具有可撤销匿名性的 DC-Net 匿名通信方案*)

李龙海[1,2] 付少锋[1] 肖国镇[2]
(西安电子科技大学计算机学院 西安 710071)[1]
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)[2]

摘 要 基于 Golle 和 Juels 的工作,提出了一种具有可撤销匿名性的 DC-Net 匿名通信方案。方案利用双线性对的密钥托管性质,使得用户广播的每个加密消息都以由 n 个执行成员组成的匿名回收部门作为一个潜在的接收者。当发现危害性匿名信息时,在至少 t 个回收执行成员的参与下对有关的协议消息进行联合门限解密,就可以追踪到发送者。在运行时几乎没有增加任何计算复杂度和通信复杂度,并且安全性与原方案相当。对 DC-Net 系统而言,这种方法比已有的利用群签名实现可回收匿名性高效得多。

关键词 匿名通信,DC-Net,可撤销匿名性,双线性对

A DC-Net Anonymous Communication Scheme with Revocable Anonymity

LI Long-Hai[1,2] FU Shao-Feng[1] XIAO Guo-Zhen[2]
(School of Computer Science, Xidian Univ., Xi'an 710071)[1]
(Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071)[2]

Abstract A DC-Net anonymous communication scheme with revocable anonymity is proposed based on Golle and Juels's work. We employ the key escrow property of bilinear parings to make the anonymity revocation authority as an implicit receiver for every encrypted protocol message broadcasted by each user. When a vicious anonymous message being detected, at least t of the authority's total n enforcing participants can jointly decrypt some related protocol messages and trace the sender. Compared with the original scheme, our construction nearly adds no computation and communication complexity and has the same security. For DC-Net, it is much more efficient than the traditional method of providing revocable anonymity by utilizing group signatures.

Keywords Anonymous communication, DC-Net, Revocable anonymity, Bilinear pairings

1 引言

利用匿名通信技术可以在通信过程中隐藏通信双方的身份信息和通信对应关系。现已提出的匿名通信方案主要包括 DC-Net[1] 和 Mix-Net[2] 两种类型,它们已被广泛应用于电子选举、匿名电子邮件、匿名 Web 浏览、电子支付等需要保护用户隐私的互联网应用系统中。但这些匿名系统也同样面临被滥用的威胁。例如,利用匿名通信系统发送垃圾邮件、恐吓信或散布谣言,以及制造拒绝服务攻击等。因此,为了避免被滥用,在设计匿名通信协议时必须考虑匿名的可控性问题。应该在必要时通过法院授权和相关权威部门的参与,能够追踪某个匿名消息的发送者,即撤销其发送者匿名性。

目前可检索到的在匿名通信中实现可撤销匿名性的主要方法是利用群签名[3,4]。该方法虽然可以适用于各种类型的匿名通信系统,但主要存在以下缺点:(1)用户需要对每个明文消息进行群签名,不但增加了计算量,而且减小了消息的有效载荷;(2)因为带有群签名的消息是经过加密之后输入匿名系统的,所以无法确定消息是否已经过了群签名。文[4]中因此增加了复杂度很高的零知识证明协议。文[3]中采取的办法是增加一个可信第三方 V,对匿名系统输出的每个消息(已恢复为明文)进行过滤,删掉那些群签名无效的消息。但这使得 V 的负载太重(要验证所有群签名),并且对于 DC-Net 这种广播型匿名通信系统,V 删除消息的代价也非常大。

本文基于 Golle 和 Juels 的工作[5],设计了一种具有可撤销匿名性的 DC-Net 匿名通信方案。该方案利用双线性对的相关性质,使得用户广播的每个加密消息都以匿名回收执行部门作为另一个潜在的接收者。执行部门回收匿名性时使用的秘密钥被 n 个执行成员利用 (t,n) 门限方案所共享。当发现危害性信息时,在至少 t 个执行成员的参与下对该信息所涉及到的相关协议消息进行门限解密,就可以追踪到信息的发送者。与原方案[5]相比,新方案在运行时没有增加任何复杂度(系统初始化阶段除外),并且不需要实施过滤的第三方 V,因而比利用群签名实现可撤销匿名性的方法高效得多。分析表明,该方案的发送者匿名性建立在双线性 Diffie-Hellman 判定问题假设之上,在安全性上与原方案是相当的。

2 预备知识

DC-Net 协议[1]:DC-Net,即"Dining Cryptographers Network",是由 Chaum 首先提出的一种广播型匿名通信协议。该协议假定存在一个可靠的广播信道,并且任意两个用户之间事先已通过安全信道建立了若干可用的共享密钥。在一轮基本 DC-Net 协议执行过程中,系统中的用户依次广播一个

*)国家自然科学基金面上项目(60473028)。**李龙海** 讲师,博士生,研究方向:密码学、计算机安全;**付少锋** 工程师,研究方向:计算机安全、嵌入式系统;**肖国镇** 教授、博导。

消息。用户 P_i 广播的消息为：$X_i=m_i+\sum_j sign(i-j)\cdot K_{ij}$。其中，$K_{ij}$ 是用户 P_i 与 P_j 之间事先已商定的仅用于本轮协议的共享密钥，m_i 是 P_i 在本轮中要匿名广播的消息。如果没有消息要广播，则令 m_i 为 0。等待所有用户广播完毕之手，任意用户都可以计算总和 $X=\sum_i X_i$。假设本轮只有 P_i 的输入消息 m_i 不为 0，则显然 $X=m_i$。Chaum 在文[1]中已经证明："如果协议中使用的所有共享密钥是绝对秘密的，则消息 m_i 具有无条件的不可追踪性，即无法追踪 m_i 的发送者。"如果一轮中有两个以上成员的输入消息不为 0，那么这些消息就会因相互冲突而发送失败。文[1,5,6]给出了解决 DC-Net 消息冲突问题的相关方案，在此就不再详细叙述了。

双线性对(Bilinear Pairings)[7]：设 G_1 是一个 q 阶加法循环群，G_2 是一个 q 阶乘法循环群，q 为足够大的素数，使得在群 G_1、G_2 上离散对数问题(DLP)难解。定义在 G_1、G_2 上的双线性对映射 $\hat{e}: G_1\times G_1\to G_2$ 满足如下性质。

(1)双线性性：$\forall P,Q\in G_1, a,b\in Z_q^*$

$\hat{e}(abP,Q=\hat{e}(P,abQ)=\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$

(2)非退化性：设 1 表示 G_2 的么元，则 $\exists P\in G_1$ 使得 $\hat{e}(P,P)\neq 1$。因为 G_1、G_2 都是素阶群，所以该性质也表明，如果 P 是 G_1 的生成元，则 $\hat{e}(P,P)$ 也是 G_2 的生成元。

(3)可计算性：$\forall P,Q\in G_1$，存在有效算法计算 $\hat{e}(P,Q)$。

满足上述条件的双线性对 $\hat{e}$ 可以通过有限域上基于超椭圆曲线的 Weil 对或 Tate 对来构造[7]。本文提出的 DC-Net 协议依赖于以下问题的困难性。

(1)双线性 Diffie-Hellman 计算问题(CBDH)：给定 P、aP、bP、cP，其中 $P\in G_1, a,b,c\in Z_q^*$，计算 $\hat{e}(P,P)^{abc}$ 的值。

(2)双线性 Diffie-Hellman 判断问题(DBDH)：给定 P、aP、bP、cP 和 dP，其中 $P\in G_1, a,b,c,d\in Z_q^*$，判断 $\hat{e}(P,dP)$ 是否等于 $\hat{e}(P,P)^{abc}$，或 d 是否等于 abc，输出 YES 或 NO。

3 具有可撤销匿名性的 DC-Net

3.1 系统的建立

由信任中心根据安全要求生成如下公用参数：(1)两个 q(q 为素数)阶群$\langle G_1,+\rangle$、$\langle G_2,\cdot\rangle$和双线性对 $\hat{e}: G_1\times G_1\to G_2$，要求关于该双线性对 DBDH 问题难解。随机选取 G_1 的生成元 Q。(2)强密码杂凑函数 $H: \{0,1\}^*\to G_1$。(3)p 阶群$\langle G_3,\cdot\rangle$，要求在 G_3 上离散对数问题难解。随机选取 G_3 的生成元 g 和 h。

由政府权威部门组建包括 n 个执行成员的匿名性回收机构 RA，该机构可以负责多个 DC-Net 匿名通信系统的匿名撤销工作。RA 的 n 个成员利用 Shamir 的(t,n)门限秘密共享协议[8]共享秘密 $a\in_U Z_q^*$。设成员 RA_i 所掌握的关于 a 的秘密份额为 a_i，其相应的公开钥为 $A_i=a_iQ$。RA 对外公布 $A=aQ$。

设某 DC-Net 系统的用户为 $P_1,\cdots,P_N$，分别拥有公钥 $PK_1,\cdots,PK_N$，且已经选定具有语义安全性的非对称加密算法 E。这些用户按照如下协议生成运行 DC-Net 所需的密钥：

(1)任意用户 P_i 在 Z_q^* 中随机选择 $N-1$ 个数 $s_{i,1},\cdots,s_{i,N-1}$，并计算 $s_{i,N}$，满足 $\sum_j s_{i,j}=0$。

(2)P_i 计算 N 维向量 C_i 和 S_i，其分量 $C_{i,k}=s_{i,k}Q$，$S_{i,k}=E_{PK_k}(s_{i,k})(1\leqslant k\leqslant N)$。$P_i$ 将向量 C_i 和 S_i 广播给系统内其它用户。

(3)等待所有用户广播完毕之后，P_i 获得了 N 个 C 向量和 N 个 S 向量。P_i 验证：对任意的 $1\leqslant j\leqslant N$，$\sum_k C_{j,k}=0$。

(4)对所有 $1\leqslant j\leqslant N$，P_i 利用自己掌握的与 PK_i 对应的密钥对 $S_{j,i}$ 进行解密获得 $s_{j,i}$，并验证：$s_{j,i}Q=C_{j,i}$。如果验证通过，则 P_i 获得了自己的 DC-Net 密钥 $s_i=\sum_j s_{j,i}$。

(5)P_i 计算自己的 DC-Net 公开钥 $Y_i=s_iQ$，并将其广播给其它成员。

(6) 等待所有用户广播完毕之后，P_i 验证：对任意的 $1\leqslant j\leqslant N$，$Y_j=\sum_k C_{k,j}$。

上述密钥生成协议的安全性基于 G_1 上离散对数问题假设。通过以上过程，$P_1,P_2,\cdots,P_N$ 最终获得的 DC-Net 密钥必然满足关系式：$\sum_i s_i=0$。

3.2 匿名消息发送协议

匿名消息发送过程包括多个会话周期，每个周期并行地执行 N 轮基本 DC-Net 协议，在每一轮中最多只能成功发送一个匿名消息。为保证一定的发送成功率，减少消息冲突，协议要求每个用户在一个周期内最多只能发送一个匿名消息。

设当前周期的流水号为 r，P_i 要发送的消息为 $m_i\in G_2$。如果 P_i 没有消息发送，则令 $m_i=1$。任意用户 P_i 执行以下动作：

(1)随机选取 $l_i\in\{1,\cdots,N\}$作为自己发送匿名消息的位置。

(2)广播经过签名的 N 维向量 X_i，其分量 $X_i(k)$的计算方法为：设 $Q_{r,k}=H(r\,\|\,k)$，则

$$X_i(k)=\begin{cases}\hat{e}(A,Q_{r,k})^{s_i}, & k\neq l_i\\ m_i\cdot\hat{e}(A,Q_{r,k})^{s_i}, & k=l_i\end{cases}$$

(3)广播 N 维承诺向量 δ_i。δ_i 的分量 $\delta_i(k)$的计算方法为：如果 $k=l_i$，令 $\delta_i(k)=gh^{r_k}$，否则令 $\delta_i(k)=h^{r_k}$，$r_k\in_U Z_p^*$。

(4)广播 $N+1$ 维非交互证明向量 σ_i。σ_i 的分量 $\sigma_i(0)=\mathrm{PoK}\{r: g^{-1}\cdot\prod_k\delta_i(k)=h^r\}$，而其余分量 $\sigma_i(k)=\mathrm{PoK}\{x,r: (Y_i=xQ\wedge X_i(k)=\hat{e}(A,Q_{r,k})^x\wedge\delta_i(k)=h^r)\vee(\delta_i(k)g^{-1}=h^r)\}$。其中 $\mathrm{PoK}\{x: P(x)\}$表示关于秘密值 x 的非交互零知识证明，x 使命题 $P(x)$为真。

(5)等待所有用户广播完毕之后，P_i 验证其它成员的 σ 向量的正确性。如果 σ_j 不能通过验证，则 P_j 一定为作弊者，协议停止。

(6)P_i 计算 N 维向量 X，其分量 $X(k)$的计算方法为：$X(k)=\prod_{j=1}^N X_j(k)(1\leqslant k\leqslant N)$。如果 $X(k)\neq 1$，则可以将 $X(k)$解释为本周期第 k 轮中广播输出的匿名消息。

上述协议中向量 δ_i 和 σ_i 的作用是确保 P_i 按协议规定的方式构造了向量 X_i，并且在一个周期内最多只发送了一个匿名消息。关于 σ_i 的详细原理和具体构造方法见文[5,9]。由于 $\sigma_i(k)$具有诚实验证者零知识性和秘密不可区分性[9]，不会暴露 P_i 是否在位置 k 处发送了匿名消息，因此不会对发送者匿名性造成任何损害。

3.3 匿名性撤销协议

在 DC-Net 系统中一旦发现危害性消息 m，RA 经过法院授权之后执行针对 m 的发送者匿名性撤销协议。该协议需要至少 t 个 RA 成员的参与。设参与成员的集合为 T，并不妨设 $T=\{RA_1, RA_2,\cdots, RA_t\}$。$T$ 中的成员首先收集所有与 m 相关的 DC-Net 协议消息。设该消息集合为 π_m，如果 m 出现于第 r 个周期的第 k 轮，则 $\pi_m=\{X_i(k)\,|\,1\leqslant i\leqslant N\}$；然后开始追踪 m 的发送者，其主要过程为：由 T 中成员对 π_m 中的消息依次进行联合解密，并判断解密结果是否与 m 相等。如果发现 $X_j(k)$的解密结果等于 m，则说明 P_i 为消息 m 的发送者，并停止追踪过程。关于 π_m 中任意消息 $X_j(k)$的具体解密

过程包括以下两步：

(1)T 的每一个成员 RA_i 计算 $W_{i,j}=\hat{e}(Y_j,Q_{r,k})^{a_i L_i}$ 和 $V_{i,j}=\mathrm{PoK}\{x:W_{i,j}=\hat{e}(Y_j,Q_{r,k})^{xL_i}\wedge A_i=xQ\}$，其中 $L_i=\prod_{1\leqslant j\leqslant t,j\neq i}\frac{j}{j-i}$。$RA_i$ 将 $W_{i,j}$ 和 $V_{i,j}$ 广播给其它成员。

(2)等待所有成员广播完毕之后，RA_i 验证其它成员的非交互零知识证明 V 的正确性。如果某成员的证明无法通过验证，则确定其为作弊者，并重新构建 T 集合；如果全部通过验证，则计算 $X_j(k)$ 的解密结果 x_j：

$$x_j=X_j(k)\cdot(\prod_{i=1}^{t}W_{i,j})^{-1}$$

以上采用的是“顺序查找”法，还可以采用“折半查找法”进一步降低计算复杂度。其具体方法为：将 π_m 尽量平分为两个子集 $\pi_{m,1}$ 和 $\pi_{m,2}$，将 $\pi_{m,1}$ 中所有消息乘到一起并对该乘积进行联合解密。如果解密结果等于 m，则说明 m 的发送者存在于集合$\{1,2,\cdots,N/2\}$中，再进一步对 $\pi_{m,1}$ 进行平分、解密；如果等于 1，则说明发送者存在于集合$\{N/2+1,\cdots,N\}$中，那么再对 $\pi_{m,2}$ 进行平分、解密。以上过程递归进行，直到所得集合中只有一个消息为止。利用这种方法可以使匿名撤销协议平均所需的联合解密次数由 $N/2$ 次减少为 $\log_2 N$ 次。

4 分析

4.1 正确性

(1)匿名消息发送协议的正确性：设在第 r 个周期的第 k 轮中，只有用户 P_i 的消息输入为 m_i，而其它用户的输入为 1，并且注意到 $\sum_i s_i=0$，则任意用户获得的 $X(k)$ 为

$$X(k)=\prod_{j=1}^{N}X_j(k)=m_i\cdot\prod_{j=1}^{N}\hat{e}(A,Q_{r,k})^{s_j}$$
$$=m_i\hat{e}(A,Q_{r,k})^{\sum_j s_j}=m_i$$

因此 m_i 被正确广播给了系统中的任意用户。

(2)匿名性撤销协议的正确性：假设消息 m 是在第 r 周期的第 k 轮中被接收到的，并且 m 的发送者为 P_j，那么 $X_j(k)=m\cdot\hat{e}(A,Q_{r,k})^{s_j}$，$X_l(k)=\hat{e}(A,Q_{r,k})^{s_l}$ $(1\leqslant l\leqslant N,l\neq j)$。根据拉格朗日插值定理和 $\hat{e}$ 的双线性特性，

$$\prod_{i=1}^{t}W_{i,j}=\prod_{i=1}^{t}\hat{e}(Y_j,Q_{r,k})^{a_i L_i}=\hat{e}(s_j Q,Q_{r,k})^{\sum_i a_i L_i}$$
$$=\hat{e}(s_j Q,Q_{r,k})^{a}=\hat{e}(A,Q_{r,k})^{s_j}$$

RA 对 $X_j(k)$ 的解密结果 $x_j=X_j(k)\cdot(\prod_{i=1}^{t}W_{i,j})^{-1}=m\cdot\hat{e}(A,Q_{r,k})^{s_j}\cdot(\hat{e}(A,Q_{r,k})^{s_j})^{-1}=m$，而将其它用户的输出解密为 1。因此，$P_j$ 必然会被 RA 确定为 m 的发送者。又因为 P_j 对 $X_j(k)$ 已经签名，所以他无法对此事实进行抵赖。

另外，如果 m 在第 k 轮中被无冲突地成功接收，则根据 DC-Net 的性质，该轮中有且只有一个用户匿名发送了 m，所以上述匿名撤销过程不会影响 P_j 之外的其它用户的匿名性。

4.2 安全性

设 $\mathcal{P}(P_i(m),*)$ 表示用户 P_i 发送消息 m，而其它用户发送任意消息时匿名通信协议 $\mathcal{P}$ 的输出，$H(|H|\geqslant 2)$ 表示诚实用户的集合。

定义 1 设 $\mathcal{A}$ 表示符合给定攻击模型 ε 的任意攻击者。对任选用户 $P_0,P_1\in H$ 和任意有效消息 m_0、m_1，投掷一个公平硬币 B，然后将协议运行结果 $\mathcal{P}(P_0(m_B),P_1(m_{1-B}),*)$ 传送给 $\mathcal{A}$，令 $\mathcal{A}$ 猜测 B 的值。如果 A 猜中 B 的概率与 1/2 相比只具有可忽略的优势，则称协议 $\mathcal{P}$ 在攻击模型 ε 下具有发送者匿名性。

针对本文的 DC-Net 方案，定义如下攻击模型 ε：该模型中的任意攻击者 $\mathcal{A}$ 只具有多项式计算能力，最多能控制 N-2 个 *DC-Net* 用户和 t−1 个 *RA* 成员，且只进行静态攻击。

定理 1 在 *Random Oracle* 模型[10]下，如果 *DBDH* 问题难解，则本文的 *DC-Net* 方案的匿名消息发送协议在上述攻击模型 ε 下具有发送者匿名性。

证明：假设存在符合模型 ε 的攻击算法 $\mathcal{A}$ 在上述游戏中猜中 B 的概率与 1/2 相比具有不可忽略的优势，下面利用 A 构造算法 $\mathcal{D}$ 来解任意 DBDH 问题(Q,aQ,bQ,cQ,dQ)以导出矛盾：(1) 首先构造一套对 $\mathcal{A}$ 而言合法的系统公开参数：任选两个诚实用户 P_0、P_1，令他们的 DC-Net 公开钥 $Y_0=bQ,Y_1=-bQ$，然后仅在集合 $P-\{P_0,P_1\}$ 上执行 DC-Net 密钥生成协议；令 $A=aQ$。(2) 以步骤 1 的结果为参数调用匿名消息发送协议子程序，执行一个传送周期。执行时，任选消息 m_0，$m_1\in G_2$ 和 $B\in_U\{0,1\}$，由 P_B 在第 1 轮发送 m_0，P_{1-B} 在第 2 轮处发送 m_1。执行过程中，由 $\mathcal{D}$ 代表 P_0、P_1 生成他们的输出。另外，在 *Random Oracle* 模型下 $\mathcal{D}$ 还可以控制函数 H 的输出。(3)开始执行时，$\mathcal{D}$ 选择 $r_k\in_U Z_q^*$，并使 *Random Oracle* 输出 $Q_{r,1}=H(r\|1)=r_1 cQ,Q_{r,2}=r_2 cQ,Q_{r,k}=r_k Q(k\neq 1,2)$。$B=0$ 时，$\mathcal{D}$ 构造 P_0 的输出 X_0 为：$X_0(1)=\hat{e}(Q,dQ)^{r_1}\cdot m_0$，$X_0(2)=\hat{e}(Q,dQ)^{r_2}$，$X_0(k)=\hat{e}(A,bQ)^{r_k}(k\neq 1,2)$；构造 P_1 的输出 X_1 为：$X_1(1)=\hat{e}(Q,dQ)^{-r_1}$，$X_1(2)=\hat{e}(Q,dQ)^{-r_2}\cdot m_1$，$X_1(k)=\hat{e}(A,bQ)^{-r_k}(k\neq 1,2)$。$B=1$ 时，D 构造 P_0 的输出 X_0 为：$X_0(1)=\hat{e}(Q,dQ)^{r_1}$，$X_0(2)=\hat{e}(Q,dQ)^{r_2}\cdot m_1$，其它不变；构造 X_1 为：$X_1(1)=\hat{e}(Q,dQ)^{-r_1}\cdot m_0$，$X_1(2)=\hat{e}(Q,dQ)^{-r_2}$，其它分量不变。(4)如果 m_0、m_1 都被正确发送，即没有与其它成员发送的消息产生冲突，则 $\mathcal{D}$ 将运行输出和系统相关公开参数作为输入传送给算法 A；否则重复进行 2、3 两步，直到没有冲突为止。A 在运行时还可以随时向 $\mathcal{D}$ 询问 P_0、P_1 之外的任何用户的秘密钥。(5)重复运行 2、3、4 多次，如果 $\mathcal{A}$ 能以不可忽略的优势猜中 B，则 $\mathcal{D}$ 输出 YES，即认为 $d=abc$，否则 $\mathcal{D}$ 输出 NO。

下面解释一下为什么上述算法 $\mathcal{D}$ 能够正确解 DBDH 问题(Q,aQ,bQ,cQ,dQ)：(1) 如果 $d=abc$，那么在上面第 3 步中构造的 X_0、X_1 是完全合法的 DC-Net 协议输出。根据假设，$\mathcal{A}$ 能够以不可忽略的优势猜中 B，因而 $\mathcal{D}$ 输出 YES。(2) 如果 $d\neq abc$，那么对 $\mathcal{A}$ 猜测 B 有帮助的 $X_0(1)$、$X_1(1)$、$X_0(2)$、$X_1(2)$ 在 $B=0$ 时具有形式：$Rand1\cdot m_0$、$Rand1^{-1}$、$Rand2$、$Rand2^{-1}\cdot m_1$，在 $B=1$ 时具有形式：$Rand1$、$Rand1^{-1}\cdot m_0$、$Rand2\cdot m_1$、$Rand12^{-1}$。这两种形式对 A 而言具有相同的分布，因而 $\mathcal{A}$ 只能随机猜测 B，最终导致 $\mathcal{D}$ 输出 NO。

4.3 效率

协议规定在包括 N 轮的一个周期内每个用户随机选择一个位置发送消息。假设 P_i 选择选在 l_i 处发布消息，而其它成员不选择在此位置发布的概率为$(1-1/N)^{N-1}$，在 N 较大时此概率接近于 $1/e\approx 0.37$。因此任意消息匿名发送成功的概率约为 37%。

下面考虑方案中最关键的匿名消息发送阶段的计算复杂度和通信复杂度。本方案用户广播的 X_i 向量的数据长度等于 $N\log_2 q$ bit，与原方案[5]相同；在计算 X_i 时要进行 N 次 G_2 上的指数运算和 N 次双线性对运算，与原方案相比还节省了 N 次 G_1 上的加运算。而两个方案构造 δ_i 和 σ_i 向量的方法是完全相同的。因此，在匿名发送阶段新方案的开销略低于原方案。

在系统建立阶段，原方案的每个用户需进行 1 次 G_1 上的

(下转第 89 页)

类，从而决定是否有违反安全策略的入侵行为发生。

3 实验分析

为了测试推进贝叶斯分类法的入侵检测引擎的检测率，我们设计了推进贝叶斯分类法的入侵检测系统（简称为BBIDS），与直接使用贝叶斯分类法的入侵检测系统作比较实验，并进行实验结果分析。

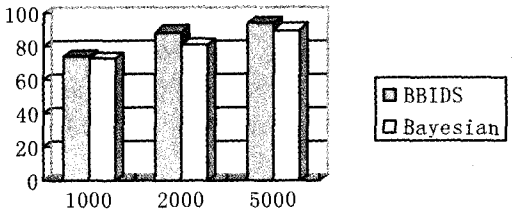

图4 比较实验结果

实验数据选用KDD Cup 1999网络数据集[3]，为了方便实验我们从中选取了10000条数据，这些数据中包含100条异常数据。从实验数据中抽取4组数据组成3个训练子集（T_1，T_2，T_3）和一个测试集（E_1），3组训练子集分别包括1000个、2000个和5000个带标记数据，测试集包含1000个不带标记的数据。实验中分别使用T_1，T_2，T_3训练基于引导聚集ID3分类法的入侵检测系统和ID3分类法的入侵检测系统，然后使用训练好的分类模型对E_1进行对比测试，得到3个测试结果。如图4所示。

通过对图4的观察，可知训练数据越丰富时，引擎检测检测率越高，BBIDS的检测率一直比贝叶斯高，当训练数据为5000时，BBIDS的检测率达到了94.07%。因此，使用推进技术可以提高分类的正确率。使用BBIDS的入侵检测系统与使用贝叶斯的入侵检测系统相比具有更高的检测率。

结论 推进贝叶斯分类算法的学习需要搜集大量的网络访问的数据进行学习，借此来训练入侵检测系统的学习模型。这是一项非常复杂的工作，但是从实验结果看来，运用加权引导聚集，通过加权学习，可以提高检测率、减小误判，因此该方法运用到入侵检测中取得了良好的效果。

参考文献

1 Lee W. A data mining framework for constructing features and models for intrusion detection systems: [dissertation of Doctor of Philosophy]. Columbia University, 1999
2 Han Jiawei, Kamber M. Data mining: concepts and techniques [M]. San Francisco: Morgan Kaufmann Publishers, 2001. 185～219
3 http://kdd.ics.uci.edu
4 唐正军. 网络入侵检测系统的设计与实现. 电子工业出版社. 2002

（上接第61页）

址利用率的衡量标准并不是通常意义的百分比利用率，而是用HD比率来衡量[6]，其定义为

$$\text{HD比率}=\frac{\text{Log}(\text{已经分配的地址空间})}{\text{Log}(\text{最大可分配地址空间})} \quad (5)$$

其中，“地址空间”表示/48的客户数量。HD比率等于0.94，相应换算成各前缀的实际使用百分率。可以看出，实际IPv6使用率一般不会高于50%，在宽松的后继申请利用率的条件下，自适应二分法按照2的幂次分解进行地址申请的机会小得多，可以预计其聚合性能将会更好。

结束语 IP地址分配方法是影响各级路由表增长速度的重要因素，地址使用单位从方便管理和控制运营成本的角度也寻求最大限度的聚类所拥有的IP地址段。然而，我国运营商在现行地址分配政策下，只能周期性地申请地址，满足网络扩容的需求，迫切需要一种有效的地址分配方法来指导其进行IP地址分配。模拟实验表明，本文所提出的改进的二分地址分配方法具有良好的聚类特性，可以有效地减少地址碎片并提高地址利用率，为不同层次的地址分配机构实际分配IPv6地址提供了有益的参考。

参考文献

1 IPv4路由表情况. http://bgp.potaroo.net/
2 Xu Z, Meng X, Zhang L, et al. Impact of IPv4 Address Allocation Practice on BGP Routing Table Growth. IEEE Computer Communications Workshop(CCW), Oct. 2003
3 Wang Mei. A Growth-based Address Allocation Scheme for IPv6 Networking. LNCS, 2005, 3462: 671～683
4 APNIC. Policies for IPv4 address space management in the Asia Pacific region. December 2005
5 Huston G. Consideration of the IPv6 Allocation Unit Size. http://www.potaroo.net/drafts/draft-huston-ip6-allocation-unit-00.txt, June 2005
6 Durand A. RFC 3194, The H-Density Ratio for Address Assignment Efficiency: An Update on the H ratio

（上接第79页）

点乘运算，而新方案的每个用户要进行N次G_1上的点乘运算和N次公钥加密运算，并且广播的数据量也扩大了N倍。但这是为原方案的DC-Net增加匿名可撤销特性所付出的代价，并且这些操作只需在初始化阶段进行一次。如果采用群签名法实现可撤销匿名性[3,4]，则需对每个匿名消息都进行群签名和签名验证，并要增加复杂的零知识证明协议，与本文的方法相比，其额外开销要大得多。

结束语 对一种新型的DC-Net匿名通信方案进行了改进，改进方案用很低的代价实现了可撤销的发送者匿名性，使得在至少t个权威执行成员的参与下可以追踪系统中任意匿名消息的发送者。可以证明，改进后的匿名性基于双线性Diffie-Hellman判定问题的困难性，在安全性上与原方案是相当的。

参考文献

1 Chaum D. The dining cryptographers problem: unconditional sender and recipient untraceability. Journal of Cryptology, 1988, 1(1): 65～75
2 Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 1981, 24(2): 84～88
3 Stefan K, Rolf W, Hannes F. Revocable anonymity. In: Proceedings of ETRICS 2006. Heidelberg: Springer-Verlag, 2006. 206～220
4 von Ahn L, Bortz A, Hopper N. Selectively traceable anonymity. In: Proceedings of PET2006. Cambridge, UK: Springer-Verlag, 2006. 586～615
5 Golle P, Juels A. Dining cryptographers revisited. In: Advances in Cryptology: Eurocrypt' 2004. Berlin: Springer-Verlag, 2004. 456～473
6 Waidner M. Unconditional sender and recipient untraceability in spite of active attacks. In: Advances in Cryptology: Eurocrypt' 89. Berlin: Springer- Verlag, 1989. 302～319
7 Boneh D, Franklin M. Identity based encryption from the Weil Pairing. SIAM J of Computing, 2003, 32(3): 586～615
8 Shamir A. How to share a secret. Communications of the ACM, 1979, 22(11): 612～613
9 Cramer R, Damgaard I, Schoenmakers B. Proofs of partial knowledge and simplified design of witness hiding protocols. In: Advances in Cryptology: Crypto' 94. Berlin: Springer-Verlag, 1994. 174～187
10 Bellare M, Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols. In: Proceedings of ACM CCS' 93. New York: ACM, 1993. 62～73