基于节点安全度的P2P网络分布式多路径中继路由协议

王浩云 徐焕良 任守纲

(南京农业大学信息科技学院 南京 210095)

摘 要 在对中继节点的安全度进行评估的基础上,提出了一种基于节点安全度的P2P网络分布式多路径中继路由协议NSD-DPMRR(Distributed Protocol for Multipath Relay Routing based on Node's Security Degree)。该协议可分布式地计算出源端节点发送数据的最佳速率以及各中继节点的最佳转发速率。仿真实验表明,该协议在将恶意中继节点对数据传输的危害降低到最低程度的同时,能够最大化目的端节点所能接收到的正常数据,保证了中继路由的安全性和有效性,且协议的复杂度较低。

关键词 P2P网络,多路径中继,节点策略,安全度

中图法分类号 TP393 **文献标识码** A

Distributed Protocol for Multipath Relay Routing Based on Node's Security Degree

WANG Hao-yun XU Huan-liang REN Shou-gang

(School of Information Science & Technology, Nanjing Agricultural University, Nanjing 210095, China)

Abstract Based on the assessment of relay node's security degree, a distributed protocol for multipath relay routing based on node's security degree (NSD-DPMRR) was proposed for P2P network. The best send rate of the source node and the best forward rate of the relay nodes can be computed with distributed method. The simulation shows that the protocol proposed will reduce the damage to the data transmission by malicious relay nodes, maximize the right data received by the destination node, and ensure the security and effectiveness of relay routing with lower complexity.

Keywords Peer-to-peer network, Multipath relay, Node strategy, Security degree

1 引言

P2P网络的核心思想是网络中的各个节点都处于平等的地位,每个节点在获取服务的同时也提供服务。但是网络地址转换协议NAT技术阻碍了P2P网络中内网节点和外网节点的直接通信[1]。最近的研究显示,在KaZaA系统中大约有30%的节点驻留在内网[2],外网节点无法直接与其建立TCP链接而获取资源。在针对NAT穿透的各种解决方案中,最可靠的方式是利用带有公网IP地址的中继节点作为中继来进行通信。目前,Skype[3]、KaZaA和Grid overlay[4]等P2P网络都是通过中继节点进行通信的。因此,对中继节点的选择和中继路由协议的设计直接影响着P2P网络的服务质量。

P2P节点的自主性使得节点可以选择自身的行为策略。如果作为中继的P2P节点采取恶意行为,将造成很大的危害。恶意中继节点很容易实现信息窃取[5]、信息篡改[5]或者路由重定向等恶意行为。如果中继路由采用单路径方式进行时,路径上中继节点的恶意行为将严重危害到数据的传递;而采用多路径方式时,数据将在源端节点进行分拆,在目的节点重新组装,数据的不同部分通过多条不同路径进行传输。这种方式降低了被恶意中继节点窃听和篡改的风险,增加了数据传输的安全性。

由于P2P网络具有良好的可扩展性,能避免单点失效问题,因此很多实时流媒体应用开始构架在P2P网络上[6]。由于流媒体业务的特点,其数据的传输对网络带宽和丢包提出了严格要求。当路径发生拥塞或者中继节点存在恶意行为时,传统的单路径方式无法保证网络性能的稳定性;而采用多路径方式,能够通过由多条路径发送数据,减少丢包率,提高网络吞吐量,保障流媒体数据传输的质量。

本文提出了一种基于节点安全度的P2P网络分布式多路径中继路由协议NSD-DPMRR(Distributed Protocol for Multipath Relay Routing based on Node's Security Degree)。该协议分为路径建立和数据传输两个阶段。在路径建立阶段,源端节点和中继节点在搜索可用路径的同时,对相邻下游节点的安全度进行评估;而在数据传输阶段,所有节点根据出口链路的可用带宽和相邻节点的安全度,计算出源端节点发送数据的最佳速率以及各中继节点的最佳转发速率,从而在将恶意中继节点对数据传输的危害降低到最低程度的同时,最大化目的端节点所能接收到的正常数据。由于本文所提协

到稿日期:2012-01-19 返修日期:2012-03-06 本文受南京农业大学青年科技创新基金项目(KJ2010022),国家科技部农业成果转化重大资金项目(2011GB2C100001),江苏省科技支撑计划重大项目(BE2011398),江苏省科技支撑计划项目(BE2011339),中央高校基本科研业务费项目(Y0201100080)资助。

王浩云(1981—),男,博士,讲师,主要研究方向为P2P网络、物联网、CPS相关协议和机制优化设计等,E-mail:why_583@163.com;徐焕良(1963—),男,博士,教授,主要研究方向为物联网关键技术;任守纲(1977—),男,博士,副教授,主要研究方向为农业物联网应用技术。

议 NSD-DPMRR 中的算法能够在所有节点上分布式执行，因此协议复杂度较小。

2 相关工作

多路径路由首次在文献[7]中提出，其中数据报在多条不相交的路径上传输，用以均衡网络负载，保证数据传输的稳定性。源节点可以增加发送数据的冗余度，即使路径拥塞导致一定程度的数据报丢失，目的节点仍然能够将接收到的数据报重组。借鉴其思想，文献[8-11]利用多路径路由解决路径上各节点存在被攻击或失效的问题。在这些协议中，文献[8,9]所提路由的多个路径均不相交，而文献[10,11]则允许多个路径相交情况的存在。本文同样利用多路径方式降低中继节点的恶意行为对数据传输所造成的危害，而且所提协议适用于路径相交和不相交的情况。

为了对中继节点潜在的恶意行为进行评估，本文利用信任模型[12]来计算中继节点的安全度。目前关于信任模型主要有基于概率统计的信任模型、基于模糊数学的信任模型、基于主观逻辑的信任模型[13]和基于证据理论的信任模型[14]等。上述几种信任模型通过直接或者间接方式收集周围节点的信息，通过信任计算得出节点的信任值。不同之处在于信任值度量和信任计算方式的差异。但由于节点行为的多样性，原始计算出来的信任值并不能直接反映中继节点的行为。例如，中继节点能够发送伪造数据来提高自身信任度，从而获取更多的流量后进行信息窃取、信息篡改等恶意攻击；或者，多条路径上的中继节点通过分别抬高和降低信任度的方式导致路由的重定向。

本文提出的 NSD-DPMRR 协议在最小化中继节点恶意行为危害的同时，实现了目的端节点接受正常数据的最大化，因此可以将其看作是一个最大最小问题。文献[15]提出将这类最大最小问题转换为最大流问题[16]来处理。传统上利用线性规划来解决最大流问题，算法通常集中在源节点上执行。因此，源节点需要知道全部的链路和中继节点的信息，且计算量较大。而 Goldberg 和 Tarjan 提出的预流推送算法[17]能够分布式解决最大流问题，且计算复杂度较小。文献[18]在此基础上提出了分布式的安全路由协议，协议中的算法在所有节点上分布执行，各节点只需要知道本地信息。但该协议中节点的行为参数为预先设定值，且考虑的恶意节点行为策略单一。

针对上述问题，本文在分析多路径中继路由中端节点和恶意中继节点的行为策略的基础上，提出了节点安全度模型，它将原有节点的信任值与其潜在行为策略相关联，对中继节点的多种恶意行为进行度量，为安全多路径中继路由协议的设计提供依据。同时，本文对预流推送算法进一步拓展，在节点安全度模型的基础上，提出了一种新型的基于节点安全度的 P2P 网络分布式多路径中继路由协议 NSD-DPMRR。同以往的研究相比，协议 NSD-DPMRR 在面对中继节点多种潜在恶意行为的威胁时，更能够保障中继路由中数据传输的有效性和安全性。

3 中继节点行为策略分析

P2P 网络中的节点按照在多路径中继路由上的位置可以分为端节点和中继节点，而中继节点按照其类型可分为善意节点和恶意节点。中继节点的类型将决定其在中继路由各阶段所采用的策略。

3.1 善意中继节点的行为策略

本文所提路由协议分为路径建立和数据传输两个阶段，在不同阶段善意节点有相应的行为策略。

在路径建立阶段，中继节点由于其善意本质将采用诚实策略，即将自己对所在路径的信任程度如实向上游中继节点提交。

在数据传输阶段，善意中继节点可以采取的行为策略有合作和非合作。虽然善意节点转发数据报的行为并没有增加其收益，但中继节点的善意本质决定它在采取合作策略时将正常接收和转发数据报。而非合作策略指的是善意中继节点在其出口链路的带宽已完全被占用时，既不接受数据报也不转发。

3.2 恶意中继节点的行为策略

恶意中继节点由于其恶意本质，将选择相应的行为策略，最大化其对多路径路由数据传输的破坏程度。恶意节点在协议的不同阶段有其相应的行为策略。

在路径建立阶段，恶意中继节点面对其他恶意中继节点时，可采用共谋策略。恶意中继节点间的共谋策略是指多条路径上的恶意中继节点通过伪造链路或发送虚假数据等方式，分别抬高和降低其对所在路径的信任度，从而将大部分流量吸引到信任度被恶意抬高的路径上来，导致该路径的瓶颈处发生拥塞，传输性能恶化，或者直接进行恶意攻击。

在数据传输阶段，恶意中继节点在面对同路径上善意中继节点转发来的数据报时，可采用的行为策略有：窃听、篡改和丢弃等。窃听策略是指恶意中继节点在转发数据的同时窃取数据信息；而篡改策略是将转发数据的信息抹去或者修改为虚假信息。丢弃策略指的是恶意中继节点不转发所接受的数据，其原因可能是出口链路拥塞或者数据报被恶意丢弃。由于窃听和篡改策略可归为不丢弃策略，因此恶意中继节点的行为又可划分为两类：丢弃和不丢弃策略。

恶意中继节点采取丢弃策略所需的成本较低，而采取不丢弃策略所需的成本较高。考虑到恶意节点在实现攻击效果最佳的同时也要将成本控制在一定的范围内，本文认为在路径建立阶段对恶意降低其所在路径信任度的中继节点，在数据传输阶段将采取不丢弃策略；而在路径建立阶段对恶意抬高其所在路径信任度的中继节点，在数据传输阶段将采取丢弃策略。

3.3 端节点和恶意中继节点行为策略博弈

当中继路由的多条路径建立后，源端节点 s 通过多条路径向目的端节点 t 传输数据，所涉及到的所有中继节点的集合为 M，链路集合为 L。某条路径上中继节点 j 的上游中继节点集合为 $U(j)$，而其下游中继节点为 $D(j)$。节点 i 和其下游节点间的链路为 $l_{i,j\in D(i)}\in L$，其带宽为 $B_{i,j\in D(i)}$。在数据传输过程中，源端节点 s 的发送速率为 X_s，而链路 $l_{i,j}$ 上所承载的数据流量为 $x_{l_{i,j}}$。

在数据传输阶段，恶意中继节点将选择相应的策略以最大化对数据传输的危害。因此恶意中继节点行为策略的选择可以看作是最大化问题。设定恶意中继节点集合为 $M_B\subset M$，其中采取丢弃策略的恶意中继节点集合为 M_B^D，而采取不丢弃策略的恶意中继节点集合为 M_B^N。节点 $i\in M_B^D$ 对所转发数

据的丢弃概率为 a_i^D，而节点 $j\in M_B^N$ 对所转发数据进行窃听或篡改的概率为 a_j^N。该最大化问题可表示如下：

$$V^*=\max_{M_B^D,M_B^N}\Big[\sum_{\{j\in M_B^D|a_j^D>0\}}a_j^D x_{i\in U(j),j}+\sum_{\{j\in M_B^N|a_j^N>0\}}a_j^N x_{i\in U(j),j}\Big] \tag{1}$$

面对恶意中继节点的行为策略，源端节点希望所传输的数据报受到恶意中继节点的影响尽可能小，保证目的端节点能够收到更多的正常数据报。因此，端节点和恶意中继节点行为策略博弈可表示为最大最小问题，即：

$$W^*=\max_{X_s,x_{i\in L}M_B^D,M_B^N}\min\Big[X_s-\sum_{\{j\in M_B^D|a_j^D>0\}}a_j^D x_{i\in U(j),j}-\sum_{\{j\in M_B^N|a_j^N>0\}}a_j^N x_{i\in U(j),j}\Big] \tag{2}$$

$$\text{s.t.}\quad \sum_{i\in U(j)}(1-a_i^D)x_{i,j}=\sum_{k\in D(j)}x_{j,k},\ \forall j\in M_B^D$$

$$\sum_{i\in U(j)}x_{i,j}=\sum_{k\in D(j)}x_{j,k},\ \forall j\notin M_B^D$$

$$0\leqslant x_{i,j}\leqslant B_{i,j}$$

式(2)中包含了本文所提最大最小问题的3个约束条件。其中：第1个条件代表采取丢包策略的中继节点处流量守恒的条件，即中继节点只转发没有被丢弃的数据报；第2个条件表示其他中继节点处的流量守恒条件；第3个条件表示链路带宽对所传输流量的限制条件。

4 中继节点安全度模型

在多路径中继路由的路径建立阶段，源端节点需要对各路径上中继节点的行为策略进行评估。本节首先对基于主观逻辑的信任模型进行简单描述；然后对传统的利用路径信任模型来评估中继节点行为的方式所存在的问题进行讨论；在此基础上，结合第3节对中继节点行为策略的分析，提出了中继节点安全度的概念和计算方法。算法的实施方案将在第6节给出。

4.1 基于主观逻辑的信任模型

A. Josang 基于主观逻辑理论提出了一种信任度模型，它引入事实空间和观念空间来描述和度量信任的关系。主观逻辑定量地定义了可信度的组成、传递与合并的方式。但它无法消除多路径中继路由中节点协同作弊和诋毁继而攻击的安全隐患。

模型中的信任度 $w_{a,b}=(b_{a,b},d_{a,b},u_{a,b})$ 表示节点 a 对节点 b 的可信度评价，$b_{a,b}$、$d_{a,b}$、$u_{a,b}$ 分别表示信任、不信任和不确定的概率，它们满足：$b_{a,b}+d_{a,b}+u_{a,b}=1$，且 $b_{a,b},d_{a,b},u_{a,b}\in[0,1]$。下面给出节点间信任度传递和合并计算的定义。

定义1(信任的传递)　节点 a 对节点 b 的信任度为 $w_{a,b}$，节点 b 对节点 c 的信任度为 $w_{b,c}$，则节点 a 对节点 c 的信任度为 $w_{a,c}$，且

$$\begin{aligned}w_{a,c}&=w_{a,b}\otimes w_{b,c}\\&=(b_{a,b},d_{a,b},u_{a,b})\otimes(b_{b,c},d_{b,c},u_{b,c})\\&=(b_{a,b}b_{b,c},b_{a,b}d_{b,c},d_{a,b}+u_{a,b}+b_{a,b}u_{b,c})\end{aligned} \tag{3}$$

定义2(信任的合并)　节点 a 通过 c 的推荐对 b 的信任度为 $w_{a,b}^c$，通过 d 的推荐对 b 的信任度为 $w_{a,b}^d$，则节点 a 对 b 的综合信任度为 $\overline{w}_{a,b}$，且

$$\begin{aligned}\overline{w}_{a,b}&=w_{a,b}^c\oplus w_{a,b}^d\\&=(b_{a,b}^c,d_{a,b}^c,u_{a,b}^c)\oplus(b_{a,b}^D,d_{a,b}^D,u_{a,b}^D)\\&=\Big(\frac{b_{a,b}^c u_{a,b}^d+b_{a,b}^d u_{a,b}^c}{k},\frac{d_{a,b}^c u_{a,b}^d+d_{a,b}^d u_{a,b}^c}{k},\frac{u_{a,b}^c u_{a,b}^d}{k}\Big)\end{aligned} \tag{4}$$

式中，$k=u_{a,b}^c+u_{a,b}^d-u_{a,b}^c u_{a,b}^d$。

4.2 路径信任模型

路径信任度是指源端节点对到达目的端节点路径的信任程度。图1中，节点 a 对其下游中继节点 $a1$、$a2$ 和 $a3$ 的信任度为 $w_{a,a1}$、$w_{a,a2}$ 和 $w_{a,a3}$，而 $a1$、$a2$ 和 $a3$ 对节点 t 的信任度为 $w_{a1,t}$、$w_{a2,t}$ 和 $w_{a3,t}$。根据主观信任度的计算法则，节点 a 通过其下游中继节点到达节点 t 的各条路径的信任度分别为 $w_{a,a1}\otimes w_{a1,t}$、$w_{a,a2}\otimes w_{a2,t}$ 和 $w_{a,a3}\otimes w_{a3,t}$。

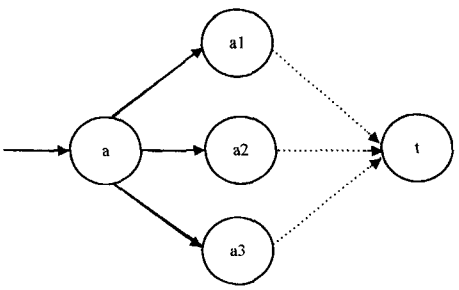


图1　路径信任示意图

考虑到恶意中继节点的行为，本文将中继节点拆分为两个独立节点，分别代表原节点的入口和出口，中间用一条链路相连。这样，节点 a 对通过下游节点到达节点 t 各条路径的信任度实际上是：$w_{a,a1_{in}}\otimes w_{a1_{in},a1_{out}}\otimes w_{a1_{out},t}$，$w_{a,a2_{in}}\otimes w_{a2_{in},a2_{out}}\otimes w_{a2_{out},t}$ 和 $w_{a,a3_{in}}\otimes w_{a3_{in},a3_{out}}\otimes w_{a3_{out},t}$。

中继节点只需增大或者减少其内部链路的信任度 $w_{a1_{in},a1_{out}}$、$w_{a2_{in},a2_{out}}$ 和 $w_{a3_{in},a3_{out}}$，就能实现对各路径信任度的恶意抬高或降低。由于善意节点和恶意节点信息的不对称，善意节点 a 只能够知道被下游恶意中继节点修改过的路径信任值。因此，通过信任传递所得到的路径信任度无法反映出中继节点潜在的恶意行为。

4.3 中继节点安全度模型

如上文所述，单条路径的信任度无法真实地反映出该路径上中继节点的历史行为。考虑到路径建立阶段恶意中继节点采用共谋策略的特点，本文将利用除该路径外的其它路径综合信任度作为参照，得出该路径信任度被抬高或降低的相对程度，再通过恶意中继节点在中继路由不同阶段行为策略的对应关系，得出中继节点在数据传输采取恶意行为的可能性，即节点安全度。

以图1为例，图中存在3条路径。节点 a 对 $a2$ 和 $a3$ 所在的路径的综合信任度为 $\overline{w}_{a,t}=(w_{a,a2}\otimes w_{a2,t})\oplus(w_{a,a3}\otimes w_{a3,t})$。由于节点 a 无法知道节点 $a1$ 内部链路的信任值 $w_{a1_{in},a1_{out}}$，因此它将以 $\overline{w}_{a,t}$ 作为参照标准，来评价节点 $a1$ 所提交的路径 $a1\to t$ 的信任度。

$$w_{a,a1}\otimes w'_{a1,t}=\overline{w}_{a,t} \tag{5}$$

式中，$w'_{a1,t}$ 是作为 $w_{a1,t}$ 的参照值。利用式(3)和式(4)将式(5)展开，可以得到：

$$w'_{a1,t}=(b'_{a1,t},d'_{a1,t},u'_{a1,t}) \tag{6}$$

式中，

$$b'_{a1,t}=\overline{b}_{a,t}/b_{a,a1}$$

$$d'_{a1,t}=\overline{d}_{a,t}/b_{a,a1}$$

$$u'_{a1,t}=\overline{u}_{a,t}-d_{a,a1}-u_{a,a1}/b_{a,a1}$$

通过将 $w'_{a1,t}$ 和 $w_{a1,t}$ 相对比，可以得到中继节点 $a1$ 的安全度。其计算方式如下：

如果 $b_{a1,t}>b'_{a1,t}$，则中继节点 $a1$ 抬高路径信任度的相对程度为 p_{a1}^D，且

$$p_{a1}^D=b_{a1,t}-b'_{a1,t}/b_{a1,t} \tag{7}$$

其在数据传输阶段采取丢弃策略的概率也为 p_{a1}^D；否则，$p_{a1}^D=0$。

如果 $d_{a1,t}>d'_{a1,t}$，则中继节点 $a1$ 降低路径信任度的相对程度为 p_{a1}^N，且

$$p_{a1}^N=d_{a1,t}-d'_{a1,t}/d_{a1,t} \tag{8}$$

其在数据传输阶段采取不丢弃策略的概率也为 p_{a1}^N；否则，$p_{a1}^N=0$。

式(7)和式(8)的性质如下：当 $b_{a1,t}$ 和 $d_{a1,t}$ 趋近于 1 时，p_{a1}^D 和 p_{a1}^N 也趋向 1。这说明中继节点 $a1$ 越是抬高或降低路径信任度，其对数据传输进行恶意攻击的可能性越大，节点 $a1$ 安全度也越小。节点 $a2$ 和节点 $a3$ 安全度的计算方式与节点 $a1$ 类似。

5 基于节点安全度的多路径中继路由模型

在路径建立阶段，源节点和各个中继节点通过式(7)和式(8)的计算能够得出其下游节点的安全度，即节点采取丢弃或者不丢弃策略的概率，则式(2)所表达的最大最小问题可以转变为最大化问题，即：

$$\begin{aligned}W^*=\max_{X_s,x_l\in L} E[X_s-&\sum_{\{j\in D(i)\mid p_j^D>0\}} p_j^D x_{i,j}-\\&\sum_{\{j\in D(i)\mid p_j^N>0\}} p_j^N x_{i,j}]\end{aligned} \tag{9}$$

$$\text{s.t.}\ \sum_{i\in U(j)}(1-p_j^D)x_{i,j}=\sum_{k\in D(j)}x_{j,k},\ \forall\, p_j^D>0$$

$$\sum_{i\in U(j)}x_{i,j}=\sum_{k\in D(j)}x_{j,k},\ \forall\, p_j^N>0$$

$$0\leqslant x_{i,j}\leqslant B_{i,j}$$

式(9)所示的最大化问题可以利用线性规划的求解方式在源端节点处集中进行求解，但这需要源端节点知道所有中继节点和中继链路的信息，且计算量较大。本文先将该问题转换为最大流问题，然后在第 6 节提出分布式算法进行求解。其转换条件如下：

$$V^*=\min_{X_s,x_l\in L} E[\sum_{\{i\in D(i)\mid p_j^D>0\}} p_j^D x_{i,j}+\sum_{\{j\in D(i)\mid p_j^N>0\}} p_j^N x_{i,j}] \tag{10}$$

式中，

$$F=W^*/V^*$$

$$f_{i,j}=x_{i,j}/V^*=(x_{i,j}/W^*)F\leqslant 1/p_j^D,\ \forall\, p_j^D>0$$

$$f_{i,j}=x_{i,j}/V^*=(x_{i,j}/W^*)F\leqslant 1/p_j^N,\ \forall\, p_j^N>0$$

$$b_{i,j}=\min(B_{i,j},W^*)/V^*=\min(B_{i,j}/W^*,1)F$$

式中，F 代表到达目的端节点的所有流的大小，$f_{i,j}$ 代表链路 $l_{i,j}$ 上所经过的流。$b_{i,j}$ 体现了链路带宽 $B_{i,j}$ 对流 $f_{i,j}$ 的限制条件。将上述转换条件代入式(9)，可得最大流问题的表达式如下：

$$F^*=\max_{F,f_l\in L} F \tag{11}$$

$$\text{s.t.}\ \sum_{i\in U(j)}(1-p_j^D)f_{i,j}=\sum_{k\in D(j)}f_{j,k},\ \forall\, p_j^D>0$$

$$\sum_{i\in U(j)}f_{i,j}=\sum_{k\in D(j)}f_{j,k},\ \forall\, p_j^N>0$$

$$0\leqslant f_{i,j}\leqslant\min(b_{i,j},1/p_j^D),\ \forall\, p_j^D>0$$

$$0\leqslant f_{i,j}\leqslant\min(b_{i,j},1/p_j^N),\ \forall\, p_j^N>0$$

6 分布式多路径中继路由协议

本节针对多路径中继路由的路径建立和数据传输两个阶段，分别提出了相应的协议，从而保证了节点安全度计算和最大流问题求解的分布式实现。同时本节还对协议的复杂度进行了分析。

6.1 分布式路径建立协议

源端节点 s 发送路径搜索数据报 Req_s 后，经过 $2\times TTL$ 的时间，多路径中继路由中源端节点和各中继节点对其后续路径的综合信任度的计算都将稳定下来。各节点根据式(7)和式(8)，能够得到其下游节点的安全度；然后所提的多路径中继路由协议进入数据传输阶段。表 1 对多路径中继路由的路径建立的步骤进行了总结。

表 1 路径建立协议

Step1	当 Time=0 时，源端节点 s 发送路径搜索数据报 Req_s
Step2	中继节点 i 收到数据报 Req_s 后转发给其下游邻居节点 $j\in D(i)$
Step3	当 Time=TTL 时，目的端节点 t 将向所发现的路径 $p\in P$ 回传路径建立数据报 Ans_t^p
Step4	源端节点 s 和中继节点将根据式(3)和式(4)计算出对该节点到达目的端节点 t 所有路径的综合信任度，中继节点将继续向其上游节点回传路径建立数据报 Ans_t^p
Step5	当源端节点 s 和中继节点收到新的数据报 Ans_t^p，重复 Step4
Step6	当 Time=$2\times$TTL 时，源端节点 s 和中继节点根据式(7)和式(8)计算出其下游节点的安全度

6.2 分布式数据传输协议

在路径建立阶段，源节点和各中继节点都能通过计算得出其下游节点的安全度，同时各节点都将实时检测其出口链路带宽的使用情况。源端节点和各中继节点将在不同路径上以不同速率发送数据，使得中继节点潜在恶意行为危害达到最小，同时保证目的端节点能够获得更多正常的数据。本文在第 5 节将其转换成为最大流问题，如式(11)所示。通常，此类问题可以利用线性规划的方式在源端节点集中求解，但这样会增加源端节点的负载。文献[19]对传统的预流推送算法进行拓展，实现对最大流问题的分布式求解。本文在此基础上提出了 NSD-DPMRR 分布式数据传输协议。

6.2.1 预流推送拓展算法

预流推送算法的核心思想是源端节点将尽可能多的流向其邻居中继节点推送，然后所有中继节点也尽力将流向目的端节点推送，驻留在中继节点的流将被推送回源端节点。传统的预流推送算法中，流推送的方向是通过距离标度来导向的，即总是从距离目的端节点较远的节点向距离较近的节点的方向推送流。但当没有可用链路来推送流时，节点能够自适应地抬高自身的距离标度，以创建新的可用链路来继续推送节点处所驻留的流。

本文将把节点在路径建立阶段所得到的对后续路径信任度中不信任概率作为节点的距离标度，且源端节点 s 的距离标度 $height_s$ 为 1，目的端节点 t 的距离标度 $height_t$ 为 0。通过路径建立协议，每个中继节点 u 都将知道自身的距离标度 $height_u$ 和其下游邻居中继节点 $v\in D(u)$ 的距离标度 $height_v$。当节点 v 没有可用路径向其下游节点推送流时，它将把自身的距离标度抬高为 1，并把所驻留的流向回推送到其上游节点。

现假设链路 $l_{u,v}$ 的容量为 $cap(l_{u,v})$，该链路上的流表示为 $f(l_{u,v})$，且满足：$0\leqslant f(l_{u,v})\leqslant cap(l_{u,v})$，而该链路的剩余容量为 $r(l_{u,v})=cap(l_{u,v})-f(l_{u,v})$。节点 v 处驻留的流表示为 $excess(v)=\sum_{u\in U(v)}f(l_{u,v})-\sum_{w\in D(v)}f(l_{v,w})$。表 2 对预流推送拓展算法进行了总结。

表 2　预流推送拓展算法

Step1	节点初始化：$height_s=1$，$height_t=0$，$height_{u\in M}=d_{u,t}$，$r(l_{u,v})=cap(l_{u,v})$
Step2	源端节点 s 将 excess(s)设为其出口链路容量总和，并开始向其下游节点 $u\in D(s)$推送，且 $\delta=\min\{excess(s),r(l_{s,u})\}$，$excess(u)=\delta$，$excess(s)=excess(s)-\delta$
Step3	对于所有中继节点 $v\in M$，将驻留的流 excess(v)向其下游节点 $w\in D(v)$推送，且 $height_w<height_v$，$\delta=\min\{excess(v),r(l_{v,w})\}$，$excess(w)=excess(w)+\delta$，$excess(v)=excess(v)-\delta$
Step4	当中继节点 $v\in M$处所驻留的流 $excess(v)>0$，如果其所有满足条件 $height_w<height_v$ 的下游中继节点 $w\in D(v)$的 $r(l_{v,w})=0$，则设节点 v 的距离标度 $height_v=1$，并通知其上游节点 $u\in U(v)$
Step5	中继节点 $v\in M$将所驻留的流 excess(v)向其上游节点 $u\in U(v)$推送，且 $\delta=excess(v)$，$excess(u)=excess(u)+\delta$，$excess(v)=0$
Step6	如果所有中继节点 $v\in M$所驻留的流 $excess(v)\neq 0$，重复 Step3-Step5
Step7	当所有中继节点 $v\in M$所驻留的流 $excess(v)=0$ 时，算法停止运行，目的端节点所接收的流为最大流：$F^*=excess(t)$

当所有中继节点所驻留的流都为 0 时，预流推送拓展算法停止运行，目的端节点所收到的流即是最大流。

6.2.2　数据传输协议

本文数据传输协议将通过重复执行预流推送拓展算法并调整链路容量的方式来解决式(11)所示的最大流问题。由于本文是基于节点安全度来设计 NSD-DPMRR 协议的，因此需要对文献[19]提出的方法进行相应的修订。

协议开始时，源端节点 s 首先设定初始数据传输速率为 W，并在各路径上进行广播，各中继节点 i 设置其出口链路的容量为：

$$cap(l_{i,j})=B_{i,j} \tag{12}$$

然后，所有节点开始执行预流推送拓展算法。当预流推送拓展算法停止后，源端节点 s 实际最大发送速率为 W^*。源端节点 s 将再次设定初始最大流为 F_s，并向所有中继节点进行广播。各路径上节点 i 将其出口链路 $l_{i,j}$ 的容量更新为：

$$cap(l_{i,j})=\min(1/p_j^D,\min(B_{i,j}/W^*,1)\times F_s),\ \forall\ p_j^D>0 \tag{13}$$

式中，

$$cap(l_{i,j})=\min(1/p_j^D,\min(B_{i,j}/W^*,1)\times F_s),\ \forall\ p_j^D>0$$

$$cap(l_{i,j})=\min(1/p_j^N,\min(B_{i,j}/W^*,1)\times F_s),\ \forall\ p_j^N>0$$

考虑到本文所需解决的最大流问题中流量守恒的条件，预流推送拓展算法中节点向其下游节点所推送的流 δ 将做如下调整：

当节点 v 的下游节点 $w\in D(v)$的安全度 $p_w^D>0$ 时，根公式(11)可知，节点 w 将会将其所驻留的流 $p_w^D f_{v,w}$ 向回推送给节点 v。因此节点 v 向节点 w 推送的流 δ' 将修正为：

$$\delta'=(1-p_w^D)\times\delta=(1-p_w^D)\times\min\{excess(v),r(l_{v,w})\},\ \forall\ p_w^D>0 \tag{14}$$

当节点 $w\in D(v)$的安全度 $p_w^N>0$ 时，根据式(11)可知，节点 v 所推送的流在节点 w 处将不会驻留，因此节点 v 向节点 w 推送的流为 δ' 将不做修正：

$$\delta'=\delta=\min\{excess(v),r(l_{v,w})\},\ \forall\ p_w^N>0 \tag{15}$$

协议稳定时，源端节点的发送速率为 W^*，而各个中继节点 i 向其下游节点 j 转发的速率为 $f_{i,j}\times W^*/F^*$。表 3 对数据传输协议进行了总结。

表 3　数据传输协议

Step1	源端节点 s 向其他所有节点广播初始数据传输速率 W
Step2	所有节点 i 将按式(12)设置其出口链路 $l_{i,j}$ 的容量
Step3	所有节点执行预留推送拓展算法，源端节点 s 实际速率为 W^*
Step4	源端节点 s 向其他所有节点广播的初始最大流 F_s
Step5	所有节点 i 将按式(14)和式(15)更新其出口链路 $l_{i,j}$ 的容量
Step6	所有节点执行预留推送拓展算法，源端节点 s 得到最大流结果为 F^*，并更新 $F_s=F^*$
Step7	如果 $F^*\neq F_s$，重复 Step4－Step6
Step8	当 $F^*=F_s$ 时，开始传输数据，源端节点的发送速率为 W^*，各中继节点的转发速率为 $f_{i,j}\times W^*/F^*$

6.3　协议复杂度分析

由于提出的 NSD-DPMRR 协议中路径建立协议和数据传输协议都是以分布式的方式实现的，因此本节将从时间、通信量和计算量 3 个方面对协议的复杂度进行分析。其中，时间复杂度反映的是协议从开始执行到终止的总时延；通信复杂度反映了协议在执行过程中交换的数据报的总数量；计算复杂度表达了协议中各节点所执行算法的计算量。

6.3.1　路径建立协议的复杂度

时间复杂度：由于路径建立协议的执行时间为 TTL 时间的 2 倍，因此其时间复杂度应为 $O(2\times TTL)$。

通信复杂度：在源端节点向目的节点发送路径搜索数据报的过程中，由于每个中继节点最多将收到 $N-2$ 个路径搜索数据报，因此通信复杂度应为 $O(N-2)$。其中，N 为 P2P 网络中节点总数。在目的端节点向源端节点回送路径建立数据报时，数据报将按原路径返回，因此其通信复杂度与发送搜索数据报时相同。但考虑到存在路径信任度更新的过程，其通信复杂度的上限为 $O((N-2)\times TTL)$。由上述分析可得知，路径建立协议通信总复杂度应为 $O((N-2)\times TTL)$。

计算复杂度：节点在路径建立过程中，将利用式(3)、式(4)、式(7)和式(8)进行计算。其中节点执行式(3)和式(4)的计算量较大，其计算复杂度分别为 $O(5\times(N-2))$和 $O(13\times(N-2))$。考虑到存在路径信任度更新的过程，在路径建立阶段所各节点执行的次数将不超过 TTL 次。因此各中继节点计算复杂度的上限为 $O(18\times(N-2)\times TTL)$。

6.3.2　数据传输协议的复杂度

时间复杂度：预流推送拓展算法先将流从源端节点向目的端节点推送，目的端节点的上游节点存在将所驻留的流沿所在路径向回推送到源端节点的可能。因此，预流推送拓展算法的时间复杂度为 $O(2\times TTL-1)$。如果数据传输协议需要执行 n 次预流推送拓展算法，则其时间复杂度为 $O(2n\times TTL-n)$。

通信复杂度：预流推送拓展算法在执行前，先要将源端节点发送速率广播给所有节点，以便节点调整其出口链路的容量，其通信复杂度为 $O(N-1)$。上游节点向下游节点推送流时，发送的推送信息的通信量上限为 $O((N-2)\times TTL)$，下游节点向上游节点回推流所发送信息的上限也同样为 $O((N-2)\times TTL)$。而下游节点向上游节点发送的更新距离标度的信息上限为 $O(N-2)$。因此，预流推送拓展算法的通信复杂度为 $O(2\times(N-2)\times TTL)$。如果数据传输协议需要执行 n 次预流推送拓展算法，数据传输协议的通信复杂度为 $O(2n\times(N-2)\times TTL)$。

计算复杂度：预流推送拓展算法中，中继节点需要执行的运算包括：距离标度的对比、推送流的计算和驻留流的更新，其总的计算复杂度为 $O(3\times(N-2))$，在数据传输阶段各节点所执行的次数将不超过 TTL 次。因此，预流推送拓展算法

的计算复杂度为 $O(3\times(N-2)\times TTL)$。如果数据传输协议需要执行 n 次预流推送拓展算法，数据传输协议中各节点的计算复杂度为 $O(3n\times(N-2)\times TTL)$。

7 仿真及分析

本文将设计仿真实验来验证所提协议 NSD-DPMRR 的复杂度，并针对该协议改善数据传输性能的效果和遏制中继节点恶意行为的能力，同基于路径信任度的单路径中继路由协议进行对比分析。

7.1 仿真环境

本文利用 C 语言作为编程语言，对协议 NSD-DPMRR 进行模拟仿真。仿真中，P2P 节点总数为 50 个，各 P2P 节点的初始随机分配的邻居节点个数为 neighbornum，且各节点对其邻居节点的初始信任度随机分配。整个仿真实验将持续 100 回合，每回合内随机发起会话请求的节点个数为 requestnum，且每次会话将持续 30 回合。实验设定节点间的链路带宽在 0Mbps 到 5Mbps 间均匀分布。

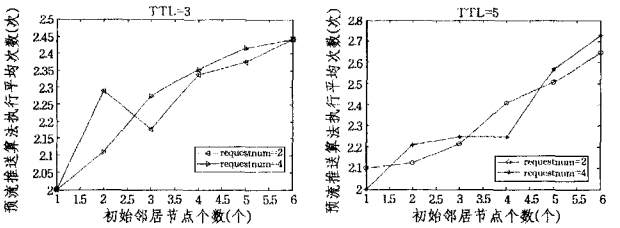
实验中，源端节点接受到服务请求后，通过路径建立协议建立起到目的端节点的多条路经。而后，源端节点和各中继节点根据数据传输协议分别得到本次中继路由中数据的最佳发送速率和转发速率。在路径建立过程中，各中继节点将随机选择其对所在路径信任度抬高或者降低的程度 p_A，且 p_A 在区间[−0.5,0.5]内均匀分布；而在数据传输阶段，各中继节点根据所选择的 p_A 对所转发的数据采取丢弃策略或者不丢弃策略。

为了检验本文所提协议 NSD-DPMRR 对数据传输性能的改善和对中继节点恶意行为的遏制，仿真实验将模拟基于路径信任的单路径中继路由协议来进行对比分析。该协议的本质为源端节点只选择路径建立阶段中信任度最高的路径进行数据传输。

7.2 结果分析

7.2.1 协议复杂度分析

由于协议 NSD-DPMRR 中数据传输阶段的复杂度主要决定于预流推送拓展算法执行的平均次数，因此本实验对其进行考察，从而验证协议 NSD-DPMRR 的复杂度。实验结果如图 2 所示。其中，图 2(a)和图 2(b)分别为 TTL 为 3 和 5 时，支持协议 NSD-DPMRR 的 P2P 节点在不同初始邻居节点个数条件下所需执行预流推送拓展算法的次数。可以看出，算法执行的次数随初始邻居节点的个数增加而上升，但其平均值保持在 3 次以内。由此可以得知，协议 NSD-DPMRR 的复杂度较低。

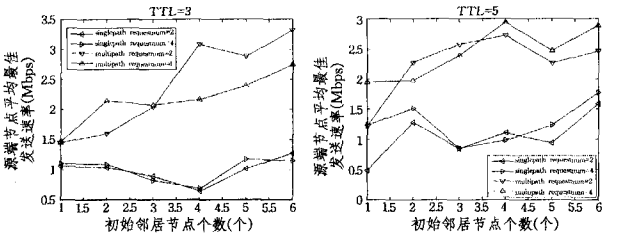


(a) TTL=3　　(b) TTL=5

图 2　预流推送拓展算法执行的平均次数

7.2.2 数据传输性能分析

本实验通过与基于路径信任的单路径中继路由协议进行对比试验，考察了多路径中继路由协议对数据传输的改善程度。实验结果如图 3 所示。其中，图 3(a)和图 3(c)分别为 TTL 为 3 和 5 时，支持协议 NSD-DPMRR 和基于路径信任的单路径中继路由协议的源端节点在不同初始邻居节点个数条件下的最佳平均发送速率。可以看出，支持两种协议的源端节点的最佳平均发送速率都随初始邻居节点个数增加而上升，且支持协议 NSD-DPMRR 的源端节点的最佳发送速率始终高于支持基于路径信任的单路径中继路由协议的源端节点。由此可以得知，采取多路径的方式能够改善数据传输的性能。

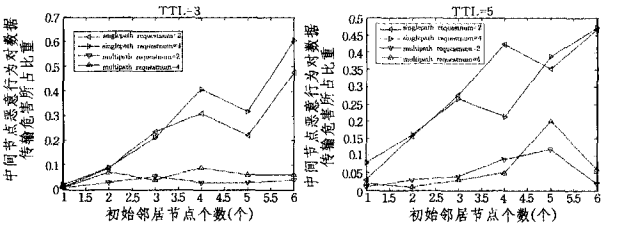


(a) TTL=3　　(b) TTL=5

图 3　源端节点平均最佳发送速率

7.2.3 恶意中继节点行为分析

本实验通过与基于路径信任的单路径中继路由协议进行对比试验，考察了多路径中继路由对中继节点恶意行为危害的遏制效果，实验结果如图 4 所示。其中，图 4(a)和图 4(c)分别为 TTL 为 3 和 5 时，支持协议 NSD-DPMRR 和基于路径信任的单路径中继路由协议的中继节点在不同初始邻居节点个数条件下对数据传输的危害占总数据流量的比重。可以看出，支持协议 NSD-DPMRR 的中继节点对数据流量危害的比重保持在 20%以内，而支持基于路径信任的单路径中继路由协议的中继节点对数据流量危害的比重最高时接近 50%。由此可以得知，本文所提协议 NSD-DPMRR 能够遏制中继节点恶意行为对数据传输的危害。



(a) TTL=3　　(b) TTL=5

图 4　中继节点恶意行为对数据传输的危害所占比重

结束语　多路径中继路由避免了网络地址转换协议 NAT 技术对 P2P 节点平等地位的破坏，同时降低了被恶意中继节点窃听和篡改的风险，增加了数据传输的安全性。而且采用多路径方式，能够减少丢包率，提高网络吞吐量，保障了数据传输的质量。本文提出了基于节点安全度的 P2P 网络分布式多路径中继路由协议 NSD-DPMRR，它在评估节点安全度的基础上，分布式计算出源端节点发送数据的最佳速率以及各中继节点的最佳转发速率，从而在实现数据传输最大化的同时，降低了恶意中继节点对数据传输的危害。由于协议中算法在各节点上分布执行，因此协议的复杂度较低。仿真实验证明了所提协议的安全性和有效性。下一步工作是将该协议嵌入到现有的 P2P 软件协议栈中，以便在实际应用中检验协议性能。

参 考 文 献

[1] Hideo Y, Nobuyuki E, Zhenlong C, et al. NAT traversal technology of reducing Load on relaying server for P2P connections[C]// 4th Annual IEEE Consumer Communications and Networking Conference. Las Vegas: Computer Society, 2007: 100-104

(下转第 64 页)

短距离通信，所提 CARQ 依然可以获得采用直接传输方式的 ARQ 的优越性。综上所述，所提 CARQ 不仅显著提高了传感器节点能量的使用效率，最大化了网络的寿命，而且为端到端的无线传输提供了有效的服务质量保障。

结束语 本文针对 WSNs 在数据传输过程中高可靠性和高能效的需求，提出了一种基于通信距离的多中继协作 ARQ 策略，以在提供有效传输可靠性的同时提高网络资源利用率。在 ARQ 机制和数据包在链路层分割为若干个数据帧的规律基础上建立了一种马尔科夫链模型，并给出了直接传输和协作传输方式下饱和吞吐率、数据包丢弃概率、平均时延和能效的分析模型，该模型能有效、准确地分析网络端到端通信性能；并在此基础上提出了一种协作 ARQ 策略。针对一种普适的线性移动无线传感器网络拓扑对所提策略与传统 ARQ 进行了性能测试，分析结果证实了所提 CARQ 相比传统 ARQ 具有更高的吞吐率、更低的数据包丢弃概率和更优的能效性能。这进一步表明，所提 CARQ 策略是一种非常适用于 WSNs 的具有高能效的可靠数据传输策略。

下一步工作是建立一种有效的测距技术，提高端到端和点到点通信距离测量的准确性和实时性；其次考虑一种能够充分考虑网络拓扑的动态变化和无线链路时变特性的协作中继选择算法；然后进一步优化发送节点和各中继节点的功能模块，降低协作 ARQ 传输数据过程的总体计算复杂度以提高其工作效率。

参 考 文 献

[1] Nosratinia A, Hunter T E, Hedayat A. Cooperative communication in wireless networks[J]. IEEE Communications Magazine, 2004, 42(10): 74-80

[2] Laneman J N, Tse D N, Wornell G W. Cooperative diversity in wireless networks: efficient protocols and outage behavior[J]. IEEE Transactions on Information Theory, 2004, 50(12): 3062-3080

[3] Elhawary M, Hass Z J. Energy-Efficient Protocol for Cooperative Networks[J]. IEEE/ACM Transactions on Networking, 2011, 19(2): 561-574

[4] 靳勇，乐德广，白光伟，等. 多跳无线传感器网络自适应链路层 FEC/ARQ 控制策略[J]. 计算机科学，2010，37(8)：114-119

[5] 张书奎，樊建席，崔志明. 无线传感器网络中可靠的数据协作传输机制[J]. 通信学报，2010，31(11)：30-40

[6] 徐文波，林家儒，牛凯，等. 多中继协作 ARQ 在 Nakagami_m 信道中的性能分析[J]. 北京邮电大学学报，2010，33(2)：74-77

[7] 孙岳，李颖，王新梅. 基于网络编码的协作 HARQ 协议[J]. 电子与信息学报，2009，31(10)：2326-2331

[8] 靳勇，乐德广，白光伟，等. 无线传感器网络跳数和通信距离自适应差错控制策略[J]. 控制理论与应用，2011，28(4)：596-600

[9] 胡映波，蔡跃明. 无线传感器网络中基于切换与保持节点选择的协同 ARQ 协议[J]. 通信学报，2010，31(11)：17-24

[10] 孟庆民，马宝萍，高西奇，等. 协同分集和截断 ARQ 在单中继无线网的使用：一种交互层研究[J]. 电子与信息学报，2007，29(11)：2593-2598

[11] 方维维，钱德沛，刘轶. 一种相邻节点协作的无线传感器网络可靠传输方案[J]. 西安交通大学学报，2009，43(2)：33-37

[12] Lee S, Su W F, Batalama S N, et al. Cooperative Decode-and-Forward ARQ Relaying: Performance Analysis and Power[J]. IEEE Transactions on Wireless Communications, 2010, 9(8): 2632-2642

[13] Harsini J S, Lahouti F, Levorato M. et al. Analysis of Non-Cooperative and Cooperative Type II Hybrid ARQ Protocols with AMC over Correlated Fading Channels[J]. IEEE Transactions on Wireless Communications, 2011, 10(3): 877-889

（上接第 59 页）

[2] Liang J, Kumar R, Ross K W. The FastTrack overlay : A measurement study[J]. Elsevier Computer Networks Journal, 2006, 50(6): 842-858

[3] Kho W, Abdul B S, Henning S. Skype relay calls: Measurements and experiments[C]// IEEE INFOCOM Workshops. Phoenix: Institute of Electrical and Electronics Engineers, 2008: 1-6

[4] 陈福，杨家海，杨扬，等. P2P/Web Service 与网格资源发现服务研究[J]. 计算机科学，2008，35(4)：16-19

[5] 苏瀚，汪芸. P2P 环境中基于信任度的服务路由系统的研究[J]. 计算机应用，2006，9(5)：230-233

[6] Lu Y, Sebastien V. Peer-to-Peer Media Steaming Application Survey[C]// Mobile Ubiquitous Computing, Systems, Services and Technologies, 2007. UBICOMM'07. 2007: 139-148

[7] Maxemchuk N. Dispersity routing [C]// International Communications Conference. 1975: 10-13

[8] Lou W, Liu W, Fang Y. SPREAD: Enhancing data confidentiality in mobile ad hoc networks[C]// Twenty-third Annual Joint Conference of the IEEE Comuter and Communications Societies. New York: Institute of Electrical and Electronics Engineers, 2004: 2404-2413

[9] Yuan L, Meng C X, Dan Y. Disjoint multi-path QoS routing in ad hoc networks[C]// International Conference on Wireless Communications, Networking and Mobile Computing. New York: IEEE, 2005: 739-742

[10] Bohacek S, Hespanha J P, Obraczka O K, et al. Enhancing security via stochastic routing[C]// Proceeding of Computer Communications and Networks, 2002. Eleventh International Conference. 2002: 58-62

[11] Brumbaugh-Smith J P, Shier D R. Minimax models for diverse routing[J]. INFORMS Journal on Computing, 2002, 14(1): 81-95

[12] 杨超，刘念祖. RepTrust：P2P 环境下基于声誉的信任模型[J]. 计算机科学，2011，38(3)：131-135

[13] 姚寒冰，胡和平，卢正鼎，等. 一种基于主观逻辑理论的 P2P 网络信任模型[J]. 计算机科学，2006，52(5)：30-35

[14] 袁禄来，曾国荪，王伟. 基于 Dempster-Shafer 证据理论的信任评估模型[J]. 武汉大学学报：理学版，2006，33(6)：29-31

[15] Georgiadis L, Georgatsos P, Floros K, et al. Lexicographically optimal balanced networks [J]. IEEE/ACM Transactions on Networking, 2002, 10(6): 818-829

[16] 毛华，毛晓亮，李斌. 网络最大流部分割矩阵算法[J]. 计算机科学，2011，38(12)：229-231

[17] Goldberg A V, Tarjan R E. A new approach to the maximum flow problem[J]. Journal of the ACM, 1988, 35(4): 921-940

[18] Lee P C, Misra V, Rubenstein D. Distributed Algorithms for Secure Multipath Routing in Attack-Resistant Networks [J]. IEEE/ACM Transactions on Networking, 2007, 15(6): 1490-1501

[19] 王浩云，张顺颐，李君. 一种基于节点主观信任度的分布式多路径路由协议[J]. 南京邮电大学学报，2009，29(1)：33-37