

# 一种基于链路质量的移动 Ad-hoc 网络地理路由算法

洪蕾 黄波 赵春霞

(南京理工大学计算机科学与技术学院 南京 210094)

**摘要** 如何实现简单的路由机制,使节点能够快速、高效地完成分组传递,是移动 Ad-hoc 网络研究的一个基本问题。针对无线链路在高误码率和抗干扰技术方面的不足,提出了将链路质量作为路由选择的度量,设计并实现了基于链路质量的地理路由算法 LQPR,解决了在非理想无线链路上采用传统贪婪算法引起数据分组传送率下降的问题。该算法综合了链路质量选择模式和边界选择模式,并利用目标定位技术获取的地理位置信息指导分组的转发,以减少控制开销,优化路径选择,实现数据分组快速有效的传输。在 NS-2 中完整实现了 LQPR 协议的仿真,并通过对网络节点发送数据包的端到端时延、吞吐量以及包传送率进行比较、评估和检测,验证了 LQPR 路由协议的有效性。

**关键词** 移动 Ad-hoc 网络,链路质量,地理位置路由,分组传送率

**中图分类号** TP393 **文献标识码** A

## Geographic Routing Algorithm Based on Link Quality in Mobile Ad-hoc Networks

HONG Lei HUANG Bo ZHAO Chun-xia

(School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China)

**Abstract** How to implement the simple routing mechanism enables nodes transfer the packets efficiently within a shorter time is a basic problem in research of the mobile Ad-hoc networks. According to the deficiencies of high bit-error rates and anti-interference technique, link quality was proposed as the new metric for route selection and a geographic routing algorithm based on link quality called LQPR was designed and implemented in this paper which solves the problem of a downward trend of packet delivery ratio on Non-ideal wireless link by using traditional greedy algorithm. The LQPR algorithm, which combines the LQ mode and Perimeter mode, guides data forwarding by use of the geographic information obtained by the location techniques, which has such advantages as less control overhead, optimal path selection and efficient transmission. The proposed routing protocol LQPR was simulated by NS-2. Through evaluating and comparing the result in term of average end-to-end delay, aggregate throughput and delivery success rate, the validation of LQPR was then carried out with simulating data.

**Keywords** Mobile Ad-hoc network, Link quality, Geographic routing algorithm, Packet delivery ratio

## 1 引言

移动 Ad-hoc 网络(Mobile Ad-hoc Network, MANET)是一种不依赖于基础设施,完全由无线连接的移动节点构建而成的多跳移动网络,其适用于动态配置的通信环境,具有广阔诱人的应用前景。

路由选择问题是目前移动 Ad-hoc 网络研究的核心问题。传统的无线网络路由协议按照路由建立和维护方式的不同分为表驱动路由(如 DSDV<sup>[1]</sup>)和按需路由(如 AODV<sup>[2]</sup>、DSR<sup>[3]</sup>)。DSDV 以路由表为基础,通过存储到任一目的节点的最佳邻节点信息来建立路由,与网络需求无关,因此,表驱动路由又称为主动式(Proactive)路由协议。特别地,在 DSDV 路由协议中,路由表内的每条记录同时包含了目的节点序列号,以解决 Bellman-Ford 选择的环路问题。AODV 协议

使用距离向量技术,当源节点需要通信时才以 on-demand 的方式建立路由和维护当前有用路由,故又将其称作反应式(Reactive)路由协议。但是表驱动路由和按需路由都不能很好地适用于拓扑变化频繁的移动 Ad-hoc 网络环境。主要原因有两方面:一方面这些协议采取周期性广播或是全网洪泛(flooding)初始化路由,因此产生大量业务开销;另一主要方面是路由建立和维护过程对拓扑和链路质量变化的收敛速率比较慢。

随着导航和移动目标定位技术的发展,对移动目标进行实时有效的定位、指挥、通信等能够弥补传统网络基础设施的不足。为了将定位所提供的地理位置信息添加到路由协议当中,使得移动 Ad-hoc 网络节点在获取局部拓扑信息和资源有限的情况下实现简单快速高效的路由机制,许多研究者已经提出了多种基于地理位置的路由协议(如 DRE-AM<sup>[4]</sup>,

到稿日期:2010-11-15 返修日期:2011-02-23 本文受国家自然科学基金(60705020),东南大学计算机网络和信息集成教育部重点实验室开放研究基金(K93-9-2010-11)资助。

洪蕾(1984-),女,研究生,主要研究方向为无线网络路由协议,E-mail:honglei314@yahoo.com.cn;黄波(1980-),男,硕士生导师;赵春霞(1964-),女,教授。

GLS<sup>[5]</sup>等),它们只需提供局部地理位置信息,不需要维护全局的拓扑结构,从而具有较好的可扩展性和对无线移动 Ad-hoc 网络更好的适应性。

DREAM 是较早提出的地理路由协议,它使用限制性泛洪搜索绕过空洞进行导航,缺点在于如何寻找一个合适的搜索范围;LEACH<sup>[6]</sup>协议选择最小代价(能量或距离)的邻居作为下一跳节点,节点需要通过发送大量的数据包递归更新代价。SPAN<sup>[7]</sup>节点通过选择“休眠”方式关闭冗余节点来提高系统寿命,这在基本维护底层网络连接上增加了一定的通信开销。相比之下,由 Brad Karp 等提出的贪婪的周边无状态路由协议(Greedy perimeter stateless routing, GPSR)<sup>[8]</sup>采用 Perimeter forwarding (周边转发)模式,较好地解决了局部优化问题,提供了有保证的单路径分组转发,是本文基于链路质量的周边路由算法 LQPR 的研究基础。

同时,考虑到移动 Ad-hoc 网络的性能往往受到无线链路上发送冲突、易受干扰等方面的影响<sup>[9]</sup>,传统的基于链路质量稳定假设的路由算法在链路质量剧烈变动的环境中性能会很差。链路质量的不确定性使得路由协议在选路时处于两难的境地。如果能充分估计链路质量的变化,将大大改进上层路由协议的选路机制,从而能在更短的时间内选择一条更有效的链路,完成与网内其它节点之间的通信。

根据移动 Ad-hoc 网的特点,综合以上关于地理路由和链路质量的考虑,本文提出了基于链路质量的周边路由算法 LQPR(Link Quality aware Perimeter Routing)。算法在对链路质量评估改善节点间通信质量的同时,利用 GPSR 中边界转发模式解决局部优化问题。各个节点只需要知道其通信半径内邻节点的地理位置信息和与邻接链路的链路质量指示值 LQI<sup>[10]</sup>,就可执行基于链路质量的 LQ 路由模式和边界路由选择模式,根据邻居节点的定位选择下一跳转发数据分组,直至到达目的节点位置为止。在整个数据传输中,节点不需要建立和维护路由信息表,也不需要路由更新,路由建立仅需要利用位置信息通过单跳邻节点拓扑信息就可以完成,而且算法易于实现,提高了传输路径的鲁棒性。

## 2 基于地理位置的路由

地理位置路由(即 GEO 路由)<sup>[11]</sup>是随着移动定位技术发展形成的一种路由策略。地理路由基本包括两个阶段,一是位置服务;二是分组转发。位置服务(Location service)并不是简单的指定位,而是将节点的 ID 与其当前的地理位置信息进行映射。分组转发策略是指节点向目的节点发送数据时如何选择下一跳,将数据发送给邻近一跳邻居节点再由其转发,最后到达目的节点。

GPSR 协议是由哈佛大学的 Brad Karp 和 H. T. Kung 提出的。该协议结合了贪婪转发与边界转发的优点,算法简单、高效且易于实现。与常规路由协议不同的是,运行此协议的移动节点不需要保存整个网络的拓扑,从而大大降低了对节点存储空间的要求,因此该协议是目前使用最广泛的基于地理位置的路由协议之一。

GPSR 总是尽可能地使用贪婪的转发策略,除非到达局部极值点。在理想环境下,当前节点( $s$ )采用传统的最远转发 MFR(Most Forward Within R)<sup>[12]</sup>,试图选择目的节点( $d$ )方向上最远的邻节点( $m$ )作为下一跳,目的是将转发跳数减到

最少。然而在非理想环境下,传统的基于链路质量稳定假设的路由算法在链路质量剧烈变动的环境中性能会很差。比如无线链路传输信号的衰减遵循  $1/d^n$  的滚降特性<sup>[13]</sup>( $d$  为发送天线和接收天线间的距离)。此时  $m$  位于  $s$  传输半径的边缘,链路( $m, s$ )质量较不稳定,MAC 层通常采用重传机制减少丢包带来的损失,分组传输的成功率大大降低。基于以上分析,本文在贪婪转发的基础上进行拓展和延伸,旨在设计一种既考虑到链路质量,又能减少转发跳数的地理路由算法 LQPR。

为了便于研究,本文根据图理论建立数学模型。移动 Ad-hoc 网络可抽象地表示为连通图  $G(V, E)$ 。其中,  $V$  为网络节点的集合,  $E$  为节点间链路的集合。节点  $u \in V$  的传输半径均为  $R$ 。节点  $u$  通过发送信标(Hello 消息)与邻节点交换信息建立本地拓扑,得到可达邻近节点的集合  $N(u)$ 。

## 3 一种基于链路质量的地理路由 LQPR

### 3.1 链路质量对分组传递的影响

通常评价链路的链路质量方法是计算该链路分组传递成功的概率<sup>[14]</sup>。在一个滑动时间窗口期间(10s)内,所有节点追踪收到来自每个邻节点的探询包。假设前向和反向的丢包率分别为  $P_f$  和  $P_r$ ,则包传输失败的概率为

$$P = 1 - (1 - P_f) \times (1 - P_r) \quad (1)$$

因此链路质量表示为  $\chi = 1 - P$ 。设无线链路( $u, v$ )传递的分组数为  $\omega_{u,v}$ 。因为链路质量问题导致部分分组不能成功到达,所以单位时间内在无线链路( $u, v$ )上实际传递的分组数  $c(u, v)$  为

$$c(u, v) = \frac{\omega}{1 - \chi_{u,v}} \quad (2)$$

任意一条从节点  $x$  到节点  $y$  的路径  $p\{x, y\}$ , 表示为  $x \rightarrow m \rightarrow \dots \rightarrow n \rightarrow y$ , 标记路径  $p\{x, y\}$  上节点的集合为  $\Lambda$ 。该路径实际传递的分组数  $\lambda(x, y)$  表示为( $\beta$  是  $\alpha$  的后继节点)

$$\lambda(x, y) = \frac{\omega}{1 - \chi_{x,m}} \times \dots \times \frac{1}{1 - \chi_{n,y}} = \frac{\omega}{\prod_{\alpha, \beta \in \Lambda} (1 - \chi_{\alpha, \beta})} \quad (3)$$

可见链路质量的好坏直接影响到节点分组传输的成功率。链路质量越好,单位时间传递的分组数就越可能是实际接收到的分组数,分组传送率越高,选择的路由越高效。链路质量变化较大时,单位时间成功传递的分组数减少,频繁的路由重建将会导致大量数据包的丢失,这不仅占用了网络资源,更延迟了数据包的发送。

### 3.2 算法中链路质量的评估

移动 Ad-hoc 网络中的链路质量问题常常导致分组传递失败的重新传输问题。根据此特点,De Couto 等人提出了基于期望传输次数 ETX (Expected Number of Transmissions)<sup>[15]</sup>的度量方法。ETX 使用广播技术来获取链路双向的丢包率,将无线链路上成功交付一个数据帧所需传输次数的期望值作为链路质量好坏的度量,一条路由的 ETX 度量是该路径上每条链路的 ETX 度量总和。因此路由由算法选择最优路径上所有链路的 ETX 的总和应为最小。

包传输失败的概率  $P$  由式(1)计算所得。则  $k$  次重传后传输成功的概率  $s(k)$  为

$$S(k) = p^{k-1} \times (1 - p) \quad (4)$$

链路上的 ETX 值为

$$ETX = \sum_{k=1}^{\infty} k \times s(k) = \frac{1}{1-P} = \frac{1}{(1-P_f) \times (1-P_r)} \quad (5)$$

分组传送率可通过实际计算收到的信标和数据帧来检测丢失的分组,这通常被认为是最准确地测量接受概率的方法。但这需要维持大量的广播探测包,增大了通信开销,会造成不必要的能量损耗。因此,对所有的方法来说,最直接和最有效的方法是基于 IEEE 802.15.4 的 MAC 层和 PHY 层所提供的每一帧的链路质量指示值 LQI。链路质量指示值(Link Quality Indicator, LQI)是 802.15.4 标准提出的反映链路质量的重要指标,表征接收数据帧的能量与质量。无线通信芯片 CC2420 对 LQI 的测量提供硬件支持。在环境动态变化或有干扰源的情况下,可在应用层通过 `afIncomingMSGPacket_t * pkt; pkt > LinkQuality` 直接获得<sup>[16]</sup>。基于链路的不对称性和应用需求,将  $(v_i, v_{i+1})$  链路上的 LQI 值  $LQI(v_i, v_{i+1})$  用一组矢量对  $\{LQI^+(v_i, v_{i+1}), LQI^-(v_i, v_{i+1})\}$  表示,其中,  $LQI^+(v_i, v_{i+1})$  表示正向链路的链路质量指示值;  $LQI^-(v_i, v_{i+1})$  表示反向链路的指示值。用 LQI 衡量链路质量需要一定长度的时间窗口。在实际操作中,为了节省时间和资源,可以采取平均的方法进行统计。

假定一个长度为  $L$  的路由  $P$  由节点  $[v_0, v_1, \dots, v_L]$  组成,链路表示为  $[v_i, v_{i+1}]$ ,则路由  $P$  的路由度量  $ETX_{LQ}(p)$  定义为

$$ETX_{LQ}(p) = \sum_{i=0}^{L-1} lq\{[v_i, v_{i+1}]\} \quad (6)$$

式中,  $lq\{[v_i, v_{i+1}]\}$  为链路选择开销,定义为

$$lq\{[v_i, v_{i+1}]\} = \frac{1}{LQI^+(v_i, v_{i+1}) \times LQI^-(v_i, v_{i+1})} \quad (7)$$

选择  $LQI(v_i, v_{i+1})$  作为链路质量评价来设计路由协议。当路由协议需要选择下一跳节点进行转发时,根据邻居节点列表中的链路质量评价来选择链路质量最高的作为下一跳节点,以获得最大的分组传送率。对应当前节点的每条链路状态进行评价,  $LQI(v_i, v_{i+1})$  最大时,路径  $p$  上所有链路选路开销  $lq\{[v_i, v_{i+1}]\}$  的总和  $ETX_{LQ}(p)$  应为最小,此时路径  $p$  为最优路径,路由算法选择最优。

### 3.3 LQPR 算法

移动 Ad-hoc 网络中的移动节点已经通过如 GPS 或是其他定位系统得到各自的网络坐标信息,同时为进一步减少控制开销,将位置信息捎带在数据包中进行传送。每个节点通过广播 Hello 报文获得无线电覆盖范围内邻节点的位置信息,从而转发数据包。

基于对链路质量的考虑,在 LQPR 中提出任意网络节点  $u$  收到 hello 信息后进入链路质量模式(LQ mode)。依据链路质量(如测量接收信号的强度)对网络图  $G$  中的所有邻居节点  $N(u)$  以递减的顺序排序  $\infty_u$ 。在这里不是把  $\infty_u$  序列对应于节点间的欧几里德距离,而是更多表示为链路质量特性,如接收信号强度或是分组递交率等。依据上一节的分析,选择  $LQI(v_i, v_{i+1})$  值对应式(7)得到  $lq\{[u, v]\}$  值进行排序

$$lq\{[u, v_1]\} < lq\{[u, v_2]\} < \dots < lq\{[u, v_n]\}$$

如果链路  $(u, v_1)$  在排序  $\infty_u$  中比链路  $(u, v_2)$  出现得早,就说明  $(u, v_1)$  比  $(u, v_2)$  链路质量高,可被定义为  $v_1 \infty_u v_2$ 。值得注意的是,如果有多条链路具有相同的链路质量,那么可根据节点 ID 号的唯一性确定排序。定义节点  $u$  到邻节点  $v$  的路由权值是一个二元组:  $\langle lq\{[u, v]\}, ID(v) \rangle$ , 对于  $v_1, v_2 \in N$

$(u, v_1 \infty_u v_2 \Leftrightarrow lq\{[u, v_1]\} < lq\{[u, v_2]\}$  或者  $lq\{[u, v_1]\} = lq\{[u, v_2]\}$ , 且  $ID(v_1) < ID(v_2)$ 。

如图 1 所示,发送节点  $x$  将其无线电覆盖范围分为白区(White Region)和黑区(Dark Region),白区再根据到目的节点距离的远近划分成不同小的区域(WS1、WS2、WS3)。

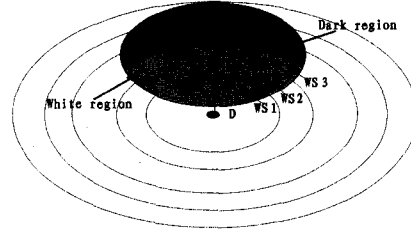


图 1 划分无线电覆盖范围

可见,从 White Region 内选择除自己以外的到目的节点最近的节点作为接收节点转发分组是从能量考虑最经济的方法。若 WS1 区域内存在节点  $\omega_1, \dots, \omega_n \in N_x$ , 则根据链路质量递减顺序进行  $\infty_x$  排序,然后遍历  $\infty_x$  序列:“质量好”的链路首先被选择。若 WS1 区域内不存在节点  $x$  的邻居节点,则转到 WS2 区域寻找……。LQ 模式如下所示

For each node  $u$ (destination: D):

- 1: neighbors  $N(u)$ ;
- 2: radius  $R$ ;
- 3: region  $n$ ;
- 4: dist\_region  $d$ ;
- 5: node  $v, w, first\_lq$ ;
- 6: nodes  $M[]$ ;
- 7: iteration  $\leftarrow 1$ ;
- 8: for (iteration=1; iteration <  $n$ ; iteration++)
- 9: {
- 10:  $d = R/n * iteration$ ;
- 11: While ( $v \in N(u)$ )
- 12: if ( $dis[v, D] < d$ )  $M[] \leftarrow v$ ;
- 13: if ( $M[]$ ) exit;
- 14: }
- 15: While ( $w \in M[]$ ) {
- 16: Sort( $first\_lq, LQ(u, w)$ );
- 17:  $u.next \leftarrow first\_lq$ ;
- 18: }

第 3 行根据距离目的节点  $D$  的远近划分  $n$  块区域;第 7 行存储迭代次数  $iteration(\leq n)$ ,第 10 行计算区域  $iteration$  的通信范围,第 12 行  $M[]$  存储区域  $iteration$  下的邻居节点;第 16 行将排序  $M[]$  中邻居节点  $w$  对应式(7)得到的  $lq\{[u, w]\}$  值进行排序  $\infty_u$ ,得到排序第一的邻节点保留在变量  $first\_lq$  中;第 17 行选择  $first\_lq$  节点作为 LQ 模式下的下一个节点转发数据包。

如果 White Region 内因缺少节点为空洞,导致发送节点  $x$  不可能完成到目的节点的转发任务,LQ 模式结束。为解决这个问题,LQPR 算法采取边界(Perimeter)转发策略,寻求路由绕过空洞,这样发送节点可以选择图 1 中黑色区域内的节点作为接收节点转发数据包。当数据分组进入边界转发模式时,LQPR 会记录模式转换点  $X$  的地理位置信息,并将它保留在数据分组中,作为恢复到 LQ 模式的判断依据。在进行边界转发时,LQPR 使用右手规则通过网络,即在逐步靠近目的节点  $D$  的面上按照右手法则将该数据分组转发到被节点

X 到节点 D 的连线 XD 所分割面 XGHIJLK 的第一条边上。一旦转发节点收到了数据分组, LQPR 首先会对保存在数据分组中 X 的位置信息和该转发节点的位置信息进行比较。如果该转发节点到目的节点的距离  $d$  比 XD 小, 则 LQPR 标志为 LQ 模式, 重新进入 LQ 模式的执行过程。如图 2 所示, 图中实线表示实际存在通信链路, 红色线条表示路由过程, 实箭头旁的字母 LQ 和 F 分别表示 LQ 模式和边界路由模式。

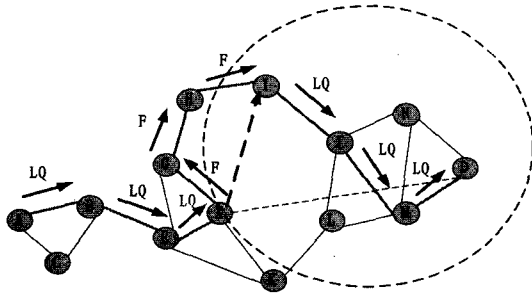


图 2 边界转发的例子

## 4 仿真

### 4.1 场景配置

仿真基于 ns-2.28, 并在  $1200\text{m} \times 1200\text{m}$  的正方形区域内进行。给网络中各节点设置的运动场景如下: 取 40 个节点随机分布在区域内, 节点采用 Random Waypoint 的运动模型, 仿真中选取的  $V_{\max}$  为  $[0, 30]\text{m/s}$ , 利用 setdest 工具来完成。在业务方面, 随机产生 (10、20、30、40) 对 CBR (constant bit rate) 连接。流量场景利用 cbrgen 流量产生工具来完成。采用基于 802.11 标准的 MAC 协议, 该 MAC 协议采用 CSMA/CA 多址接入方式。仿真中选取传输半径 150m。具体的仿真参数设置见表 1。

表 1 仿真参数设置

节点数量	40
通信半径/m	150
信道速率/Mbps	2
环境尺寸/ $\text{m}^2$	$1200 \times 1200$
节点最大移动速度/ $\text{m} \cdot \text{s}^{-1}$	30
业务类型	CBR
产生分组数率/ $\text{s}^{-1}$	2
分组长度/Byte	256
仿真时间/s	1000

### 4.2 仿真结果

评价一个无线移动网络的协议性能是否优良, 主要有以下几个评估参数:

- 1) 分组传送率(归一化): 被成功传送分组的比例;
- 2) 分组平均延时(单位 s): 成功将分组转发到目的地所需时间的平均值;
- 3) 平均吞吐量(单位 kbps): 单位时间成功传送的分组数。

DSDV (Destination Sequenced Distance Vector Routing) 是目的序列距离向量路由协议, 属于传统路由协议中表驱动路由的一种。AODV (Ad-hoc On-demand Distance Vector Routing) 是距离向量路由协议, 属于传统路由协议中按需路由的一种。图 3—图 6 分别给出采用 DSDV、AODV、GPSR 和本文提出的 LQPR 算法下的仿真结果对照。

图 3 显示节点最大移动速度在  $[0, 30]$  范围内分别使用

DSDV 和 LQPR 获得的平均端到端延时变化。LQPR 协议下的延迟远小于 DSDV, 这主要是由于 DSDV 发送数据包之前首先要寻找路由, 建立和维护路由信息表, 在信道获取上消耗了较多的网络资源。LQPR 不需要存储路由信息, 也不需要发送路由更新信息, 利用节点位置信息转发数据包减少了类似于包丢失等中断。

同时, 随着节点运动速度的增大, 网络拓扑结构迅速变化, 节点间的链路则经常割裂断开, 导致 AODV 在花费了较高代价来维护和更新路由信息的同时, 却得不到较高的平均吞吐量, 如图 4 所示。LQPR 充分考虑了链路质量因素选择较稳定的路由, 势必会减少不必要的网络开销以及延迟等待, 相应的网络吞吐量也得到了改善。因此, LQPR 适用于拓扑变化相对频繁的网络环境。

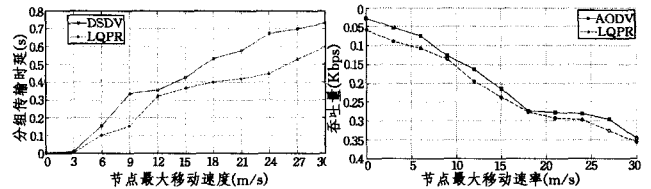


图 3 DSDV 和 LQPR 分组传输时延的比较 图 4 AODV 和 LQPR 吞吐量比较

图 5 显示在通信源数(数据流数目)分别为 10、20、30、40、50 下得到的丢包数。其中, LQPR 的丢包数受通信源数量变化的影响不大, 基本上都在 100 (packets) 以下。而 GPSR 受通信源数量变化的影响最大, 最多的时候(通信源数量为 50 的时候)已经达到 400 (packets) 左右。这主要是由于 GPSR 协议下的数据分组可能在大量无效甚至断裂的链路上传输, 增加了产生冲突的可能性, 导致了大量的数据包在传输过程中丢失。

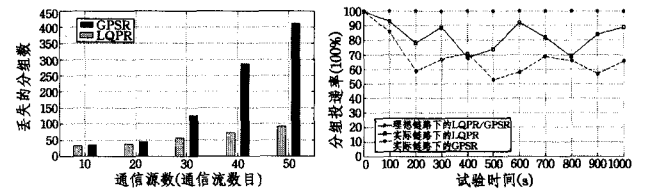


图 5 GPSR 和 LQPR 丢弃分组数随网络规模的变化 图 6 GPSR 和 LQPR 实际链路下分组投递率的比较

为了模拟无线链路的误码率, 使用 NS2 提供的错误模型 ErrorMode, 在每个节点输入和输出的无线信道上插入给定的统计错误率。该模型将工作在节点的 MAC 层与物理层间的所有数据从 MAC 层发往物理层 (OutgoingErrProc) 或由物理层发往 MAC 层 (IncomingErrProc) 时, 由系统随机生成介于 0 到 1 之间的数值。分组增加标志位 error, 当其小于预设的错误率时, 标志位 error=1; 否则为 0。从 MAC 层接收到数据分组, 如果 error 标志为 1, 说明无线链路质量较差, 则丢弃该分组, 否则成功接收, 从而达到仿真实际链路的效果。

分别比较 GPSR 和 LQPR 在实际链路状态下的分组传送率, 如图 6 所示。在理想链路上, GPSR 和 LQPR 的传送率为 100%, 这是因为理想链路上链路质量均设定为 1, LQPR 的链路质量模式退化为贪婪模式; 而在实际链路上, LQPR 的传送率比 GPSR 有较大幅度的提高。

图 6 示出节点在试验时间  $[0, 1000]$  秒内获得的分组传

(下转第 83 页)

射的参数、LFSR的初始值以及LFSR所使用的本原多项式4部分构成,可以有效地防止密钥搜索攻击。

**结束语** 利用PWLCM映射的良好密码学特性,采用 $m$ -LFSR与PWLCM相结合的方式,提出了一种收缩式伪随机序列发生器。理论分析和统计测试表明,该伪随机序列发生器具有良好的密码学性质。

### 参考文献

[1] Kohda T, Tsuneda A. Statistics of chaotic binary sequences[J]. IEEE Transactions on Information Theory, 1997, 43 (1): 104

[2] Stojanovski T, Kocarev L. Chaos-based random number generators-part I: analysis[J]. IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, 2001, 48 (3): 281-288

[3] Stojanovski T, Pihl J, Kocarev L. Chaos-based random number generator-part II, practical realization[J]. IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, 2001, 48(3): 382

(上接第54页)

速率的变化。由GPSR和LQPR路由算法的对比结果可知, LQPR始终具有较稳定及相对较高的分组传送率,这主要是由于LQPR在建立路由时,综合考虑了邻居节点的位置、链路质量等因素,它试图使包到达目的节点的链路状况达到最好且所经过的跳数减到最小,因而对转发节点的选择较GPSR路由协议更加准确,有效降低了中断等链路质量下降引起的数据分组丢失的概率,提高了分组成功传输率。

**结束语** 本文从提高分组传送率的角度出发,提出了一种根据链路质量选择路由,并运用在基于地理位置基础上的LQPR协议。LQPR算法适用于节点数多、拓扑控制变化频繁、链路质量不稳定的Ad-hoc网络环境中。通过对比AODV、GPSR和LQPR的仿真结果,证明了LQPR在一定的速度范围内能够有效地减少端到端传输延迟,增大吞吐量,提高数据分组的传输效率。它受无线环境的影响较GPSR要小得多,所形成的路由更为可靠,在很大程度上提高了传输路径的鲁棒性。

### 参考文献

[1] Perkins C, Bhagwat P. Highly Dynamic Destination-sequenced Distance-Vector (DSDV) Routing for Mobile Computers[C]// Proceedings of the SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications, Aug. 1994: 234-244

[2] Perkins C E, Royer E M. Ad-hoc on Demand Distance Vector (AODV) Routing[C]// Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, Feb. 1999: 90-100

[3] Johnson D B. Routing in Ad hoc Networks of Mobile Hosts[C]// Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, Dec. 1994: 158-163

[4] Basagni S, Chlamtac I, Szyrogi V R, et al. A Distance Routing Effect Algorithm for Mobility (DREAM) [C]// Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM). 1998: 76-84

[5] DeCouto D S J, Morris R. Location Proxies and Intermediate Node Forwarding for Practical Geographic Forwarding [R].

[4] 鞠磊, 翁贻方, 赵耿, 等. 一种具有时变密钥的自同步混沌加密方法[J]. 计算机科学, 2009, 36(9): 46-48

[5] 桑涛, 王汝笠, 严义坝. 一类新型混沌反馈密码序列的理论设计[J]. 电子学报, 1999, 27(7): 47

[6] 胡国杰. 混沌保密通信系统的保密性能分析及新型混沌数字加密系统理论设计[D]. 上海: 上海交通大学, 2003

[7] Coppersmith D, Krawczyk H, Mansour Y. The shrinking generator [C] // Advances in Cryptology-CRYPTO '93, Lecture Notes in Computer Science, vol. 773. 1993: 22-39

[8] Sang Tao, Wang Rui-li, Yan Yi-xun. Clock-controlled chaotic keystream generators [J]. Electronics Letters, 1998, 34 (20): 1932-1934

[9] 李树钧. 数字化混沌密码的分析与设计[D]. 西安: 西安交通大学, 2003

[10] 周红, 罗杰, 凌燮亭. 混沌非线性反馈密码序列的理论设计和有限精度实现[J]. 电子学报, 1997, 25(10): 57

[11] Baranousky A, Daems D. Design of one-dimensional chaotic maps with prescribed statistical properties[J]. Int. J. Bifurcation and Chaos, 1995, 5(6): 1585-1598

Tech. Rep. MIT-LCS-TR824, MIT Lab. Comp. Sci. June 2001

[6] Heinzelman W B, Chandrakasan A P, Balakrishnan H. An Application-specific Protocol Architecture for Wireless Microsensor Networks[J]. IEEE Transactions on Wireless Communications, 2002, 1(4)

[7] Chen B, Jamieson K, Balakrishnan H, et al. Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks[C]// Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking, July 2001

[8] Karp B, Kung H T. GPSR: Greedy Perimeter Stateless Routing for Wireless Networks[C]// Proceedings of ACM-IEEE Mobile Comp. Net. 2000: 243-254

[9] Kim Y-J, Govindan R, Karp B, et al. Geographic Routing Made Practical[C]// 2nd Symposium on Networked Systems Design & Implementation (NSDI). 2005: 220-230

[10] Reijers N, Halkes G, Langendoen K. Link layer measurements in sensor networks [A] // Proceedings of First International Conference on Mobile Ad-hoc and Sensor Systems [C]. Fort Lauderdale, USA, 2004: 224-234

[11] Imielinski T, Navas J C. GPS-based Geographic Addressing Routing and Resource Discovery [J]. Communications of the ACM, 1999, 42(4): 87-92

[12] Takagi H, Kleinrock L. Optimal transmission range for randomly distributed packet radio terminals[J]. IEEE Transactions on Communications, 1984, 32(3): 246-257

[13] Rappaport T S. Wireless Communications: Principles and Practice (2nd edition) [M]. Beijing: Publishing House of Electronics Industry, 2004

[14] 韩冰青, 陈伟, 张宏. 一种新的QoS感知的Ad-hoc网络多径DYMO路由协议[J]. 计算机科学, 2010, 37(3): 79-82

[15] De Couto D S J, Aguayo D, Bicket J, et al. A High-throughput Path Metric for Multi-hop Wireless Routing [C] // Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MobiCom '03). New York, USA: ACM, 2003: 134-146

[16] 孙佩刚, 赵海. 无线网络链路通信质量测量研究[J]. 通信学报, 2007, 28(10): 14-22