基于几何性质一般访问结构上的多重秘密共享方案*)

庞辽军[1] 李慧贤[2] 王育民[1]
(西安电子科技大学综合业务网国家重点实验室 西安 710071)[1]
(大连理工大学计算机科学与工程系 大连 116024)[2]

摘 要 提出了一个基于几何性质的一般访问结构上的多重秘密共享方案,其中秘密和各参与者的秘密份额皆为(t-1)维向量。每个参与者只需保护一个秘密份额,就可以实现任意多个秘密的共享。与现有一般访问结构上的秘密共享方案相比,文本的方案更为有效,尤其是在共享一个大秘密时。分析表明,本文的方案满足秘密共享的安全性要求与规则,是一个计算上安全且有效的方案。

关键词 秘密共享,多重秘密共享,访问结构

A Multi-secret Sharing Scheme with General Access Structures Based on a Geometric Property

PANG Liao-Jun[1] LI Hui-Xian[2] WANG Yu-Min[1]
(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071)[1]
(School of Electronic and Information Engineering, Dalian Univ. of Tech., Dalian 116024)

Abstract A new multi-secret sharing scheme with general access structure is proposed, which is based on a geometric approach. In this scheme, the shared secret and each participant's secret shadow should be vectors of (t-1) dimensions. Each participant only needs to keep one secret shadow in sharing multiple secrets without updating each participant's secret shadow. Compared with the existing schemes with general access structures, the proposed scheme is very effective, especially in sharing a large secret. Analyses show that the proposed scheme reinforces the requirements and rules of security and that it is computationally secure and efficient scheme.

Keywords Secret sharing, Multi-secret sharing, General access structure

1 引言

秘密共享是在一组参与者中共享秘密的技术,它在重要信息和秘密数据的安全保存、传输及合法利用中起着非常关键的作用;它也是密码学和分布式计算领域中一个非常重要的研究内容。Shamir[1]和 Blakley[2]最早提出秘密共享的概念,并分别基于 Lagrange 插值法和多维空间点的性质提出(t, n)门限秘密共享方案。一个秘密 s 被 n 个参与者共享,至少 t 个参与者合作可以重构 s;而(t(t-1)个或更少的参与者得不到 s 的任何信息。较早的秘密共享体制还有基于中国剩余定理的 Asmuth-Bloom 方法[3]以及使用矩阵乘法的 Karnin-Greene-Hellman 方法[4]等。Wu 和 He[5]基于几何性质提出了一个(t, n)门限秘密共享方案。与上述方案不同的是,秘密和各参与者的秘密份额皆表示为(t-1)维向量。该方案有非常重要的应用价值,尤其是在共享大秘密时比其它方案更为有效[6]。

但是他们的方案都只适合于(t, n)门限应用,而不适合于一般访问结构上的应用;而且 Wu-He 方案还是一个一次性的方案[7],即各参与者的秘密份额只能使用一次,在每次共享过程中,秘密分发者必须重新分配各参与者的秘密份额,这会增加 Wu-He 方案的存储和通信复杂度,影响系统性能[6]。Benaloh 等人[8]指出,门限方案仅处理了秘密共享问题的一小部分,而更为一般、更为普遍的是访问结构上的秘密共享方案,即一般的秘密共享方案,并给出一般访问结构上秘密共享方案的模型:秘密分发者将所要共享的秘密 s 分拆为 n 个子秘密(份额),并通过安全信道将其分发给这 n 个参与者,使得每一个参与者仅知道自己的子秘密而不知道其它任何参与者的子秘密;同时,秘密分发者定义一些授权子集,使得这些集合中的参与者联合可以恢复 s,而非授权子集中的参与者合作不能得到 s 的任何信息。由所有授权子集组成的集合称为访问结构[9],常用 Γ 表示,称 $B\in\Gamma$ 是最小授权子集,如果无论何时 $A\subset B$,那么 $A\notin\Gamma$。Γ 的最小授权子集的集合 Γ_0 称为 Γ 的基,Γ 可以由 Γ_0 唯一地确定,即 $\Gamma=\{C|B\subseteq C,\ B\in\Gamma_0\}$,其中 C 为由参与者组成的集合。本文约定授权子集均指最小授权子集。

由于最普遍的应用为访问结构上的应用,因此,有必要进行访问结构上秘密共享方案的研究。本文基于几何性质[5]提出了一个一般访问结构上的多重秘密共享方案。该方案不仅具有与 Wu-He 方案相同的优点,同时也避免了它的缺点,即新方案不仅适合于一般访问结构上的应用,而且各参与者的秘密份额可以重复使用,只需保护一个秘密份额就可以实现任意多个秘密的共享,提高了数据的利用率,从而降低了由于秘密份额更新导致的大的通信复杂度。

*)基金项目:国家 973 项目资助课题(G1999035805);"十五"军事通信技术预研项目资助课题(Y1010122)。**庞辽军** 博士生,主要研究方向为电子商务中的安全理论与技术;**李慧贤** 主要研究领域为电子商务中的安全理论与技术;**王育民** 中国电子学会和中国通信学会会士,中国密码学会理士,IEEE 高级会员,主要研究方向为信息论,密码,编码。

2 数学原理

这里简单介绍一下本文的方案所基于的数学原理，同时它也是方案[5]所基于的数学原理。

定理 1[5] 假设$(y_{i,1}, y_{i,2}, \cdots, y_{i,(t-1)})$，其中$i=1,2\cdots,t$，为满足方程$\sum_{i=1}^{t-1}(x_i-a_i)^2=s$的任意$t$个点。如果它们不在同一$(t-2)$维空间上，那么它们可以唯一地确定该方程。

定理 2[5] 令 p 为一奇素数，如果 2 不是模 p 下的二次剩余，那么任意$z\in[0, p)$可以表示为模 p 下任意$k(k\geqslant 2)$个整数的平方之和。

定理 1 和 2 的证明、$(a_1, a_2, \cdots, a_{t-1})$和 s 的解的存在性及其计算方法请参见文[5]。定理 1 为方案[5]提供了实现秘密共享的思路，它将秘密共享问题转化为确定一个$(t-1)$维空间上的几何图形$\sum_{i=1}^{t-1}(x_i-a_i)^2=s$的问题。容易得知在该图形上的任意$t$个不在同一$(t-2)$维空间上点$(y_{i,1}, y_{i,2}, \cdots, y_{i,(t-1)})(i=1,2\cdots,t)$，就可以唯一地确定该图形，将图形上的$n$个点看作秘密份额(要求任意$t$个点都不在同一$(t-2)$维空间上)，这样就可以实现$(t, n)$门限秘密共享方案。定理 2 为方案[5]的实现提供了一个有效的秘密分发方法。本文的方案也是基于上述定理。

3 本文提出的方案

在介绍本文方案之前，首先简单地介绍一下方案需要用到的双变量单向函数的定义。

定义 1[6] 双变量单向函数：$f(r, u)$表示一个具有两个变量的单向函数，它能够将任意长的 r 和 u 映射为固定长的函数值$f(r, u)$。该函数具有以下 6 条性质：

(1)已知 r 和 u，$f(r, u)$易于计算；

(2)已知 u 和 $f(r, u)$，求 r 在计算上是不可行的；

(3)在 u 未知的情况下，对于任意的 r，求 $f(r, u)$在计算上是不可行的；

(4)已知 u 的情况下，找到不同的 r_1 和 r_2 满足 $f(r_1, u)=f(r_2, u)$在计算上是不可行的；

(5)已知 r 和 $f(r, u)$，求 u 在计算上是不可行的；

(6)已知任意多的$(r_i, f(r_i, u))$对，求 $f(r', u)$在计算上是不可行的，其中$r'\neq r_i$。

下面从三个方面来介绍本文提出的方案：

3.1 系统参数

$f(r, u)$为前面定义过的双变量单向函数；p 是一个形如$8m\pm 3$的大素数，其中 m 为正整数，p 取这种形式是为了保证 2 不是模 p 下的二次剩余；系统工作在有限域 $GF(p)$上；设系统中有 n 个用户 $P_1, P_2, \cdots, P_n$，秘密分发者任意选取 n 个互不相同的$(t-1)$维向量$(z_{i,1}, z_{i,2}, \cdots, z_{i,(t-1)})(i=1,2,\cdots,n)$分别做为参与者的秘密份额；令 $\Gamma=\{\gamma_1, \gamma_2, \cdots, \gamma_k\}$为访问结构。该方案需要一个公告牌(Noticeboard)，秘密分发者将所有的公开信息，如 p，Γ 等信息在公告牌上进行公布。只有秘密分发者可以修改、更新公告牌上的内容，其他人只能阅读或下载。值得说明的是，在几乎所有的秘密共享方案中，公告牌或具有相似功能的工具是必需的[9]，因为在秘密共享过程中至少需要公布参与者的数目、参与者身份等公开信息。

3.2 秘密分发

假设要共享的秘密为 S，这里 S 表示为一个$(t-1)$维向量，即$S=(a_1, a_2, \cdots, a_{t-1})$。秘密分发者首先选取两个随机数 r 和 s，利用 s 和$(a_1, a_2, \cdots, a_{t-1})$构造$(t-1)$维空间上的几何图形$\sum_{i=1}^{t-1}(x_i-a_i)^2=s$；然后，在该几何图形上取任意$(t-1)$个不同的点并公布，表示为 $X_i=(x_{i,1}, x_{i,2}, \cdots, x_{i,(t-1)})(i=1,2,\cdots,t-1)$。对每个授权子集 $\gamma_i=\{P_1, P_2, \cdots P_{|\gamma_i|}\}\in\Gamma$($|\gamma_i|$表示授权子集 γ_i 中参与者的个数)进行以下相同的处理：选取一个唯一的$(t-1)$维空间点 X_{t+i-1}，使得它和前面公布的$(t-1)$个点不在同一$(t-2)$维空间上；计算 γ_i 中每个参与者 P_i 的伪份额 $Y_i=(y_{i,1}, y_{i,2}, \cdots, y_{i,(t-1)})$，其中 $y_{i,j}=f(r, z_{i,j})$；再计算 $D_i=Y_1\oplus Y_2\oplus\cdots\oplus Y_{|\gamma_i|}\oplus X_{t+i-1}=(d_{i,1}, d_{i,2}, \cdots, d_{i,(t-1)})$，其中 $d_{i,j}=y_{1,j}\oplus y_{2,j}\oplus\cdots\oplus y_{|\gamma_i|,j}\oplus x_{(t+i-1),j}$，并将 D_i 的值公布。

秘密分发过程的伪代码表示如下，需要说明的是以下计算都在模 p 条件下进行的。

(Ⅰ)任意选取两个一次性随机数 r 和 s；

(Ⅱ)For $i=1,2,\cdots,n$，执行以下步骤(Ⅱ-1～ Ⅱ-2)

(Ⅲ-1) For $j=1,2,\cdots,t-1$，计算 $y_{i,j}=f(r, z_{i,j})$；

(Ⅱ-2) 令 $Y_i=(y_{i,1}, y_{i,2}, \cdots, y_{i,(t-1)})$；

(Ⅲ)For $i=1,2,\cdots,t+k-1$，执行以下步骤(Ⅲ-1～ Ⅲ-7)；

(Ⅲ-1) For $j=1,2,\cdots,t-3$，执行以下步骤(Ⅲ-2-1～ Ⅲ-2-2)；

(Ⅲ-2-1) 随机选取$(r_{i,j}, w_{i,j})$，满足 $r_{i,j}=w_{i,j}^2$；

(Ⅲ-2-2) 令 $x_{i,j}=w_{i,j}+a_j$ 或 $x_{i,j}=p-w_{i,j}+a_j$；

(Ⅲ-2) 选取$(r_{i,(t-2)}, w_{i,(t-2)})$和$(r_{i,(t-1)}, w_{i,(t-1)})$，满足 $r_{i,(t-2)}=w_{i,(t-2)}^2$，$r_{i,(t-1)}=w_{i,(t-1)}^2$ 和 $r_{i,(t-2)}+r_{i,(t-1)}=s-\sum_{j=1}^{t-3}r_{i,j}$；

(Ⅲ-3) 令 $x_{i,(t-2)}=w_{i,(t-2)}+a_{(t-2)}$ 或 $x_{i,(t-2)}=p-w_{i,(t-2)}+a_{(t-2)}$；

$x_{i,(t-1)}=w_{i,(t-1)}+a_{(t-1)}$ 或 $x_{i,(t-1)}=p-w_{i,(t-1)}+a_{(t-1)}$；

(Ⅲ-4) 令 $X_i=(x_{i,1}, x_{i,2}, \cdots, x_{i,(t-1)})$且 $X'_i=(x_{i,1}, x_{i,2}, \cdots, x_{i,(t-1)}, 1)$；

(Ⅲ-5) 当 $i<t$ 且 $X'_1, X'_2, \cdots, X'_i$ 线性相关时，或者当 $i\geqslant t$，且 $X'_1, X'_2, \cdots, X'_{t-1}, X'_i$ 线性相关或 $X'_t, X'_{t-1}, \cdots, X'_i$ 出现重复时，重复步骤(Ⅲ-1～ Ⅲ-4)；

(Ⅳ)For $i=1,2,\cdots,k$，对于每个合法子集 γ_i 计算 $D_i=Y_1\oplus Y_2\oplus\cdots\oplus Y_{|\gamma_i|}\oplus X_{t+i-1}$；

(Ⅴ)以认证的方式公布 r，$D_i(i=1,2,\cdots,k)$和 $X_i(i=1,2,\cdots,t-1)$，并将 s 和 $X_t, X_{t+1}, \cdots, X_{t+k-1}$销毁。

3.3 秘密重构

在秘密重构过程中，访问结构中的任何授权子集利用它们的秘密份额和公布的信息，可以恢复所共享的秘密。不失一般性，假设授权子集 $\gamma_i=\{P_1, P_2, \cdots, P_{|\gamma_i|}\}$中的参与者要重构秘密 S。首先，每个参与者 P_i 计算他的伪份额 $Y_i=(y_{i,1}, y_{i,2}, \cdots, y_{i,(t-1)})$，其中 $y_{i,j}=f(r, z_{i,j})(j=1,2,\cdots,t-1)$，并提交给指定的秘密恢复者；然后，秘密恢复者根据公开信息 D_i 计算子秘密 $X_{t+i-1}=Y_1\oplus Y_2\oplus\cdots\oplus Y_{|\gamma_i|}\oplus D_i$；最后，由得到的向量 X_{t+i-1}和公开信息 $X_1, X_2, \cdots, X_{t-1}$可以恢复秘密 $S=(a_1, a_2, \cdots, a_{t-1})$，其中，

$$a_i=\frac{\begin{vmatrix} \sum_{j=1}^{t-1}x_{1,j}^2 & x_{1,1} & \cdots & x_{1,(i-1)} & x_{1,(i+1)} & \cdots & x_{1,(t-1)} & 1 \\ \sum_{j=1}^{t-1}x_{2,j}^2 & x_{2,1} & \cdots & x_{2,(i-1)} & x_{2,(i+1)} & \cdots & x_{2,(t-1)} & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \sum_{j=1}^{t-1}x_{(t-1),j}^2 & x_{(t-1),1} & \cdots & x_{(t-1),(i-1)} & x_{(t-1),(i+1)} & \cdots & x_{(t-1),(t-1)} & 1 \\ \sum_{j=1}^{t-1}x_{(t+i-1),j}^2 & x_{(t+i-1),1} & \cdots & x_{(t+i-1),(i-1)} & x_{(t+i-1),(i+1)} & \cdots & x_{(t+i-1),(t-1)} & 1 \end{vmatrix}}{\begin{vmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,(t-1)} & 1 \\ x_{2,1} & x_{2,2} & \cdots & x_{2,(t-1)} & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{(t-1),1} & x_{(t-1),2} & \cdots & x_{(t-1),(t-1)} & 1 \\ x_{(t+i-1),1} & x_{(t+i-1),2} & \cdots & x_{(t+i-1),(t-1)} & 1 \end{vmatrix}}\times\frac{1}{2}\times(-1)^{(i+1)} \qquad (1)$$

4 分析和讨论

4.1 骗子的揭发

对于任何面向群体的秘密共享方案来说，如何发现存在欺骗以及指出骗子非常重要。在本文的方案中，为了防止内部用户或外部攻击者进行欺骗，有必要提供一种方法用来检验秘密重构过程中每个合作的参与者 P_i 提供的伪份额 Y_i 是否真实。防止欺骗的最简单的方法是使用一个强的杂凑函数 $h(x)$。秘密分发者在秘密分发过程中，为每一个参与者 P_i 的伪份额计算杂凑值 $h(Y_i)=h(y_{i,1}\parallel y_{i,2}\parallel\cdots\parallel y_{i,(t-1)})$，其中 $y_{i,j}=f(r, z_{i,j})(j=1,2,\cdots,t-1)$，“$\parallel$”表示链接操作，并将其在公告牌上公布。由杂凑函数的性质可知，由 $h(Y_i)$ 来推导 Y_i 在计算上是不可行的，而且要找到一个向量 $Y'_i\neq Y_i$，使得 $h(Y'_i)=h(Y_i)$，在计算上也是不可行的。这个杂凑值 $h(Y_i)$ 可以被用来检验参与者 P_i 所提交的伪份额 Y_i 的正确性。许多研究人员对预防欺骗这一方面也做了大量的研究，他们的研究成果都可以应用于本文方案来发现欺骗和找出骗子。读者可以参阅文[12]，这里不再赘述。

4.2 安全性分析

尽管在重构秘密 S 时，合作的每个参与者 P_i 必须公开自己的信息 $Y_i=(y_{i,1}, y_{i,2},\cdots, y_{i,(t-1)})$，但是，由双变量单向函数的性质(5)可知，他的秘密份额 $(z_{i,1}, z_{i,2},\cdots,z_{i,(t-1)})$ 不会被披露。而且，公开信息 $D_i(i=1,2,\cdots,k)$ 也不会披露有关秘密任何信息。

一个秘密共享方案必须满足两个基本的要求：一是任意一个授权子集中的参与者的合作可以很容易地计算出所共享秘密；二是非授权子集中的参与者的合作不能得到该秘密的任何信息。在本文方案的秘密重构过程中，要确定方程式 $\sum_{i=1}^{t-1}(x_i-a_i)^2=s$，需要知道 t 个不在同一 $(t-2)$ 维空间的向量 $X_i=(x_{i,1}, x_{i,2},\cdots, x_{i,(t-1)})(i=1,2,\cdots,t)$。由公开信息可以直接得到 $(t-1)$ 个向量 $X_1, X_2,\cdots,X_{t-1}$，必须再得到一个向量才可以重构秘密。对于授权子集 $\gamma_i=\{P_1,P_2,\cdots,P_{|\gamma_i|}\}$，在不存在欺骗的情况下，其中的参与者合作可以得到另一个向量 X_{t+i-1}，即 $X_{t+i-1}=Y_1\oplus Y_2\oplus\cdots\oplus Y_{|\gamma_i|}\oplus D_i$，从而很容易地计算出所共享秘密。而非授权子集的参与者合作则不能得到这样的点。如果一个非授权子集 $\overline{\gamma_i}$ 的参与者或系统外的攻击者想要得到向量 X_{t+i-1}，需要设法得到任何一个合法子集 γ_i 中所有参与者的伪份额的异或值 $C_{\gamma_i}=Y_1\oplus Y_2\oplus\cdots\oplus Y_{|\gamma_i|}$，否则只能凭猜测来获得向量 X_{t+i-1}。由于系统工作在有限域 $GF(q)$ 上，所以猜测 C_{γ_i} 成功的概率仅为 $1/q^{t-1}$；也可以直接对 X_{t+i-1} 进行猜测，其成功的概率也仅为 $1/q^{t-1}$。当 q 足够大时，这种攻击的成功概率接近于 0。因此，本文提出的方案符合秘密共享的安全性要求和规则。

4.3 性能分析

本文方案有非常重要的应用价值，尤其是在共享大的秘密时比其它一般访问结构上的方案[9~11]更为有效。假设所共享的秘密的长度为 $(t-1)\times 512$ 比特，以文[9]中方案为例与本文方案做一比较。采用文[9]中的方案，模 p 的长度至少应为 $(t-1)\times 512$ 比特。而采用本文方案，可以先将该秘密分成 $(t-1)$ 个子秘密，再实现对这 $(t-1)$ 个子秘密的共享，因而，模 p 的长度取 512 比特即可，比起文[9]中的方案，大大地降低了计算复杂度。当然也可以采用文[9]中的方案来分别对这 $(t-1)$ 个子秘密进行共享，这时，尽管模 p 的长度可以取 512 比特，但秘密分发者需要重复秘密分发过程 $(t-1)$ 次，并进行 $(t-1)$ 次秘密份额的分配，同时在秘密重构中，秘密计算者需要重复 Lagrange 插值计算 $(t-1)$ 次。而利用本文方案，秘密分发过程和秘密重构过程都仅需执行一次。可见，本文方案在共享大的秘密时比现有其他方案更为有效。

本文方案中所涉及操作主要有单向函数的计算、数乘、异或操作以及行列式的计算等。显然，方案的性能主要依赖于行列式的计算。行列式的计算实现非常方便，而且 Wiedemann[13] 提出了一种行列式计算的概率算法，能够有效地提高有限域上 $k\times k$ 阶行列式的计算。使用 Wiedemann 的算法必将提高本文提出方案的运算性能，相应的计算复杂度和时间复杂度可以参考文[5,13]。

上述分析表明，本文方案具有以下特点：(1)允许并行地共享多个秘密，一次共享过程可以实现 $(t-1)(t\geqslant 2)$ 个秘密的共享；(2)秘密分发者可以动态地决定每次共享过程所要共享的秘密数量；(3)各参与者的秘密份额可以重用，即多次用来进行秘密共享而不必更新参与者的秘密份额；(4)适合一般访问结构上的应用。

结论 本文基于几何性质并提出了一个一般访问结构上的多重秘密共享方案，其中秘密和各参与者的秘密份额皆为 $(t-1)$ 维向量。与现有一般访问结构上的秘密共享方案相比，本文方案允许并行地共享多个秘密；而且，秘密分发者可以动态地决定每次共享过程所要共享的秘密数量。本文方案有非常重要的应用价值，尤其是在共享大的秘密时比其它一般访问结构上的方案更为有效。分析表明，本文方案是一个安全有效的方案。

参 考 文 献

1 Shamir A. How to share a secret. Communications of the ACM 1979,22(11):612~613

攻击行为系统化分析方法*)

严 芬[1,2,3] 黄 皓[1,2]

(南京大学软件新技术国家重点实验室 南京 210093)[1] (南京大学计算机科学与技术系 南京 210093)[2]

(扬州大学工学院计算机科学与工程系 扬州 225009)[3]

摘 要 针对日益严重的攻击行为,通过对大量攻击以及现有攻击分析方法的研究,本文提出了一个系统地分析和描述攻击行为的方法。此方法不仅能够有效地分析和描述攻击的本质特征,还能分析攻击的过程,具有广泛的适用性。文中还讨论和分析了在此基础上对该方案进行裁剪的原则和方法,以增加其适用性。通过诸多攻击实例验证了所给方案的有效性和适用性。

关键词 安全,攻击,攻击过程,裁剪,裁剪规则

Research on Systematically Describing Attacks

YAN Fen[1,2,3] HUANG Hao[1,2]

(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)[1]

(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)[2]

(Department of Computer Science and Engineering, Technology Institute, Yangzhou University, Yangzhou 225009)[3]

Abstract To deal with the increasingly serious problem of attack, after researched on many attack and existing attack analyzing methods, a systematical method to analyzing and describing attack is put forward in this paper. This method can not only effectively analyze and describe the essence characteristics of attack, but also can analyze attack process, thus it has extensive applicability. Then, how to tailor the method and the corresponding tailoring rule are talked in order to enhancing the method's applicability. The validity and applicability of this schema are validated via many attack examples.

Keywords Security, Attack, Attack process, Tailoring, Tailoring rule

1 引言

计算机和网络的广泛应用和普及,造成攻击日益增多,安全问题越来越突出。为了尽早地防御攻击的发生,更好地检测攻击的存在,有效地采取措施响应攻击,减少攻击造成或可能造成的危害,首先需要对攻击行为本身进行分析和描述。攻击行为的分析和描述具有深远意义,在密码学与信息安全、计算机网络、操作系统、软件工程、计算机应用技术等研究领域都发挥着重要的作用。攻击的复杂多样性导致很难找到一个有效、通用的方法来分析和描述所有的攻击行为。目前,已有的研究工作或者是侧重于对攻击的概念性介绍[1],或者是针对某一个或者某一类攻击行为的详细分析[2],还有一些则侧重于攻击行为模型分析[3]。总的来讲,现有工作缺乏对攻击行为分析和描述的系统性和通用性。

通过对大量攻击行为的分析和研究,在研究攻击分类和攻击方法[4~11]的基础上,本文提出了一个利用多特征属性来分析攻击行为、具有一定的通用性的攻击行为分析方法,并且提出了对其进行不同程度的裁剪后,可以使该方法具有更强的适用性,能更好地用于分析和描述攻击,且可以描述攻击行为之间存在的关联性。文中的攻击分析和描述方法不仅可以有效地分析和描述攻击的本质特性,还可以分析攻击的过程。

本文第2部分介绍系统化的攻击行为分析方法;第3部

*)国家863高技术研究发展计划"分布式网络监控与预警系统"(2003AA142010)和江苏省高技术研究计划"计算机网络分布式主动防御、监控与预警技术研究"(BG2004030)资助项目。严 芬 博士研究生,主要研究方向为网络与信息安全;黄 皓 博士生导师,主要研究方向为计算机信息系统安全、网络与信息安全。

2 Blakley G. Safeguarding cryptographic key. In:Proc. AFIPS 1979 Natl. Conf., New York,1979. 313~317

3 Asmuth C, Bloom J. A Modular approach to key safegrarding [J]. IEEE Transactions On Information Theory, 1983, 29(2):208~210

4 Karnin E D, Green J W, Hellman M E. On sharing secret system [J]. IEEE Transactions On Information Theory, 1983, 29(1):35~41

5 Wu T C, He W H. A geometric approach for sharing secrets [J]. Computers & Security, 1995, 14(2):135~145

6 Pang Liao-jun, Wang Yu-min. A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing [J]. Applied Mathematics and Computation, 2005, 167(2):840~848

7 Yang Chou-Chen, Chang Ting-Yi, Hwang Min-Shiang. A (t, n) multi-secret sharing scheme [J]. Applied Mathematics and Computation, 2004, 151(2):483~490

8 Benaloh J, Leichter J. Generalized secret sharing and monotone functions [A]. Advance in Cryptology-Crypto'88 [C], Springer-Verlag, Berlin, 1990. 27~35

9 Hwang Ren-Junn, Chang Chin-Chen. An on-line secret sharing scheme for multi-secrets [J]. Computer Communications, 1998, 21(13):1170~1176

10 Wang Shiuh-Jeng. Direct construction of a secret in generalized group-oriented cryptography [J]. Computer Standards and Interfaces, 2004, 26(5):455~460

11 Yuanbo Guo, Jianfeng Ma. An efficient and secure fault-tolerant conference-key distribution scheme [J]. IEEE Transactions on Consumer Electronics, 2004, 50(2):571~575

12 Tan K J, Zhu H W, Gu S J. Cheater identification in (t, n) threshold scheme [J]. Computer Communications, 1999, 22: 762~765

13 Wiedemann D H. Solving sparse linear equations over finite fields [J]. IEEE Transaction on Information Theory, IT-32(1), 1981. 54~62