基于重路由匿名通信系统的负载分析*

眭鸿飞+, 陈松乔, 陈建二, 王建新, 王伟平

(中南大学 信息科学与工程学院,湖南 长沙 410083)

Payload Analysis of Rerouting-Based Anonymous Communication Systems

SUI Hong-Fei+, CHEN Song-Qiao, CHEN Jian-Er, WANG Jian-Xin, WANG Wei-Ping

(School of Information Science and Engineering, Central South University, Changsha 410083, China)

+ Corresponding author: Phn: +86-731-8830212, E-mail: hfsuicn@hotmail.com, http://sise.csu.edu.cn/cise/

Received 2002-12-04; Accepted 2003-06-23

Sui HF, Chen SQ, Chen JE, Wang JX, Wang WP. Payload analysis of rerouting-based anonymous communication systems. *Journal of Software*, 2004,15(2):278~285.

http://www.jos.org.cn/1000-9825/15/278.htm

Abstract: Rerouting mechanism is adopted by rerouting-based anonymous communication systems such as Mixes, Onion Routing, and Crowds, to store and forward data in application layer. With this, users can communicate in an indirect way. Thus, identity information such as IP addresses can be effectively hidden against eavesdropper. This mechanism, however, can result in extra overhead in performance such as communication delay and participant payload, which may affect the applications of anonymous communication systems. In this paper, the participant payload induced by the rerouting mechanism is studied quantitatively. By investigating the establishment of rerouting paths in detail, a probability formula for calculating the participant payload is derived, which proves that the participant payload is determined by the number of participants, the number of rerouting paths, and the probability distribution of length of the rerouting paths. By applying this formula to a practical anonymous communication system, Crowds, a precise expected participant payload $1/(1-p_f)+1$ can be derived, which significantly improves Reiter and Rubin's original analysis $O((n+1)/((1-p_f)^2 n))$, and demonstrates that the participant payload in Crowds remains constant and is independent of the variation of the number of participants in Crowds. Simulation results are presented to testify the theoretical analysis. The conclusions can provide a theoretical support for the design and implementation of anonymous communication systems.

Key words: network security; information hiding; anonymous communication

摘 要: 基于重路由匿名通信系统,如 Mixes, Onion Routing, Crowds 等,采用重路由机制在应用层转发数据,使实体之间的通信以间接的方式进行,从而有效地隐藏通信实体的身份信息,如主机的 IP 地址等.在性能方面,这种机制

* Supported by the National Natural Science Foundation of China under Grant No.90104028 (国家自然科学基金); the National Science Foundation for Distinguished Young Scholars of China under Grant No.69928201 (国家杰出青年科学基金)

作者简介: **眭鸿飞**(1973－),男,湖南衡阳人,博士生,主要研究领域为网络安全,信息隐藏;**陈松乔**(1941－),男,教授,博士生导师,主要研究领域为软件工程;**陈建二**(1954－),男,教授,博士生导师,主要研究领域为计算机网络,优化理论;**王建新**(1969－),男,博士,副教授,主要研究领域为计算机网络;**王伟平**(1969－),女,博士生,副教授,主要研究领域为网络安全,信息隐藏.

导致系统中产生额外的开销,如通信延时、负载等.着重从理论上分析了系统中的成员负载.通过深入考查基于重路由匿名通信系统的重路由机制,推导出了基于重路由匿名通信系统中成员负载的概率公式,证明了成员负载由系统中成员数目重路由路径数目以及重路由路径长度的概率分布所决定.应用该公式计算 Crowds 系统中成员的负载,得出精确的负载期望值为 $1/(1-p_f)+1$,改进了 Reiter 等人的分析结果 $O((n+1)/((1-p_f)^2 n))$,证明了 Crowds 系统的成员负载不受系统中成员数目 n 的影响,具有良好的可伸缩性.并通过仿真实验验证了该分析结果.其结论为设计和规划匿名网络提供了理论依据.

关键词: 网络安全;信息隐藏;匿名通信

中图法分类号: TP393 **文献标识码**: A

Internet 作为通信与信息传播的工具,正快速发展并且广为人们所接受.其中的安全与隐私问题也越来越突出.在一些应用中,如电子投票(e-voting)、电子银行(e-banking)、电子商务(e-commerce),保护用户的隐私信息已成为一种基本需求.匿名通信主要保护网络应用中通信实体的身份标识,如通信者的 IP 地址等,使其无法为外部观察者获知.匿名保护的形式有 3 种:发送方匿名(sender anonymity),即报文无法被关联到其发送者;接收方匿名(recipient anonymity),即报文无法被关联到其接收者;通信关系匿名(relationship anonymity),即无法关联报文的发送者与接收者[1].目前的研究主要集中在发送方匿名服务方面.

目前已有的匿名通信系统包括 DC-Net[2,3],Mixes[4,5],Anonymous Remailer[6],LPWA[7],Onion Routing I[8~11],Onion Routing II[11],Crowds[12]以及 Hordes[13]等.这些系统均采用重路由机制(rerouting)与/或通信流填充机制(padding),以提供匿名保护[14].重路由机制是一种应用层路由机制.它为用户提供间接通信.包含在一次通信中的多个主机在应用层存储转发数据,从而形成一条由多个安全信道组成的虚拟路径,称为重路由路径(rerouting path).从安全信道上传送的 IP 数据包首部,外部攻击者无法获得真实的发送者和/或接收者的 IP 地址信息.因而,通信实体的身份信息被有效地隐藏.基于重路由的匿名通信系统通常提供发送者匿名和通信关系匿名服务.例如,Mixes 隐藏邮件发送者的身份信息.Onion Routing 隐藏实时通信中通信实体之间的通信关系.Crowds 则保护 Web 浏览用户的身份信息,使其不被正在浏览的 Web 站点利用.

重路由机制的引入导致在系统性能,如通信延时、成员负载方面产生额外的开销.必须从理论上对系统性能进行定量分析,以便于在实际应用中作出权衡.Guan 等人采用信息熵作为匿名性度量,探讨了匿名通信系统的匿名性与重路由路径长度的关系,隐含地给出了匿名性与通信延时的关系[14].Reiter 等人计算了 Crowds 系统中成员负载的近似值[12].Wright 等人比较了几种主要匿名通信系统的匿名性及性能[15].Wang 等人则提出了一种改进的重路由算法,以限制重路由路径的长度,降低通信延时[16].本文分析了基于重路由匿名通信系统中的成员负载.推导出了成员负载的概率计算公式.将该公式与 Crowd 系统中的重路由策略相结合,精确地计算出了 Crowds 系统中成员负载的数学期望值,并通过仿真系统对该结果进行了验证.

1 基于重路由的匿名通信系统[14]

Guan 等人建立了基于重路由匿名通信系统模型[14].为了便于讨论,本节给出该模型的简要描述,并引入一些新的概念.

1.1 系统模型

基于重路由的匿名通信系统可被视为一个多代理通信系统,通信数据经过多个代理存储转发至接收者,以达到匿名保护的目的.我们的讨论将主要针对发送者匿名形式的保护,关系匿名与此类似.一个基于重路由的匿名通信系统是由网络中若干个提供匿名服务的主机组成的集合,设为 $V=\{v_j|0\le j<n\}$,其中的主机 v_j 称为成员(participant),系统中成员数为 $|V|=n(n\ge 1)$.在系统运行期的某一间隔时间内,如 1 小时,成员数目 n 固定为一个常数.通过安全通信信道,两两成员之间可进行直接通信.需要匿名通信服务的用户选择一个成员 $s\in V$ 作为其代理成员,并将接收者地址传送给该代理成员.由该代理成员发起建立一条由多个成员组成的到达接收者的重路由路径,以用于用户和接收者之间的间接通信.形式化地,一条重路由路径 Γ 可以表示为

$$\langle s,I_1,I_2,...,I_t,...,I_L,r\rangle,$$

其中,$s\in V$ 称为通信的发送者(sender),$r\notin V$ 为通信的接收者(recipient),$I_t(I_t\in V,1\le t\le L)$为中继节点(intermediator). $L(L=1,2,...)$为重路由路径所经过的中继结点数目,称为路径长度.L 为独立的离散随机变量,服从概率分布:

$$\Pr\{L=k\}=f(k),\ 0\le f(k)\le 1,\sum_{k=1}^{\infty}f(k)=1,k=1,2,...$$

在一个运行周期内,系统中将建立多条重路由路径.重路由路径一经建立,将被保持至该周期内结束.令 P (P=1,2,...)为重路由路径的数目.某成员在一条转发路径上的一次出现称为一个转发任务.成员负载(participant payload)为单个成员 v_j 所承担的转发任务总数,也即 v_j 在所有重路由路径上作为中继结点出现的总次数[15],记为 F_j.如图 1 所示为一个基于重路由匿名通信系统.可以看到,系统中成员数目 n=16,重路由路径数 P=2,重路由路径分别为 $\Gamma_1=\langle 0,5,2,7,11,8,r_1\rangle$和 $\Gamma_2=\langle 5,10,3,9,r_2\rangle$.其中,成员 0 与 5 分别为 Γ_1,Γ_2 的发送者,路径长度分别为 L_1=5 和 L_2=3.成员 10 在系统的重路由路径上出现 1 次,承担 1 个转发任务,故其负载 F_{10}=1.成员 5 在两条重路由路径上出现两次,但作为中继成员只承担 1 个转发任务,故其负载 F_5=1.需要引起特别注意的是,Reiter[12]等人将发送者自身看作是重路由路径上第 1 个中继结点,在下文中我们将看到,这导致成员负载的计算结果有稍许差异.

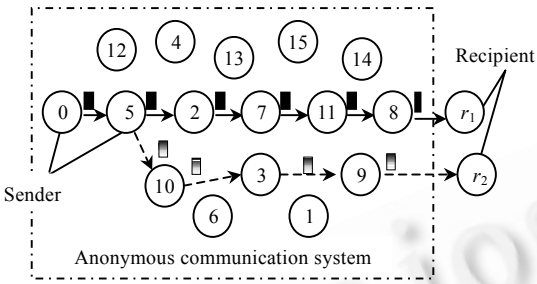

Fig.1 Rerouting-Based anonymous communication system

图 1 基于重路由匿名通信系统

1.2 重路由算法

在建立重路由路径时,有几个问题需要考虑.如图 2 所示,重路由算法通常包含两步:确定重路由路径的长度,所采用的策略称为路长控制策略(length control strategy);选定路径上中继结点序列,所采用的策略称为成员选择策略(member selection strategy).在实际匿名通信系统的重路由算法中,并非每个步骤都会显式地出现.例如,在 Onion Routing I 中,重路由路径的长度为一个常数值,则路长选择被省略.

Input: s, r: Sender, Recipient
1. Determine the length of rerouting path L;
2. Choose intermediators $I_1,I_2,\ldots,I_L$;
3. Return the rerouting $path\langle s,I_1,I_2,...,I_L,r\rangle$;

Fig.2 Rerouting algorithm

图 2 重路由算法

路长控制策略有两种:定长策略(fixed length strategy)与变长策略(variable length strategy).在定长策略下,产生的重路由路径的长度恒定为某常数 C,路径长度 L 的概率分布为

$$\Pr\{L=k\}=f(k)=\begin{cases}1, & k=C\\ 0, & k\ne C,\end{cases}\quad k=1,2,...$$

Onion Routing I 与 Freedom 中采用的是定长策略.与此相反,变长策略下,路径长度 L 为服从某一概率分布的离散随机变量.这种策略在 Crowds 与 Onion Routing II 中被采用.本文主要讨论变长策略的情况,定长策略则被视为变长策略的一种特例.

用于成员选择的策略也可分为两种:随机策略(randomized strategy)与非随机策略(non-randomized strategy).随机策略较为简单,从系统 n 个成员(包括发送者自身)随机选取作为重路由路径上的中继结点,这样产生的重路由路径有可能出现环.非随机策略则根据已有负载、可信任程度或运行可靠性等参数选取符合给定条件的结点.目前主要的基于重路由匿名通信系统,如 Crowds, Onion Routing II 等采用的是随机策略,我们将主要针对这种情况加以讨论.

2 负载分析

这一节我们考察基于重路由匿名通信系统的成员负载.如上文所述,基于重路由匿名通信系统中某成员上的负载 F,主要计算该成员在所有重路由路径上的出现次数.设在某一运行周期,系统中含有 n 个成员

(n=1,2,...),P 条重路由路径(P=1,2,...),Γ_m 为第 m($1\le m\le P$)条重路由路径,其长度$\{L_m\}$为离散型随机变量,$\{L_m\}$独立同分布,且服从分布律:

$$\Pr\{L_m=k\}=f(k),(0\le f(k)\le 1,\sum_{k=1}^{\infty}f(k)=1,k=1,2,...,\infty) \tag{1}$$

考察系统中任意一个成员 v_j.令 F_j 为成员 v_j 所承担的负载,R_j 为 v_j 在系统中所有重路由路径上作为中继结点出现的次数,R_j^m 为成员 v_j 在第 m 条重路由路径 Γ_m 上出现的次数,则

$$F_j=R_j=\sum_{m=1}^{P}R_j^m \tag{2}$$

由式(1)可以得到重路由路径 Γ_m 的长度的数学期望值 $E(L_m)$:

$$E(L_m)=\sum_{k=1}^{\infty}k\Pr\{L_m=k\}=\sum_{k=1}^{\infty}kf(k) \tag{3}$$

当采用随机策略构造重路由路径时,充当路径上中继结点的成员为从系统中 n 个成员中随机抽取,可以得出重路由路径 Γ_m 长度为 k 时成员 v_j 在该路径上出现 i(i=0,1,2,...,k)次的条件概率:

$$\Pr\{R_j^m=i|L_m=k\}=C_k^i\left(\frac{1}{n}\right)^i\left(\frac{n-1}{n}\right)^{k-i},i=0,1,2,...k \tag{4}$$

由式(1)和式(4)可以得到重路由路径 Γ_m 长度为 k,且在该路径上成员 v_j 出现 i 次的概率为

$$\begin{aligned}\Pr\{R_j^m=i,L_m=k\}&=\Pr\{L_m=k\}\Pr\{R_j^m=i|L_j=k\}\\&=f(k)C_k^i\left(\frac{1}{n}\right)^i\left(\frac{n-1}{n}\right)^{k-i}\end{aligned} \tag{5}$$

由于第 m 条重路由路径长度 L_m 为 k(k=1,2,...)的事件两两不相容,根据全概率公式,可以得出成员 v_j 在 Γ_m 上出现 i 次的概率:

$$\begin{aligned}\Pr\{R_j^m=i\}&=\Pr\{R_j^m=i,L_m=1\}+\Pr\{R_j^m=i,L_m=2\}+...+\Pr\{R_j^m=i,L_m=\infty\}\\&=\sum_{k=1}^{\infty}\Pr\{R_j^m=i,L_m=k\}\\&=\begin{cases}\sum_{k=1}^{\infty}f(k)\left(\frac{n-1}{n}\right)^k, & i=0\\ \sum_{k=i}^{\infty}f(k)C_k^i\left(\frac{1}{n}\right)^i\left(\frac{n-1}{n}\right)^{k-i}, & i\ge 1\end{cases}\end{aligned} \tag{6}$$

由式(2)、式(3)和式(6),可以得到下面的基于重路由匿名系统中成员负载概率公式的定理.

定理 1. 在基于重路由匿名通信系统中,在某一运行周期,系统中有 n(n=1,2,...)个成员,P(P=1,2,...)条重路由路径,第 m($1\le m\le P$)条重路由路径的长度为$\{L_m\}$,$\{L_m\}$为离散型随机变量且独立同分布,服从分布律:

$$\Pr\{L_m=k\}=f(k),(0\le f(k)\le 1,\sum_{k=1}^{\infty}f(k)=1,k=1,2,...,\infty).$$

若系统构造重路由路径时采用随机策略选择中继结点,则系统中任一成员 v_j($0\le j<n$)个成员的负载 F_j 的数学期望值为

$$E(F_j)=\left(\frac{P}{n}\right)E(L_m) \tag{7}$$

其中 $E(L_m)$为重路由路径的长度的数学期望值.

证明详见附录.

由定理 1 可知,在基于重路由匿名通信系统中,在某一运行周期,成员负载由该时刻系统中成员数目 n、重路由路径数 P 以及重路由路径长度的数学期望值 $E(L_m)$所决定.由于重路由路径长度的概率分布系统运行前就已确定,系统运行期间,$E(L_m)$恒定为常数,F_j 将主要取决于 n 与 P.当提供匿名服务的成员数目 n 通常只能有限增

长的情况下,倘若 P 的增长不受限制,则将导致成员因负载过重而降低转发效率乃至崩溃.因此,在具体应用时应当采用相应的机制对重路由路径数目 P 进行限制.下文我们会看到,Crowds 正是通过一定的机制使 $P=n$,系统中负载期望为与 n 及 P 无关的常数,因而系统具有良好的可扩展性.

3 Crowds 系统的成员负载分析

本节我们将应用上一节的定理来分析 Crowds 中成员的负载情况.由于 Onion Routing II 中采用的选路策略与 Crowds 相同,故 Crowds 的分析结果同样适用于 Onion Routing II.

Crowds[12]是一种基于重路由匿名通信系统,为 Web 浏览用户提供发送者匿名形式的保护.需要匿名保护的主机必须加入系统成为成员,在被保护的同时提供匿名服务.当成员需要发起一次匿名通信时,将请求转发给其他成员.其他成员将该请求继续转发或直接提交.具体说来,系统中每个成员上运行一个名为 Jondo 的代理程序,用于转发源自于本地浏览器或其他成员上 Jondo 的 HTTP 请求.初始时,Jondo 向系统中行使管理功能的成员 Blender 注册,并获得系统中的活动 Jondo 表及相应的密钥.当收到来自本地浏览器的 HTTP 请求时,Jondo 从 Jondo 表中随机选取一个作为后继,并将请求转发给该后继 Jondo.当后继 Jondo 获得请求,以概率 $p_f(1/2\le p_f<1)$ 将请求继续转发,否则将请求直接提交给接收者,从而形成一条由 Jondo 组成的重路由路径.后续的来自本地浏览器的请求将沿该重路由路径转发.在如图 3 所示的 Crowds 系统中,$n=6,P=6$,重路由路径分别为 ⟨1,5,server1⟩;⟨2,0,2,server2⟩;⟨3,1,0,server3⟩; ⟨4,4,server4⟩;⟨5,4,0,server1⟩;⟨0,3,server2⟩.

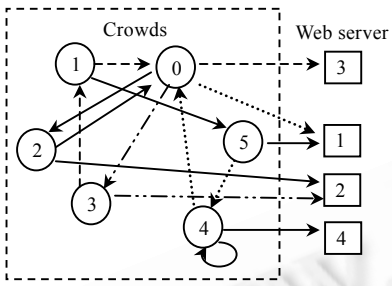

Fig.3 Crowds system
图 3 Crowds 系统

可以看到,Crowds 中采用变长策略控制路长,采用随机策略选取中继结点.系统运行以后,为每个成员形成的重路由路径数目不多于 1 条,故 $P\le n$,满负荷运行时有 $P=n$.由于重路由路径长度的概率分布为

$$\Pr\{L_m=k\}=f(k)=(1-p_f)p_f^{\,k-1},\ \frac{1}{2}\le p_f<1,k=1,2,... \tag{8}$$

则可以得到重路由路径长度的数学期望:

$$E(L_m)=\frac{1}{1-p_f},\left(\frac{1}{2}\le p_f<1\right) \tag{9}$$

又 $P=n$,由定理 1 可得成员 v_j 上负载期望值 $E(F_j)$:

$$E(F_j)=\left(\frac{P}{n}\right)E(L_m)=E(L_m)=\frac{1}{1-p_f} \tag{10}$$

需要注意的是,Reiter[12]将发送者作为中继结点计入重路由路径长度,由于成员 v_j 在所有 n 条重路由路径上作为发送者只出现一次,则可以得到 Reiter 定义下 Crowds 中成员负载数学期望值为 $1/(1-p_f)+1$.文献[12]中的定理 7.1 给出了结点负载数学期望值的上界为 $2n/(n-1)(1-p_f)^2$.将两种分析结果进行比较,可以看到,本文的分析给出了精确的负载期望值,改进了 Reiter 的分析结果.

为了进一步验证该分析结果,我们模拟了 Crowds 系统的运行,测试了成员的负载,计算出负载均值 F_a.在模拟运行时,以时间 t 为一个运行周期,每个周期内为系统中每个结点产生一条重路由路径,共为 n 条.针对 n 或 p_f 的不同取值,运行 100 000 个周期,记录每个运行周期内某结点 v_j 的负载并求均值,得到负载均值 F_a 随 n,P 变化的曲线如图 4 和图 5 所示.为了便于对照,我们在图中同时给出了根据 Reiter 分析的负载期望上界值 $2n/(n-1)(1-p_f)^2$ 以及由本文得出的负载期望 $1/(1-p_f)+1$ 计算出的结果得到的曲线.由图 4 中可以看到,$p_f=0.8$,当 n 增大时,负载均值 F_a 为水平直线,与本文分析得到的 $E(F)=6$ 基本重合,远远低于 Reiter 的负载期望上界.从图 5 可以看到,$n=60$,当 p_f 增大时,负载均值 F_a 与本文分析得到的负载期望曲线基本一致,为一条缓慢趋近于无穷大的曲线,其增长趋势远低于 Reiter 的负载期望上界值.因此,本文对 Crowds 的负载分析是正确的,对于 Reiter 的结论作出了较大改进,从另一个方面也验证了定理 1 的正确性.

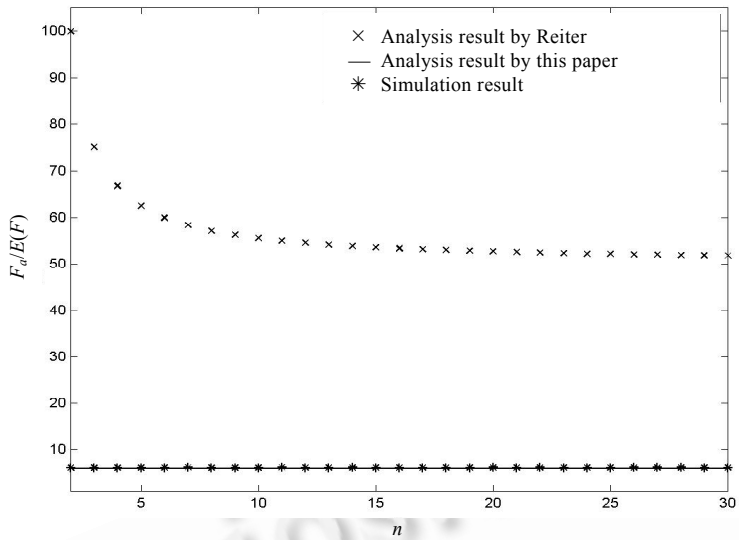

Fig.4 Average payload F_a/expected payload $E(F)$ vs. Number of participant n (p_f=0.8)

图 4 负载均值 F_a/负载期望 $E(F)$ vs. 结点数 n (p_f=0.8)

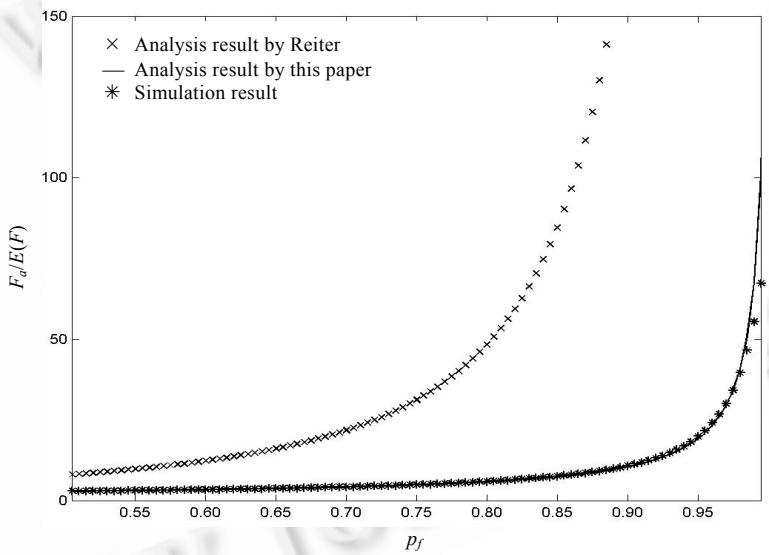

Fig.5 Average payload F_a/expected payload $E(F)$ vs. probability of forwarding p_f (n=60)

图 5 负载均值 F_a/负载期望 $E(F)$ vs. 转发概率 p_f (n=60)

此外,我们还可以得出以下结论:首先,Crowds 系统消除了系统中成员数目 n 以及重路由路径数目 P 的变化对成员负载 F 产生的影响.由于 Crowds 采用一定的机制使重路由路径数目 P 成为系统中成员数目 n 的线性函数,负载期望值 $E(F)$简化为 p_f的函数.在系统运行期间,p_f为一个恒定的常数,因此成员的负载期望也为常数.这意味着,当系统满负荷运行时,系统中成员数目的动态变化不会导致系统中成员负载发生变化.系统中成员数目的增加不受系统中成员负载的瓶颈限制,具有良好的可伸缩性.其次,Crowds 系统中成员的平均负载由转发概率 p_f 所惟一决定.当增大 p_f 时,重路由路径变长,将导致成员负载增加以及转发请求中的延时增大.因此,在实际应用时应当对 p_f的取值进行仔细斟酌,以获得较好的系统性能.

4 结 语

本文通过分析基于重路由匿名通信系统的内在机制,给出了基于重路由机制的匿名通信系统成员负载数

学期望的公式.从中可以看到,在基于重路由的匿名通信系统中,重路由路径数目、路径长度以及系统中成员数目的动态变化都将影响成员上的负载.因此,应当对系统产生的重路由路径的数目以及路径长度进行限制,以降低负载.应用该概率公式分析 Crowds 匿名通信系统中的负载情况,得出了精确的负载期望值 $1/(1-p_f)+1$,仿真实验结果也证实了这一结论的正确性.这改进了 Reiter 的分析结果,表明在 Crowds 系统中,由于对重路由路径数目进行了限制,使得系统满负荷运行时成员负载为一个恒定的常数.成员数目的动态变化不对成员负载产生影响.因而,Crowds 系统具有良好的可伸缩性.

我们进一步的工作包括:(1) 根据本文提出的方法,分析现有匿名通信系统的性能,并进行优化;(2) 研究在基于重路由的匿名通信系统中,重路由机制如何影响系统的匿名保护能力.

附录:**定理 1 的证明**.

证明:由式(6)可以得到 R_j^m 的数学期望为

$$\begin{aligned} E(R_j^m) &= \sum_{i=0}^{\infty} i \Pr\{R_j^m = i\} \\ &= \sum_{i=1}^{\infty} i \Pr\{R_j^m = i\} \\ &= \sum_{i=1}^{\infty} i \sum_{k=i}^{\infty} f(k) C_k^i \left(\frac{1}{n}\right)^i \left(\frac{n-1}{n}\right)^{k-i} \\ &= \sum_{k=1}^{\infty} f(k) \sum_{i=1}^{k} i C_k^i \left(\frac{1}{n}\right)^i \left(\frac{n-1}{n}\right)^{k-i} \end{aligned} \tag{i}$$

由二项式定理:

$$\sum_{i=0}^{k} C_k^i a^{k-i} (bx)^i = (a+bx)^k \tag{ii}$$

两边对 x 求导,可得:

$$\sum_{i=0}^{k} i C_k^i a^{k-i} b^i x^{i-1} = kb(a+bx)^{k-1} \tag{iii}$$

令 $x=1$,$a=(n-1)/n$,$b=1/n$,则式(iii)可化为

$$\sum_{i=1}^{k} i C_k^i \left(\frac{n-1}{n}\right)^{k-i} \left(\frac{1}{n}\right)^i = \frac{k}{n} \tag{iv}$$

由式(3)、式(i)和式(iv)可得:

$$E(R_j^m) = \sum_{k=1}^{\infty} f(k)\left(\frac{k}{n}\right) = \left(\frac{1}{n}\right)\sum_{k=1}^{\infty} f(k)k = \left(\frac{1}{n}\right)E(L_m) \tag{v}$$

由式(2)和式(v)可得:

$$E(F_j) = E(R_j) = E\left(\sum_{m=1}^{P} R_j^m\right) = \sum_{m=1}^{P} E(R_j^m) = \left(\frac{P}{n}\right)E(L_m) \tag{vi}$$

定理得证. □

References:

[1] Pfitzmann A, Köhntopp M. Anonymity, unobservability, and pseudonymity—A proposal for terminology. In: Hannes F, ed. Designing Privacy Enhancing Technologies: Int'l Workshop on Design Issues in Anonymity and Unobservability. 2000. 1~9. http://citeseer.nj.nec.com/context/1914705/0

[2] Chaum D. The dining cryptographers problem: Unconditional sender and recipient untraceability. Journal of Cryptology, 1988,1(1):65~75.

[3] Waidner M. Unconditional sender and recipient untraceability in spite of active attacks. In: Quisquater J-J, Vandewalle J, eds. Advances in Cryptology—EUROCRYPT'89: Workshop on the Theory and Application of Cryptographic Techniques. 1990. 302~319. http://citeseer.nj.nec.com/waidner89unconditional.html

[4] Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 1981,24(2):84~90.

[5] Gulcu C, Tsudik G. Mixing Email with Babel. In: Proc. of the 1996 ISOC Symp. on Network and Distributed System Security (NDSS'96). 1996. 2~16. http://csdl.computer.org/comp/proceedings/sndss/1996/7222/00/7222toc.htm

[6] Anonymous remailer. http://www.lcs.mit.edu/research/anonymous.html

[7] Lucent personalized Web assistant. http://www.bell-labs.com/projects/lpwa

[8] Goldschlag D, Reed M, Syverson P. Onion routing for anonymous and private Internet connections. Communications of the ACM, 1999,42(2):39~41.

[9] Reed M, Syverson P, Goldschlag D. Anonymous connections and onion routing. IEEE Journal on Selected Areas in Communications, 1998,16(4):482~494.

[10] Syverson P, Tsudik G, Reed M, Landwehr C. Towards an analysis of onion routing security. In: Hannes F, ed. Designing Privacy Enhancing Technologies: Int'l Workshop on Design Issues in Anonymity and Unobservability. 2000. 96~114. http://citeseer.nj.nec.com/syverson00towards.html

[11] Syverson P, Reed M, Goldschlag D. Onion routing access configurations. In: Proc. of the DARPA Information Survivability Conf. and Exposition (DISCEX 2000). 2000. 34~40. http://csdl.computer.org/comp/proceedings/discex/2000/0490/01/04900034abs.htm

[12] Reiter MK, Rubin AD. Crowds: Anonymity for Web transactions. ACM Trans. on Information and System Security, 1998,1(1): 66~92.

[13] Shields C, Levine BN. A protocol for anonymous communication over the Internet. In: Proc. of the 7th ACM Conf. on Computer and Communication Security. 2000. 33~42. http://citeseer.nj.nec.com/shields00protocol.html

[14] Guan Y, Fu X, Bettati R, Zhao W. An optimal strategy for anonymous communication protocols. In: Proc. of the 22nd International Conf. on Distributed Computing Systems (ICDCS 2002). 2002. 257~266. http://csdl.computer.org/comp/proceedings/icdcs/2002/1585/00/15850257abs.htm

[15] Wright M, Adler M, Levine BN, Shields C. An analysis of the degradation of anonymous protocols. In: Proc. of the 2002 ISOC Symp. on Network and Distributed System Security (NDSS 2002). 2002. http://citeseer.nj.nec.com/context/1767080/446934

[16] Wang WP, Chen JE, Wang JX, Sui HF. An anonymous communication protocol based on groups with definite route length. Journal of Computer Research and Development, 2003,40(4):609~614 (in Chinese with English abstract).

附中文参考文献:

[16] 王伟平,陈建二,王建新,眭鸿飞.基于组群的有限路长匿名通信协议.计算机研究与发展,2003,40(4):609~614.