Journal of System Simulation

Volume 27 | Issue 12 Article 25

7-30-2020

Improved Anonymous Communication Protocol Based on Crowds

Gaofeng He
China Electric Power Research Institute, Nanjing 210009, China;

Chen Lu
China Electric Power Research Institute, Nanjing 210009, China;

Zhang Tao
China Electric Power Research Institute, Nanjing 210009, China;

Yuanyuan Ma
China Electric Power Research Institute, Nanjing 210009, China;

Improved Anonymous Communication Protocol Based on Crowds

Abstract

Abstract: The Crowds system is effective and practical, however there are two deficiencies: intermediate nodes can know receivers' identities and there is no upper bound for the route length. To address the deficiencies mentioned above, an improved anonymous communication protocol is proposed. The new protocol is based on Crowds, while it is added with more designs of Pseudo receiver and Max-Min route length. *Pseudo receivers' addresses substitutes as receivers' in packets to prevent intermediate nodes getting receivers' identities; Users can decide max and min route length to limit the route length and meet the anonymity demand*. By comparing the related data calculated under the same expected value for the route length, it is concluded that the new protocol effectively improves the degree of anonymity for users. At the same time, the new protocol is simulated and validated.

Keywords

anonymous communication, pseudo receiver, max-min route length, Crowds

Recommended Citation

He Gaofeng, Chen Lu, Zhang Tao, Ma Yuanyuan. Improved Anonymous Communication Protocol Based on Crowds[J]. Journal of System Simulation, 2015, 27(12): 3050-3056.

第 27 卷第 12 期 系统仿真学报© Vol. 27 No. 12
2015 年 12 月 Journal of System Simulation Dec., 2015

一种改进的 Crowds 匿名通信协议

何高峰，陈璐，张涛，马媛媛
（国网智能电网研究院，江苏 南京 210009）

摘要：Crowds 匿名通信系统高效、实用，但存在两个不足之处：中间节点能够知道接收者身份信息且转发路径长度随机。针对上述不足之处，提出了一种改进的匿名通信协议。新协议在 Crowds 基础上增加了伪接收者和最长最短转发路径。*报文中用伪接收者地址代替接收者地址以阻止中间节点获得接收者身份信息; 用户设定报文转发路径长度最大最小值实现转发路径长度有界性和满足一定匿名需求*。相关分析结果表明，在相同转发路径长度期望值下，新协议能有效增加用户匿名度。同时，对新协议进行了仿真验证。

关键词：匿名通信；伪接收者；最长最短转发路径；Crowds
中图分类号：TP393 文献标识码：A 文章编号：1004-731X (2015) 12-3050-07

Improved Anonymous Communication Protocol Based on Crowds

He Gaofeng, *Chen Lu*, *Zhang Tao*, *Ma Yuanyuan*
(China Electric Power Research Institute, Nanjing 210009, China)

Abstract: The Crowds system is effective and practical, however there are two deficiencies: intermediate nodes can know receivers' identities and there is no upper bound for the route length. To address the deficiencies mentioned above, an improved anonymous communication protocol is proposed. The new protocol is based on Crowds, while it is added with more designs of Pseudo receiver and Max-Min route length. *Pseudo receivers' addresses substitutes as receivers' in packets to prevent intermediate nodes getting receivers' identities; Users can decide max and min route length to limit the route length and meet the anonymity demand*. By comparing the related data calculated under the same expected value for the route length, it is concluded that the new protocol effectively improves the degree of anonymity for users. At the same time, the new protocol is simulated and validated.

Keywords: anonymous communication; pseudo receiver; max-min route length; Crowds

引言

随着 Internet 应用的发展，隐私保护已越来越受到人们的重视。人们希望自己网页浏览习惯不被别人所获知；放心使用电子货币而不能够被追查。在电子商务、电子银行、电子投票这些应用中，隐私保护已成为一项基本需求。现有的一些加密协议，如 IPSec，虽然能够保证信息内容的安全，但不能保护通信双方的实体特征，如 IP 地址，无法保证用户的隐私信息不被攻击者所获取。因此，目前有关匿名通信技术的研究已经越来越受到网络安全研究人员的重视。匿名通信技术是指通过一定的方法将业务流中的通信关系加以隐藏，使窃听者无从直接获知或推知双方的通信关系或者通信方具体信息。依据隐藏的信息对象不同，匿名保护可

收稿日期：2014-10-28 修回日期：2014-12-02;
基金项目：国家电网公司科技项目(EPRIXXKJ[2014]2244);
作者简介：何高峰(1984-)，男，安徽安庆，博士，工程师，研究方向为网络安全、机器学习；陈璐(1984-)，女，江苏丹阳，硕士，工程师，研究方向为信息安全及网络安全。

具体划分为发送者匿名、接收者匿名以及通信关系的匿名。

最早的匿名通信技术是 David Chaum 于 1981 年提出的混淆(Mix)技术[1]。在 Mix 技术的基础上，相继提出了多种改进的 Mix 技术并实现了一些实用匿名通信系统，如 Tor[2]、Web Mixes[3]、以及 Mixminion[4]等。目前，P2P 匿名通信技术已引起越来越多的关注[5-7]，并已有一系列原型系统，如 Crowds[8]、I2P[9]以及 JointCache[10]等。其中，Crowds 的最大特点是简单有效地随机转发数据从而实现匿名通信。

然而，Crowds 系统简单的随机转发使其存在两个不足之处：中间节点知道接收者身份信息与转发路径长度随机，无法实现接收者匿名且系统服务性能得不到保证。因此本文在 Crowds 的基础上提出了一种新的能够实现接收者匿名的有限路长随机转发匿名通信协议。新协议通过引入伪接收者(Pseudo Receiver)克服了 Crowds 系统中中间节点能够获知真正接收者身份信息这个不足；由用户随机指定转发路径长度最大值来解决 Crowds 系统路径长度无界问题；同时，用户可根据自身服务需求来指定转发路径长度最小值以满足一定匿名需求。新协议与 Crowds 相比能有效增加用户匿名度，满足一定服务需求，且更具灵活性和实用性。

1 相关工作

Crowds 系统的基本思想是通过混入人群来隐藏踪迹(blending into a crowd)，即在由若干用户组成的群中以随机重叠传递报文的方式来隐藏消息发送者，客户端的报文不是直接传给服务器，而是以概率 p_f 转发给群中某个成员，而发送给服务器的概率为 1-p_f。其它节点接收到报文后，采用同样的转发策略，以概率 p_f 重新进行转发，以概率 1-p_f 直接发送给服务器。在 Crowds 系统中，群内的成员被称为 jondo。

Crowds 系统的特点是简单的随机转发。简单减少了系统的开销，但也带来了一些不足之处。Crowds 系统主要的不足有：①中间节点确切知道接收者身份，无法实现接收者匿名；②系统路径长度随机，可能趋于无穷，用户无法与服务器进行正常通信，同时转发路径长度也可能为 1，用户的匿名性要求得不到满足。这些不足使得 Crowds 系统受到抗泄密性与服务质量的限制。

针对 Crowds 系统的转发路径长度可能趋于无穷的问题，文献[11-13]分别给出了不同解决办法。文献[11,13]摒弃了 Crowds 系统的随机转发而采用随机长度路径，而文献[12]则提出转发概率递减的方法。但上述文献对于转发路径长度过短和接收者匿名问题并没有给出解决方案。文献[14]针对 Crowds 接收者匿名问题，提出一种基于 IPv6 的密钥共享方法。本文提出的有限路长随机转发匿名通信协通过伪接收者解决 Crowds 系统的第一个不足，克服了文献[14]只适用 IPv6 通信协议的问题，便于实现和部署应用；对于第二个不足，提出一种由用户设定转发路径长度最大最小值的方法，报文在最大最小值之间按一定概率转发。转发路径长度最大值由用户随机设定，泄密者并不能从该值推测出发送者身份信息，克服了文献[11,13]中泄密者可根据随机路径长度等于路径长度最大值来断定其前一个节点为发送者这个缺陷。转发路径长度最小值由用户根据自身的服务需求来设定且保密，其值可固定不变。最小值并不直接保存于报文中，只需保存最大值与最小值之差。该差值可视为随机数，泄密者并不能从该值推测出发送者身份信息。

2 有限路长随机转发匿名通信协议

有限路长随机转发匿名通信协议通过伪接收者和最长最短转发路径来提升 Crowds 安全性和系统性能。其中，伪接收者由协议随机选择，而最长最短转发路径则由用户的输入确定。假定用户输入的转发路径长度为随机正整数，若不然，则可对输入的转发路径长度进行增加随机数和取整运算来保证该要求，从而确保攻击者无法依据转发路径长度来推断出用户的身份信息。

第 27 卷第 12 期 系统仿真学报 Vol. 27 No. 12
2015 年 12 月 Journal of System Simulation Dec., 2015

2.1 伪接收者

在 Crowds 系统中，中间节点确切知道接收者的身份信息。假设 Crowds 群组中共有 n 个 jondo 成员，这些成员中有 c 个泄密者。如果泄密者为转发路径上的第一个节点，则该泄密者就获得了发送者、接收者的身份信息以及它们之间的关联性。这种情形的概率为 c/n。为了阻止中间节点确切知道接收者的身份信息，降低泄密者泄密成功的概率，本文引入伪接收者概念。

伪接收者 *PR* 为群组中的任一 jondo 节点。与 Crowds 系统不同，发送者 *S* 准备发起会话时首先任意选择一 jondo 作为这次会话的 *PR*。*S* 用 *PR* 的公钥对真正接收者的地址和待发送的数据加密并将 *PR* 作为报文的接收者。报文的格式为：

$$E_{nj}\{PR \| E_{PR}\{R \| Data\}\} \quad (1)$$

其中，*R* 表示接收者，E_{nj} 与 E_{PR} 分别表示用下一个 jondo 与 *PR* 的公钥对相应内容进行加密。

为了提高加密与解密的效率，*S* 还可采用混合密钥的方式：*S* 用 *PR* 的公钥加密会话对称密钥 *K*，用 *K* 加密数据。*PR* 相应得用自己的私钥解密得到公共密钥 *K* 并用 *K* 解密数据。这时(1)式变为：

$$E_{nj}\{PR \| E_K\{R \| Data\} \| E_{PR}\{K\}\} \quad (2)$$

其中，E_K 表示用对称密钥 *K* 对数据进行加密。

当报文到达 *PR* 时，*PR* 对相应内容进行解密，并将数据发送至接收者 *R*。转发路径上的中间节点看到的接收者为 *PR*，而并非真正的接收者 *R*，只有 *PR* 知道接收者的身份信息。因此，只有转发路径的第一个节点与 *PR* 同时为泄密者时，泄密者才能确切知道发送者、接收者的身份信息以及它们之间的关联性，而这时的概率为 $(c/n)^2$。

泄密者可对 *PR* 的通信链路进行监听获得接收者 *R* 地址，但同时平均有 $O(\frac{1}{(1-P_f)^2}.(1+\frac{1}{n}))$ 个节点与其通信[8]，泄密者并不能确定与 *R* 相对应的 *S*。

2.2 最长最短转发路径

2.2.1 最长转发路径

转发路径长度定义为转发路径中间节点个数加 1，即报文所经过的跳数。Crowds 系统的转发路径长度不存在上界，且根据文献[8]，平均路径长度 $L_{\text{avg}} = p_f / (1 - p_f) + 2$，随着转发概率 p_f 增大而增长。当 p_f 为 1 时，L_{avg} 趋向无穷。转发路径增长使得网络服务延时增加，Crowds 的服务质量得到限制。为解决这个不足，本文提出由用户随机设定转发路径长度最大值。设定最大值可确保转发路径的长度不会超过该最大值，服务质量得到保证。同时该最大值为用户随机设定，泄密者并不能从该最大值来获知谁是发送者。中间节点(不包括 *PR*)在路径长度最大值范围内按概率 p_f 转发报文。设用户设定的路径长度最大值为 $L_{\max}$，报文在(2)的基础上再增加路径长度最大值项，报文格式为：

$$E_{nj}\{PR \| L_{\max} \| E_K\{R \| Data\} \| E_{PR}\{K\}\} \quad (3)$$

此时，每个中间节点的操作如图 1 所示，*PR* 则将解密后的报文发送至接收者。

每接收到一个报文，将报文中的 $L_{\max}$ 值减 1
if($L_{\max}$=2) 将报文转发给 PR
else 产生概率值 p
  if($p \leqslant p_f$) 任选一 jondo 将报文转发至该节点
  else 将报文发送给 *PR*

图 1 设定 L_{max} 时中间节点的操作

2.2.2 最短转发路径

在群组中 jondo 个数 n 和非泄密者所占的比例 p 一定的情形下，转发路径的长度必须大于某一最小值才能满足发送者 probable innocence(猜测对象比其他对象更像发起者，但猜测对象是发起者的概率不比不是发起者的概率高)。如当 n 为 10，p 为 0.85 时，最短路径长度为 4。为了保证一定的匿名度需求，用户可根据自身服务需求来设定转发路径长度的最小值 $L_{\min}$，中间节点在路径最小值与最大值之间按概率 p_f 转发报文。报文中并不需要保存

该最小值，只需保存最大值与其之差。由于最大值和最小值由用户设定，该差值可视为随机数，泄密者并不能从该值推测出发送者身份信息。设 $L_{\text{diff}} = L_{\max} - L_{\min} + 2\ (L_{\max} > L_{\min})$，报文格式为：

$$E_{nj}\{PR \| L_{\max} \| L_{\text{diff}} \| E_K\{R \| Data\} \| E_{PR}\{K\}\} \quad (4)$$

此时，每个中间节点的操作如图 2 所示。

每接收到一个报文，将报文中的 L_{max} 值减 1
if(L_{max}=2) 将报文转发给 PR
else 产生概率值 p
　if(L_{max}>L_{diff}) 将报文转发至任一 jondo
　/*满足最小值的要求*/
　else 产生概率值 p
　　if($p \le p_f$) 从 n-1 个 jondo 节点中任选一个将将报文转发至该节点
　　/*不包括 *PR**/
　　else 将报文发送给 *PR*

图 2　设定 $L_{\max}$，$L_{\min}$ 时中间节点的操作

PR 的操作如图 3 所示。

每接收到一个报文，将报文中的 L_{max} 值减 1
if(L_{max} > L_{diff}) 将报文转发至任一 jondo
else 解密报文，将数据发送给接收者 *R*

图 3　设定 $L_{\max}$，$L_{\min}$ 时 *PR* 的操作

2.2.3 转发路径长度期望值

由于设定了转发路径长度范围，转发路径期望值与设定的 $L_{\max}$，$L_{\min}$ 值以及转发概率 p_f 等有关。在仅设 $L_{\max}$ 时，计算公式为：

$$L_{avg} = (1-p_f)\sum_{l=3}^{L_{\max}-1} l p_f^{\,l-3} + L_{\max} p_f^{\,L_{\max}-3} \quad (5)$$

在同时 $L_{\max}$、$L_{\min}$ 时，计算公式为：

$$L_{avg} = (1-p_f)\sum_{l=L_{\min}}^{L_{\max}-1} l p_f^{\,l-L_{\min}} + L_{\max} p_f^{\,L_{\max}-L_{\min}} \quad (6)$$

且有 $L_{\min} \geqslant 3$。特别的，当 p_f 为 0 时，$L_{\text{avg}}=L_{\min}$；当 p_f 为 1 时，$L_{\text{avg}}=L_{\max}$。

设 $L_{\min}=4$，$L_{\max}=10$，p_f 从 0 变化至 1。仅设定转发路径长度最大值、同时设定转发路径长度最大最小值和 Crowds 系统的转发路径长度期望值变化曲线如图 4 所示。

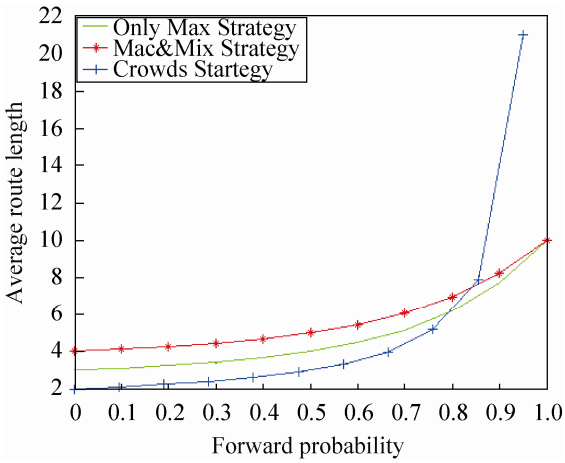

图 4　不同策略下转发路径长度期望值($L_{\max}$=10, $L_{\min}$=4)

由于设定了 $L_{\min}$ 值，在 n 为 10，p 为 0.85 时，即使转发概率 $p_f < 0.5$，仍能够满足用户的 probable innocence。而 Crowds 则要求在任何情形下都需 $p_f > 0.5$[8]，图 4 也表明了其原因。这也给系统转发概率的设定带来更多选择。

值得注意的是在仅设定转发路径长度最大值情形下，当 $p_f < 0.8$ 时，平均路径长度均大于 Crowds 系统，增强了对用户的匿名保护。

3　匿名度分析

在 Crowds 系统中，转发路径上的每个 jondo 都可以看到接收者的地址，接收者对于任何路径上的 jondo 都是暴露的。但在满足服务需求的有限路长匿名通信协议中，伪接收者地址代替了接收者地址，转发路径上的中间节点所看到的仅是 *PR* 的地址。因此对于接收者而言，满足服务需求的有限路长匿名通信协议与 Crowds 相比具有更好的抗泄密性，匿名保护得以增强。

对于发送者的匿名度分析，我们仍用 Crowds 的讨论模型。转发路径上的中间节点所知道的仅是它的前一个与后一个 jondo 节点，而它所能做的猜测是它的前一个 jondo 节点比其他任何一个 jondo 更像发送者。为了便于匿名度分析，先对一些变量做出如下定义：

第 27 卷第 12 期 系统仿真学报 Vol. 27 No. 12
2015 年 12 月 Journal of System Simulation Dec., 2015

L 表示转发路径长度的事件；

I 表示转发路径上第一个泄密者的前者确实是发送者的事件；

H_k，$1 \leqslant k \leqslant L$ 表示第一个泄密者在转发路径上占据第 k 个位置的事件，发起者的位置为 0；

$H_{k+}=H_k \vee H_{k+1} \vee H_{k+2} \vee \ldots H_L$ 代表第 k 个位置及以后有泄密者的事件；

$P(I|H_k)$表示转发路径上有泄密者的情况下，攻击者猜测正确的概率；

$p=(n-c)/n$ 表示非泄密者所占的比例。

第 1 个泄密者占据转发路径上第 i 个位置的概率为：

$$P(H_i)=\left(\frac{n-c}{n}\right)^{i-1}\frac{c}{n}=p^{i-1}(1-p) \tag{7}$$

第 1 个泄密者位于转发路径上第 2 个或以后位置的概率为：

$$P(H_{2+})=\sum_{k=2}^{L}P(H_i)=\sum_{k=2}^{L}p^{i-1}(1-p)=p-p^L \tag{8}$$

第 1 个泄密者位于转发路径上第 1 个或以后位置的概率为：

$$P(H_{1+})=\sum_{k=1}^{L}P(H_i)=\sum_{k=1}^{L}p^{i-1}(1-p)=1-p^L \tag{9}$$

因为 $P(I|H_{1+})=1$，$P(I|H_{2+})=1/(n-c)$，有：

$$P(I)=P(H_1)P(I|H_1)+P(H_{2+})P(I|H_{2+})=\frac{c}{n}+(p-p^L)\frac{1}{n-c}=1-p+(p-p^L)\frac{1}{np} \tag{10}$$

$$P(I|H_{1+})=\frac{P(I\wedge H_{1+})}{P(H_{1+})}=\frac{P(I)}{P(H_{1+})}=\frac{1-p+(1-p^{L-1})\frac{1}{n}}{1-p^L} \tag{11}$$

而根据文献[13]，在 Crowds 系统中，有

$$P(I|H_{1+})=\frac{n-p_f(n-c-1)}{n}=1-p_f\left(p-\frac{1}{n}\right) \tag{12}$$

在用户环境(n，p)相同和转发路径长度期望值相等的情形下，新协议与 Crowds 系统的匿名度比较如表 1 所示，其中(12)式中的 p_f 由 Crowds 系统的平均路径长度计算公式求出。

表 1 表明，与 Crowds 相比，在转发路径长度期望值相等的情况下，新协议能够有效降低泄密者成功猜测发送者的概率，增加用户匿名度。从表 1 还可得知：①随着泄密者所占的比例增加(p 减小)，泄密者成功猜测发送者的概率增加；②随着转发路径长度的增加，泄密者成功猜测发送者的概率降低。这同时也符合已有的研究结论[12-13]。

表 1 固定 n 的取值，p 可变，还可以固定 p，n 可变。如在转发路径长度期望值为 4 的情形下，n=70，p=0.60，式(11)等于 0.472，(12)式等于 0.561；n=80，p=0.60 时，(11)式等于 0.471，(12)式等于 0.559。由于篇幅限制，本文省略了与表 1 类似的计算结果表。其它计算结果同样支持由表 1 所得出的结论，同时还表明随着 n 增加(p 固定)，泄密者成功猜测发送者的概率降低。

表 1 在用户环境转发路径长度期望值相等的情形下，有限路长匿名通信协议与 Crowds 系统匿名度比较

用户环境	转发路径长度期望值													
	4		5		6		7		8		9		10	
	(11)	(12)	(11)	(12)	(11)	(12)	(11)	(12)	(11)	(12)	(11)	(12)	(11)	(12)
60*0.85	0.33	0.44	0.28	0.37	0.26	0.33	0.23	0.31	0.22	0.29	0.21	0.27	0.20	0.26
60*0.80	0.35	0.48	0.31	0.41	0.29	0.37	0.27	0.35	0.26	0.33	0.25	0.31	0.24	0.30
60*0.75	0.38	0.51	0.34	0.45	0.32	0.41	0.30	0.39	0.29	0.37	0.29	0.36	0.28	0.35
60*0.70	0.40	0.54	0.38	0.49	0.36	0.45	0.34	0.43	0.33	0.41	0.33	0.40	0.33	0.39
60*0.65	0.44	0.58	0.41	0.53	0.39	0.49	0.38	0.47	0.38	0.46	0.37	0.45	0.37	0.44
60*0.60	0.47	0.61	0.45	0.56	0.44	0.53	0.43	0.51	0.42	0.50	0.42	0.49	0.42	0.48

注：第 1 列为用户环境，*号前为 n，*号后为 p；(11)，(12)分别表示公式(11)，(12)。

4 仿真实验

本文利用 PeerSim[15]进行仿真模拟实验。PeerSim 是意大利博洛尼亚大学开发的基于生物启发技术的 P2P 模拟器，模拟的节点个数可达 1,000,000 并支持节点任意上下线，能较好模拟真实的 P2P 环境。PeerSim 既提供周期驱动的模拟又提供离散事件的模拟。本文的模拟实验为周期驱动模拟，节点个数为 1024。实验中省略了 Crowds 中的 Blender 服务器，而采用由节点自身维护其它所有节点信息的方式，这并不影响实验结果。

实验中转发概率 p_f 以 0.01 递增。对每一转发概率，均运行 5 000 轮以求该转发概率下的转发路径长度期望值，实验结果如图 5 所示。实验结果与理论分析(图 4)保持了很好的一致性，验证了新协议的正确性。

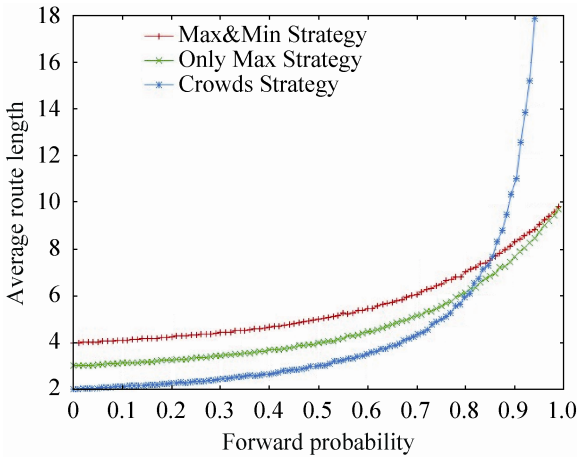

图 5 不同策略下转发路径长度期望值(L_{max}=10, L_{min}=4)

我们还对节点负载进行了仿真实验。与文献[8]相同，定义节点被选择的次数为这个节点的负载，节点负载主要与转发概率相关。不同策略下节点负载如图 6 所示。

当转发概率低于 0.9 时，3 种策略下节点负载基本相同。当转发概率大于 0.9 时，由于设定了 L_{max} 值，新协议中节点的负载并没有大幅提升，这减轻了节点的负载。

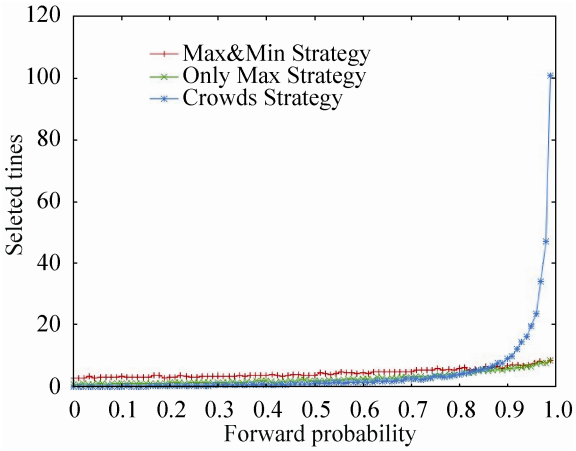

图 6 不同策略下节点的负载(L_{max}=10, L_{min}=4)

节点负载的降低减少了资源消耗，但同时给攻击者对匿名系统的攻击(如流量分析)带来便利。实验中我们发现增大 L_{min} 的值可增加节点负载，实验结果如图 7 所示。这是因为在 L_{min} 值范围内，节点以概率 1 转发。L_{min} 值越大，转发的次数越多，增加了节点负载。利用这个性质，可以设定合适的 L_{min} 与 L_{max} 值以达到系统性能与安全性的平衡。

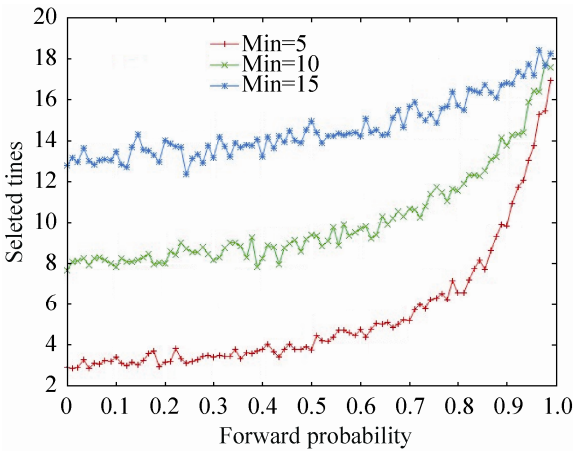

图 7 增大 L_{min} 值可增加节点的负载(L_{max}=20)

5 结论

本文针对 Crowds 的两个不足之处进行了改进，提出一种新的有限路长随机转发匿名通信协议。新协议通过伪接收者阻止了中间节点获得接收者身份信息，而由用户设定转发路径长度最大最小值克服了 Crowds 系统转发路径长度无上界并且提升了匿名保护强度。计算分析表明，新协议能有效

第 27 卷第 12 期 系统仿真学报 Vol. 27 No. 12
2015 年 12 月 Journal of System Simulation Dec., 2015

增加用户的匿名度，满足特定服务需求。同时，泄密者并不能从报文中的最大值与差值推测出发送者身份信息。这些均使得新协议更加实用。

参考文献：

[1] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms [J]. Communication of the ACM (S0001-0782), 1981, 24(2): 84-88.

[2] Dingledine R, Mathewson N, Syverson P. Tor: The second-generation onion router, Proc of 13th USENIX Security Symposium, San Diego, CA, USA, 2004. [C/OL]. (2004-05-18) [2014-9-13]. http://tor.eff.org/tor-design.pdf.

[3] Berthold O, Federrath H, Kopsell S. Web MIXes: A system for anonymous and unobservable Internet access [C]// Proc of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009. Germany: Springer-Verlag, 2000: 115-129.

[4] Danezis G, Dingledine R, Mathewson N. Mixminion: Design of a type III anonymous remailer protocol [C]// Proc of the 2003 IEEE Symposium on Security and Privacy. USA: IEEE, May 2003: 2-15.

[5] Rao S, Priya D D. Cooperative Caching in Wireless P2P Networks: Design, Implementation and Evaluation [J]. International Journal of Research in Computer and Communication Technology (S2248-9622), 2013, 2(10): 915-919.

[6] Jia J, Zhang F. Twice Anonymity Algorithm for LBS in Mobile P2P Environment [J]. Journal of Computational Information Systems, 2013, 9(9): 3715-3722.

[7] Sabra Z, Artail H. Preserving anonymity and quality of service for VoIP applications over hybrid networks [C]// 2014 17th IEEE Mediterranean Electrotechnical Conference (MELECON). USA: IEEE, 2014: 421-425.

[8] Reiter M K, Rubin A D. Crowds: Anonymity for web transactions [J]. ACM Transaction on Information and System Security (S1094-9224), 1998, 1(1): 66-92.

[9] Herrmann M, Grothoff C. Privacy-implications of performance-based peer selection by onion-routers: a real-world case study using I2P [C]// Privacy Enhancing Technologies. Germany: Springer Berlin Heidelberg, 2011: 155-174.

[10] Dong K, Gu T, Tao X, *et al*. JointCache: Collaborative path confusion through lightweight P2P communication [C]// 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). USA: IEEE, 2013: 352-355.

[11] Memon I, Domenic K, Memon H, *et al*. Rumor Riding: An anonymity approach for decentralized peer to peer systems [J]. Wireless Personal Communications (S0929-6212), 2014, 79(1): 647-660.

[12] 睦红飞, 陈松乔, 陈建二. Crowds 系统中基于递减转发概率的路长控制策略 [J]. 小型微型计算机系统, 2005, 26(3): 557-391.

[13] 王伟平, 陈建二, 王建新, 等. 基于群组的有限路长匿名通信协议 [J]. 计算机研究与发展, 2003, 40(4): 609-614.

[14] Xu J, Wang Z X, Zhang L C, *et al*. Recipient anonymity: An improved Crowds protocol based on key sharing [C]// Proc of WASE International Conference on Information Engineering, Beidaihe, China. USA: IEEE, 2010: 60-64.

[15] Jelasity M, Montresor A, Jesi G P, *et al*. PeerSim: A Peer-to-Peer Simulator [EB/OL]. (2014-05-29) [2014-09-13]. http://peersim.sourceforge.net, 2014.