第41卷 第6期 西 安 交 通 大 学 学 报 Vol.41 №6
2007年6月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Jun. 2007

一种防破坏广播型匿名通信网的多路访问协议

李龙海[1,2]，肖国镇[2]
(1.西安电子科技大学计算机学院，710071，西安；2.西安电子科技大学
综合业务网理论与关键技术国家重点实验室，710071，西安)

摘要：针对Golle等提出的广播型匿名通信网络，设计了一种新的多路访问协议.将每个传送周期分为预约、确认和发送3个阶段，第1阶段采用随机预约映射技术对共享匿名信道进行公平分配，在第2阶段用匿名方式确认分配结果，而成员在第3阶段开始发送匿名消息，同时公布一个非交互式知识证明，以确认自己只在与确认结果一致的位置发送了匿名消息.所提协议可以保证成员绝对遵守分配规则，能有效防御破坏性拒绝服务攻击.利用该协议，不会损害通信系统的匿名性，并能显著提高匿名传输效率.仿真结果表明，在发送长匿名消息时，匿名信道利用率由原来的37%提高到了90%以上.

关键词：匿名通信；译解密码者网络；非交互式知识证明
中图分类号：TN918.4 **文献标识码**：A **文章编号**：0253-987X(2007)06-0674-05

Disruption-Resistant Multi-Access Protocol for Broadcast Anonymous Communication Network

Li Longhai[1,2], Xiao Guozhen[2]
(1. School of Computer Science, Xidian University, Xi′an 710071, China; 2. National Key Laboratory on Theory and Chief Technology of Integrated Services Networks, Xidian University, Xi′an 710071, China)

Abstract: A novel multi-access protocol is designed for the broadcast anonymous communication network proposed by Golle et al. Every sending period is divided into reservation phase, confirmation phase and sending phase. A random reservation map technique is used for fair sharing of the common anonymous channel in the first phase. Then all participants are required to confirm the reservation results anonymously in the second phase. In the third phase everyone begins to send his anonymous messages, and simultaneously publishes a non-interactive knowledge proof to prove the fact that only in the positions consistent with the confirmation has he sent the anonymous messages. This protocol can guarantee absolute observation of the sharing rules by every participant and resist disruptive denial-of-service attacks effectively. This protocol doesn't impair communication system's anonymity and can notably improve its anonymous-transmission efficiency. Simulations show that the anonymous channel usage rate is raised from 37% to more than 90% when it works with long messages.

Keywords: anonymous communication; cryptographer network; non-interactive knowledge proof

DC-Net是由Chaum首先提出的一种广播型匿名通信协议[1]，利用它能够在通信过程中隐藏消息的发送者以达到保护用户隐私的目的.DC-Net提供的是一种总线型共享信道，如果2个成员在同一时槽发送匿名消息就会产生冲突，所以必须利用多路访问协议将信道进行合理分配.然而，恶意成员往往

收稿日期：2006-07-28. 作者简介：李龙海(1976～)，男，在职博士生，讲师；肖国镇(联系人)，男，教授，博士生导师.
基金项目：国家自然科学基金资助项目(60473028).

不遵守分配规则，在不属于自己的时槽内发送噪声数据以制造拒绝服务(DoS)攻击，但恰恰是 DC-Net 的发送者匿名性使得追踪这些破坏者变得非常困难，针对此问题迄今尚无有效的解决方案.

为了抵御攻击，现有的 DC-Net 多路访问协议[1-3]均采用“设置陷阱”加“秘密公开”法，但这种方法捕获破坏者的概率比较低，如果要提高成功捕捉的概率，就必须加大陷阱消息与正常消息的比值，其后果是匿名消息发送效率大大降低.

本文针对 Golle 等人提出的新型 DC-Net[4](GJ DC-Net)设计了一种新的多路访问协议，它采用预约映射法对信道进行公平分配，当需发送长匿名消息或者预约开销较小时，可以显著提高匿名信道的利用率. 另外，该方案同样适用于 von Ahn 的 DC-Net 变体型协议——k-AMT[5].

1　协议的基本思想

协议将一个会话周期依次分为预约阶段、确认阶段和发送阶段. 如果在前 2 个阶段发现了作弊行为，那么就直接进入审查阶段，找出破坏者.

(1)预约阶段. 采用预约映射技术[1]，即利用 $m(m=O(n^2)\gg n)$个 DC-Net 匿名发送过程，构成一个长为 m 的预约帧，而每个成员在预约帧中随机选择一个位置来发送预约字符. 如果成员之间没有发生冲突，则表示预约成功. 预约结束后，所有成功预约的成员将分别获得一个序号.

(2)确认阶段. 所有成功预约的成员根据自己获得的序号在确认帧的相应位置发送一个确认消息. 确认帧长 w 等于成功预约的成员个数.

(3)发送阶段. 该阶段由若干个长为 w 的发送帧构成. 每个成功预约的成员同样按照自己的序号在每个发送帧的相应位置发送匿名消息. 伴随每个发送帧的成员必须提供一个非交互式知识证明，证明他在发送帧中发送的匿名消息的位置与确认帧中发送的确认消息的位置是相同的.

(4)审查阶段. 在该阶段用完全公开法找出内部攻击者，这样做的理由是前 2 个阶段不包含敏感消息，公开后不会破坏匿名性.

为简化模型，本文假设存在一个可靠的广播信道.

2　协议的设计

2.1　系统参数

设 $P(|P|=n)$表示成员集合. 由信任中心根据安全要求生成公用参数：①2 个 q(q 为素数)阶群 $\langle G_1,+\rangle$、$\langle G_2,\cdot\rangle$和一个可接受的双线性对映射[6] $\hat{e}:G_1\times G_1\to G_2$，并要求关于 $\hat{e}$ 判定性双线性 Diffie-Hellman(DBDH)问题[6]难解，同时随机取 G_1 的生成元 Q；②强密码杂凑函数 $H:\{0,1\}^*\to G_1$；③伪随机码生成器 $f:G_2\to\{0,1\}^*$；④预约帧长度 m，它为一正整数(根据生日悖论，要想在预约阶段的无冲突概率达到 α，m 至少等于 $n^2/(-2\ln\alpha)$)；⑤发送阶段所包含的 u 个发送帧为一正整数.

P 中的每个成员 P_i 选择其密钥 $x_i\in_U\boldsymbol{Z}_q$，并公布相应的公钥 $y_i=x_iQ$.

2.2　预约阶段

在预约阶段，包含了 m 个工作在群 $G_3=\langle\boldsymbol{Z}_d,+_d\rangle$上的基本 DC-Net 协议的执行过程，其中 $+_d$ 表示模 d 加法. 令 $l=\lceil\mathrm{lb}n\rceil$，则 $d=2^l$. 成员 P_i 与 P_j 之间所需的 m 个共享密钥 $K_{ij}(1),\cdots,K_{ij}(m)$，是以 $S_{ij}=\hat{e}(Q_R,y_j)^{x_i}=\hat{e}(Q_R,y_i)^{x_j}$ 为种子并利用 f 生成的，其中 $Q_R=H(s)$，s 表示会话周期的流水号.

任意成员 P_i，在预约阶段执行以下动作.

(1)随机选择 $t_i(1\leqslant t_i\leqslant m)$作为预约位置.

(2)广播 m 维向量 $\boldsymbol{V}_{i,R}$，其分量

$$V_{i,R}(k)=\begin{cases}\sum_j \mathrm{sign}(i-j)K_{ij}(k) & k\neq t_i\\ 1+\sum_j \mathrm{sign}(i-j)K_{ij}(k) & k=t_i\end{cases}$$

(3)等待所有成员广播完毕之后，利用自己获得的 n 个向量 $\boldsymbol{V}$，计算 m 维向量 $\boldsymbol{R}$，分量 $R(k)=\sum_{i=1}^{n}V_{i,R}(k)$.

(4)计算 $S_{\mathrm{SUM}}=\sum_{i=1}^{m}R(i)$，如果 $S_{\mathrm{SUM}}>n$，则说明有人发送了多个预约字符 1 或者发送了大于 1 的非法字符，此时将直接进入审查阶段.

(5)找出向量 $\boldsymbol{R}$ 中的所有等于 1 的分量，取其标号构成集合 T. 如果 $t_i\notin T$，则表示 P_i 预约失败，令 $c_i=0$；否则，将 T 中的元素由小到大排成一列 $T_1,T_2,\cdots,T_w$(设 $w=|T|$)，t_i 必然等于序列中的某个元素 T_j. 令 $c_i=j$，至此 P_i 获得了在发送阶段序号为 c_i 的子信道的使用权.

2.3　确认阶段

确认阶段包括了 w 个工作在群 G_2 上的基本 DC-Net 协议过程. 在此阶段，任意成员 P_i 执行以下动作.

(1)针对每一个 $P_j(j\neq i)$，计算它们之间的 w

个共享密钥 $K_{ij}(k)=\hat{e}(Q_{k,C},y_j)^{x_i}$，其中 $Q_{k,C}=H(s\|1\|k)$，$1\leqslant k\leqslant w$.

(2)广播 w 维向量 $\boldsymbol{V}_{i,C}$，其分量

$$V_{i,C}(k)=\begin{cases}\prod\limits_j K_{ij}(k)^{\mathrm{sign}(i-j)} & k\neq c_i\\ Z\prod\limits_j K_{ij}(k)^{\mathrm{sign}(i-j)} & k=c_i\end{cases}$$

式中：$Z\in G_2$ 是由大家事先选定的确认消息.

(3)广播 w 维证明向量 $\boldsymbol{\sigma}_{i,C}$，设 $\widetilde{Q}_{k,C}=\hat{e}\left(Q_{k,C},\sum\mathrm{sign}(i-j)y_j\right)$，则 $\boldsymbol{\sigma}_{i,C}$ 的分量

$$\sigma_{i,C}(k)=\mathrm{PoK}\{x:y_i=xQ\wedge[V_{i,C}(k)=\widetilde{Q}_{k,C}^{x}\vee V_{i,C}(k)/Z=\widetilde{Q}_{k,C}^{x}]\}$$

式中：$\mathrm{PoK}\{x:P(x)\}$ 表示关于秘密 x 的非交互式知识证明，x 的值使命题 $P(x)$ 为真. $\sigma_{i,C}(k)$ 的具体构造方法可参见文献[7-8]. 该证明具有诚实验证者零知识性和秘密不可区分性[8]，所以验证者和监听者无法确定 $P(x)$ 中运算符 $\vee$ 左右的 2 个子命题到底哪个取真.

(4)等待所有成员广播完毕之后，验证其他成员的向量 $\boldsymbol{\sigma}$ 的正确性. 如果 $\boldsymbol{\sigma}_{j,C}$ 不能通过验证，则 P_j 一定为作弊者.

(5)计算 w 维向量 $\boldsymbol{R}$，其分量 $R(k)=\prod V_{i,C}(k)$. 如果 $\boldsymbol{R}$ 的所有分量均等于 Z，则说明确认成功，转入发送阶段；否则，转入审查阶段.

2.4 发送阶段

发送阶段由 u 个发送帧组成，每个发送帧又包括了 w 个工作在 G_2 上的 DC-Net 协议过程. 设成员 P_i 要发送的匿名消息 $m_i=m_{i,1}\|m_{i,2}\|\cdots\|m_{i,u}$ $(m_{i,t}\in G_2,1\leqslant t\leqslant u)$，则在第 t 个发送帧中，P_i 执行以下动作.

(1)针对每一个 $P_j(j\neq i)$，计算它们之间的 w 个共享会话密钥 $K_{ij}(k)=\hat{e}(Q_{k,S}^{t},y_j)^{x_i}$，其中 $Q_{k,S}^{t}=H(s\|t+1\|k)$，$1\leqslant k\leqslant w$.

(2)广播 w 维向量 $\boldsymbol{V}_{i,S}^{t}$，其分量

$$V_{i,S}^{t}(k)=\begin{cases}\prod\limits_j K_{ij}(k)^{\mathrm{sign}(i-j)} & k\neq c_i\\ m_{i,t}\prod\limits_j K_{ij}(k)^{\mathrm{sign}(i-j)} & k=c_i\end{cases}$$

(3)广播 w 维非交互式证明向量 $\boldsymbol{\sigma}_{i,S}^{t}$，设 $\widetilde{Q}_{k,S}^{t}=\hat{e}\left(Q_{k,S}^{t},\sum\mathrm{sign}(i-j)y_j\right)$，则分量

$$\sigma_{i,S}^{t}(k)=\mathrm{PoK}\{x:y_i=xQ\wedge[V_{i,C}(k)V_{i,S}^{t}(k)=(\widetilde{Q}_{k,C}\widetilde{Q}_{k,S}^{t})^{x}\vee V_{i,C}(k)/Z=\widetilde{Q}_{k,C}^{x}]\}$$

(4)等待所有成员广播完毕之后，验证其他成员的证明向量的正确性，然后计算 w 维向量 $\boldsymbol{M}_t$，其分量 $M_t(k)=\prod\limits_{i=1}^{n}V_{i,S}^{t}(k)$.

整个发送阶段完成之后，P_i 利用获得的 u 个 w 维向量 $\boldsymbol{M}_1,\cdots,\boldsymbol{M}_u$，在本会话内计算第 $k(1\leqslant k\leqslant w)$ 个子信道中广播的匿名消息

$$m_k=M_1(k)\|M_2(k)\|\cdots\|M_u(k)$$

2.5 审查阶段

在审查阶段，要求每个成员公布自己在前 2 个阶段使用过的所有秘密消息和共享密钥 $K_{ij}(k)$，然后任何人都可以验证它的输入和广播输出是否一致，以及成员是否遵守了协议规定的预约和确认规则. 另外，协议要求成员在公布共享密钥 $K_{ij}(k)$ 的同时，必须提供有效性证明 $\mathrm{PoK}\{x:K_{ij}(k)=\hat{e}(Q_R,y_j)^{x}\wedge y_i=xQ\}$，这样作弊者无法制造密钥争议，而是将错误转嫁给别人.

3 分 析

3.1 安全性

当 P_i 发送消息 m 而其他成员发送任意消息时，可用 $\mathscr{P}(P_i(m),*)$ 表示匿名通信协议 $\mathscr{P}$ 的输出. $H(|H|\geqslant 2)$ 表示诚实用户集合，A 则表示最多能够控制 $n-2$ 个成员且具有多项式计算能力的被动攻击者.

定义 1 对任选成员 $P_0,P_1\in H$，任意有效消息 m_0、m_1，投掷一个公平硬币 b，然后将 $\mathscr{P}(P_0(m_b),P_1(m_{\bar{b}}),*)$ 传送给 A. 令 A 猜测 b 的值，如果 A 猜中 b 的概率与 1/2 之差可以忽略的话，则称协议 $\mathscr{P}$ 具有发送者匿名性.

定理 1 在 DBDH 假设下，增加了多路访问协议的 DC-Net 匿名通信系统具有发送者匿名性.

证明 在猜测游戏中，假设 $u=1$，则 A 能够获得的信息包括任意成员的公钥、被 A 控制的成员密钥，以及由向量 $\boldsymbol{V}_{i,R}$、$\boldsymbol{V}_{i,C}$、$\boldsymbol{V}_{i,S}$、$\boldsymbol{\sigma}_{i,C}$ 和 $\boldsymbol{\sigma}_{i,S}$ $(1\leqslant i\leqslant n)$ 组成的协议广播输出 $\mathscr{P}(P_0(m_b),P_1(m_{\bar{b}}),*)$. 另外，由于 m_0、m_1 最终会以明文形式出现，所以 A 也可以获得 m_0、m_1 在 $\boldsymbol{V}_{i,S}$ 中的发送位置 k_0、k_1，进而推出所对应的预约消息在 $\boldsymbol{V}_{i,R}$ 中出现的位置 k'_0 和 k'_1. 由于 $\boldsymbol{\sigma}_{i,C}$、$\boldsymbol{\sigma}_{i,S}$ 具有诚实验证者零知识性和秘密不可区分性[8]，所以关于 x_i 的信息不会被泄漏，也不会暴露 P_i 是否在任意位置 k 处发布了确认消息或匿名消息. 因此，$\boldsymbol{\sigma}_{i,C}$、$\boldsymbol{\sigma}_{i,S}$ 对 A 猜测 b 的值不会有任何帮助，A 也只能通过分析 3 个向量 $\boldsymbol{V}$ 来猜测 b. 现假设

处在最坏情况下，即 A 已经控制了除 P_0、P_1 之外的所有成员，此时 A 只需分析 $V_{u,R}(k'_v)$、$V_{u,C}(k_v)$、$V_{u,S}(k_v)$($u,v\in\{0,1\}$)等 12 个值.

设 $H(s)=Q^r$，则

$$V_{0,R}(k'_0)=f(\hat{e}(Q^{x_0},Q^{x_1})^r)+1+c,\quad b=0$$

$$V_{0,R}(k'_0)=f(\hat{e}(Q^{x_0},Q^{x_1})^r)+c,\quad b=1$$

其中 c 是由所有不诚实成员与 P_0 的共享密钥构成的，且 A 知道 c. 如果视 f 为随机预言机[9]，则其输出是均匀分布的，因此在 $b=0$、$b=1$ 这 2 种情况下的 $V_{0,R}(k'_0)$对于 A 是不可区分的，除非 A 知道 f 的输入，即 A 能够由 P_0 的公钥 Q^{x_0}、P_1 的公钥 Q^{x_1} 和 H 的输出 Q^r 计算出 $\hat{e}(Q^{x_0},Q^{x_1})^r$，但这与计算性双线性 Diffie-Hellman 假设[6]相矛盾. 同理，$V_{1,R}(k'_0)$、$V_{0,R}(k'_1)$、$V_{1,R}(k'_1)$在 $b=0$、$b=1$ 这 2 种情况下对于 A 也具有多项式不可区分性.

设 $H(s\|t+1\|k)=Q^r$，则

$$V_{0,S}(k_0)=\hat{e}(Q^{x_0},Q^{x_1})^r cm_0,\quad b=0$$

$$V_{0,S}(k_0)=\hat{e}(Q^{x_0},Q^{x_1})^r c,\quad b=1$$

且 A 知道 c，那么 $V_{0,S}(k_0)$在 $b=0$、$b=1$ 这 2 种情况下的取值对于 A 具有多项式不可区分性，否则与 DBDH 假设相矛盾，即 A 能够在只知道 Q^{x_0}、Q^{x_1} 和 Q^r 的情况下，判断 $V_{0,S}(k_0)/c$ 是否等于 $\hat{e}(Q^{x_0},Q^{x_1})^r$. 同理，在 DBDH 假设下，$V_{u,C}(k_v)$、$V_{u,S}(k_v)$($u,v\in\{0,1\}$)在 $b=0$、$b=1$ 这 2 种情况下的取值对于 A 都具有多项式不可区分性.

因为这些相关的协议输出对于 A 都具有多项式不可区分性，所以它们对于 A 猜测 b 没有任何帮助，A 只能随机猜测 b.

下面 3 个定理说明了系统的防破坏能力和良好的健壮性.

定理 2　任意成员发送 Z 和发送消息 m 的位置不一致而不被发现的概率是可以忽略的.

证明　如果 P_i 发送 m 的位置 k 与发送 Z 的位置 c_i 不一致，则有

$$V_{i,C}(k)=\hat{e}\Big(Q_{k,C},\sum \mathrm{sign}(i-j)y_j\Big)^{x_i}$$

$$V_{i,S}(k)=\hat{e}\Big(Q_{k,S},\sum \mathrm{sign}(i-j)y_j\Big)^{x_i}m$$

在这种情况下，2 个命题$[y_i=x_iQ]\wedge[V_{i,C}(k)V'_{i,S}(k)=(\tilde{Q}_{k,C}\tilde{Q}_{k,S})^{x_i}]$和$[y_i=x_iQ]\wedge[V_{i,C}(k)/Z=\tilde{Q}^r_{k,C}]$都不成立，所以 P_i 能够构造合法证明$\sigma_{i,S}(k)$的概率是可以忽略的(除非 P_i 能猜中验证者的质询 c，而此概率为 $1/q$).

定理 3　设 T 表示 $P-H$ 集合中的恶意成员在预约阶段成功占用的位置集合，则 $P-H$ 中的成员在不属于 T 的位置处能成功发送匿名消息的概率是可以忽略的.

证明　在确认阶段，如果 $P-H$ 集合中的成员在不属于 T 的位置处发送确认消息 Z，则必然会与诚实成员发送的确认消息互相冲突而被发现，该诚实成员使系统进入审查阶段. 经过审查阶段的公开过程，这些作弊者一定会被捕获. 因此，$P-H$ 中的成员发送确认消息的位置集合 $T'=T$. 再根据定理 2，这些成员在发送阶段发送匿名消息的位置集合 T''与 T' 不一致的概率是可忽略的. 因此，恶意成员只能在自己成功预约的位置范围内发送匿名消息.

定理 4　在一个周期内，诚实成员的任意匿名消息能够被成功发送的概率至少为 α.

证明　生日悖论理论保证系统在最繁忙时，诚实成员能够成功预约一个位置的概率至少为 α，而定理 3 保证了该位置不会被恶意成员占用，因此一旦预约成功，该成员的匿名消息在发送阶段一定会被成功地发送. 当系统繁忙度下降时，成员预约成功的概率会更高，因此匿名消息被成功发送的概率至少为 α.

在 GJ DC-Net 方案中，任意匿名消息发送成功的概率为 $(1-1/n)^{n-1}\approx 1/e\approx 0.37$，而新方案在 α 取值较大时就可以获得很高的发送成功率.

3.2　效率

与原方案相比，新方案在每一帧的发送中只是证明向量 $\boldsymbol{\sigma}$ 的构造方法有所改变，但没有增加计算复杂度和通信复杂度，并且不再需要额外广播一个承诺向量. 因此，这 2 种方案每发送 1b 的匿名消息(不管是否发送成功)都需要广播的数据为 $O(n)$，而且每个周期都要进行 $O(n)$ 次模指数运算. 为了进一步提高运算速度，还可以对用户间的共享密钥进行预计算.

当没有发生冲突时，一次基本 DC-Net 协议的执行过程可以正确发送一条匿名消息. 因此，DC-Net 的匿名信道利用率 r_{ACUR} 等于成功发送的匿名消息数与基本 DC-Net 协议执行次数之比，它与单位周期内用户平均发送请求的总数 p 有关，该数目越大，系统越繁忙，一般 r_{ACUR} 也就越大.

设预约帧等效为 l 个 G_2 上的基本 DC-Net 协议(按通信量)，则

$$r_{\mathrm{ACUR}}=\overline{w}u/(l+\overline{w}+\overline{w}u)\qquad(1)$$

式中：$\overline{w}$ 表示单位周期内平均预约成功的成员人数. 由式(1)可以看出，如果发送阶段长度 u 取得合适，使预约和确认阶段的通信量与整个周期的通信量之

比值很小，那么就可以获得较高的 r_{ACUR}. 在新方案中，r_{ACUR} 在不同的 u 下随单位周期内用户平均发送请求的总数的变化如图1所示. 测试中取 $n=100$，$\alpha=0.9$，G_1、G_2 和映射 $\hat{e}$ 按照文献[6]中给出的参数进行构造.

由图1可以看出，当 u 较大时，r_{ACUR} 与 GJ DC-Net 的值之比从37%提高到了90%以上. α 的取值对系统的匿名信道利用率的影响如图2所示.

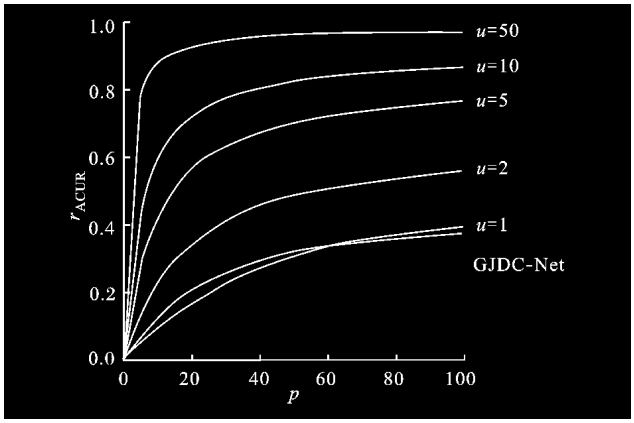

图1 不同 u 值情况下 r_{ACUR} 的变化趋势($\alpha=0.9$)

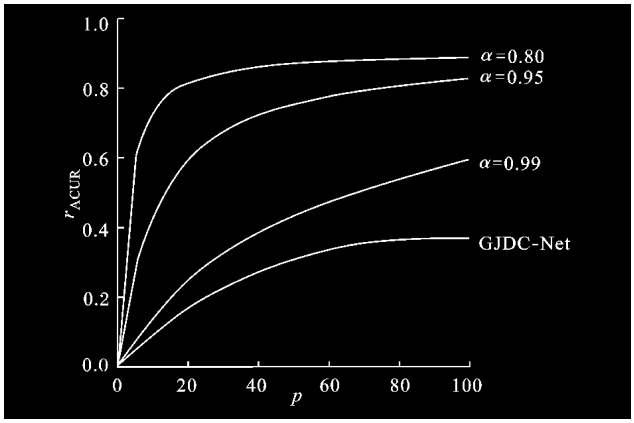

图2 不同 α 值情况下 r_{ACUR} 的变化趋势($u=10$)

4 结束语

本文针对文献[4]的新型 DC-Net，设计了一种多路访问协议. 该协议在保持匿名性的前提下，可以有效地解决信道冲突问题并且可以显著提高匿名信息传输效率. 协议利用非交互式知识证明技术能够以压倒性概率发现破坏者，解决了传统 DC-Net 易遭受 DoS 攻击的难题.

参考文献：

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

[2] Bos J, den Boer B. Detection of disrupters in the DC Protocol [C] // Proceedings of Eurocrypt. Berlin: Springer-Verlag, 1989:320-327.

[3] Waidner M. Unconditional sender and recipient untraceability in spite of active attacks [C]// Proceedings of Eurocrypt. Berlin: Springer-Verlag, 1989:302-319.

[4] Golle P, Juels A. Dining cryptographers revisited [C] // Proceedings of Eurocrypt. Berlin: Springer-Verlag, 2004:456-473.

[5] von Ahn L, Bortz A, Hopper N. k-anonymous message transmission [C] // Proceedings of ACM Conference on Computer and Communications Security. New York: ACM, 2003:122-130.

[6] Boneh D, Franklin M. Identity based encryption from the Weil pairing [J]. SIAM Journal of Computing, 2003, 32(3):586-615.

[7] Cramer R, Gennaro R, Schoenmakers B. A secure and optimally efficient multi-authority election scheme [C] // Proceedings of Eurocrypt. Berlin: Springer-Verlag, 1997:103-118.

[8] Cramer R, Damgaard I, Schoenmakers B. Proofs of partial knowledge and simplified design of witness hiding protocols [C] // Proceedings of Crypto. Berlin: Springer-Verlag, 1994:174-187.

[9] Bellare M, Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols [C]// Proceedings of ACM Conference on Computer and Communications Security. New York: ACM, 1993:62-73.

（编辑 苗凌）