks [C]// ACM SIGCOMM Workshop on Delay-Tolerant NETWORKING. ACM,2005:252—259.
- [9] TOURNOUX P U,LEGUAY J,BENBADIS F,*et al.* The accordion phenomenon: Analysis, characterization, and impact on DTN routing [C]// INFOCOM. IEEE,2009:1116—1124.
- [10] LINDGREN A,DORIA A,SCHELÉN O. Probabilistic routing in intermittently connected networks [J]. Acm Sigmobile Mobile Computing & Communications Review,2004,7(3):19—20.
- [11] WEI K,LIANG X,XU K. A survey of social-aware routing protocols in delay tolerant networks: Applications, taxonomy and design-related issues [J]. IEEE Communications Surveys & Tutorials,2014,16(1):556—578.
- [12] PAN H,CROWCROFT J,YONEKI E. BUBBLE rap: Social-based forwarding in delay-tolerant networks [J]. IEEE Transactions on Mobile Computing,2011,10(11):1576—1589.
- [13] DALY E M,HAAHR M. Social network analysis for routing in disconnected delay-tolerant MANETs [C]// Acm International Symposium on Mobile Ad Hoc Networking & Computing. 2007:32—40.
- [14] PAN H,YONEKI E,SHU Y C,*et al.* Distributed community detection in delay tolerant networks [C]// MobiArch'07, ACM, 2007:1—8.