第 43 卷 第 6A 期
2016 年 6 月

计 算 机 科 学
Computer Science

Vol. 43 No. 6A
June 2016

# 一种属性基加密方案的外包解密方法

丁晓红 秦敬源 王 新
(大连海洋大学信息工程学院 大连 116023)

摘 要 Sahai 和 Waters 提出的属性基加密(Attribute-Based Encryption,ABE)能够实现一对多加密,因而具有广泛的应用价值。随着云计算技术的不断发展,云计算也与属性基加密有了紧密的联系。将快速高效的外包技术应用在属性基解密算法中。在云计算中,云服务器存储了客户的密文。当客户对远程数据进行解密时,解密者将转换密钥上传给云服务器。云服务器利用转换密钥将密文转换成一个中间密文并发送给客户,客户解密中间密文并获得明文的计算量很小,从而减轻了解密者的负担。安全性分析和效率分析证明所提出的方法是安全的和高效的。

关键词 属性基加密,数据外包,快速解密
中图法分类号 TP309 文献标识码 A

## Attribute-based Encryption Scheme with Outsourcing Decryption Method

DING Xiao-hong QIN Jing-yuan WANG Xin
(School of Information Engineering, Dalian Ocean University, Dalian 116023, China)

**Abstract** Sahai and Waters proposed ABE (Attribute-based Encryption) which realizes one to more encryption. ABE has extensive application value. With the continuous development of cloud computing, cloud computing is also closely linked with attribute based encryption. This paper applied the rapid and efficient outsourcing computation technique into ABE decryption algorithm. In cloud computing, the cloud server stores the clients' ciphertexts. When the client decrypts its remote data, the decryptor uploads the transform key to the cloud server. By using the transform key, the cloud server transforms the ciphertext into semi-ciphertext and sends it to client. The client decrypts the semi-ciphertext and gets the plaintext. This outsourcing computation technique saves the clients' computation overhead. Through security analysis and efficiency analysis, our proposed scheme is secure and efficient.

**Keywords** Attribute-based encryption, Outsourcing, Fast decryption

## 1 引言

基于模糊身份基的加密,Sahai 和 Waters 提出了属性基加密体制[1]。在属性基加密体制中,用户身份由一系列属性来表示。在 ABE 体制中,用户能否解密密文是由某个函数 $f(\cdot)$ 控制的。设用户的属性集为 $S$,如果 $f(S)=1$,那么拥有属性集 $S$ 的用户可以对密文进行解密。根据访问结构是跟密文相结合还是与用户密钥相结合,ABE 分为密钥策略属性基加密(Key-Policy ABE,KP-ABE)和密文策略属性基加密(Ciphertext-Policy ABE,CP-ABE)[2,3]。在 KP-ABE 中,用户密钥和访问结构相结合,而密文与属性集相关,消息被加密后,授权的用户利用自己的属性获取密钥,从而解密他有权访问的密文;在 CP-ABE 中,密文和访问结构相结合,而密钥与属性集相关,访问策略由消息发送方指定,数据加密之后就确定了哪些用户能够对它进行解密[4]。本文研究 KP-ABE 机制。

在基于双线性对的 ABE 方案中,解密过程中由于双线性对计算消耗较大,使得计算能力受限的终端设备受到限制,解密密文所需的双线性对的数目随着访问策略的复杂性增长而增长[5]。在大数据时代,用户需要保护的信息越来越多,加密者所设计的访问结构会越来越复杂,这对移动终端设备是一个极大的挑战,比如计算能力、电池的寿命等[6]。随着云计算的兴起,前面提出的挑战也迎刃而解了,通过云服务器的计算能力,可以将数以万计的信息利用硬件设备在数秒之内处理。密码学的研究被引进了云计算后,将一部分比较复杂的算法外包给云服务器,云服务器将计算完的结果反馈给有权访问密文的用户,这样不仅减轻了用户的负担而且提高了效率。

本文使用了 ElGamal 密钥和转换密钥[7],ElGamal 密钥是用户私有的,只有用户自己知道,而转换密钥被分享给云服务器。在"Transform"算法中,利用了云计算的计算能力,通过转换密钥将密文转为一个更简单的密文给授权解密的用户,客户解密中间密文并获得明文的计算量很小,从而减轻了解密者的负担。为了降低用户的计算消耗,使用了 GPSW 系统[8]提出的技术,将双线性对操作外包给云服务器完成[9]。本文提出了一个外包解密的属性基加密方案,降低了计算能力受限的移动终端设备的计算负担,提高了效率。

## 2 预备知识

### 2.1 双线性对

设 $G$ 和 $G_T$ 是两个阶为素数 $p$ 的乘法群,$g$ 是 $G$ 的生成

丁晓红(1990—),女,硕士生,主要研究方向为属性基加密。

元，双线性映射 $e:G\times G\to G_T$ 满足下述性质：

1）可计算性：对任意的 $u,v\in G$，存在有效的算法计算 $e(u,v)$；

2）双线性：任意的 $a,b\in z_p$，都满足 $e(g^a,g^b)=e(g,g)^{ab}$；

3）非退化性：存在 $u,v\in G$，满足 $e(u,v)\neq 1$，其中 $1$ 代表群 $G_T$ 的单位元。

决策双线性对 Diffie-Hellman 问题：

对于给定的元组 $\langle g,g^a,g^b,g^c,Z\rangle$，其中 $a,b,c\in Z_p^*$，$Z\in G$，检测 $Z$ 与 $e(g,g)^{abc}$ 是否相等。

本文中，假设决策双线性对 Diffie-Hellman 问题是困难的。

### 2.2 线性秘密分享机制(Liner Secret Sharing Schemes, LSSS)

如果一个秘密分享机制 $\Pi$ 是线性的，那么：

1）每个参与者的秘密份额是 $Z_p$ 的一个向量；

2）存在一个 $l\times n$（$l$ 行，$n$ 列）的矩阵，称为 $\pi$ 的秘密分享矩阵，存在一个函数 $\rho$ 可以映射矩阵中的每一行到相应的参与者，对于 $i=1,\cdots,l$，函数 $\rho(i)$ 的值是与 $i$ 行相关的参与者。考虑一个列向量 $v=(s,r_2,\cdots,r_n)$ 是要被分享的秘密，其中 $s\in Z_p$，随机选择 $r_2,\cdots,r_n\in Z_p$，那么 $Mv$ 是关于 $\Pi$ 的秘密 $s$ 的 $l$ 份分享的向量，其中分享向量 $(Mv)_i$ 属于每一个参与者 $\rho(i)$。

文献[10]中指出，每个满足上述定义的秘密分享方案都具有线性重构的性质：假设 $\Pi$ 是一个访问结构 $A$ 的线性秘密分享方案，设 $S\in A$ 是任意的授权集合，$I\subseteq\{1,2,\cdots,l\}$ 定义为 $I=\{i:\rho(i)\in S\}$，如果 $\lambda_i$ 是 $S$ 的任意秘密值 $s$ 的有效分享，那么一定存在常量 $\{\omega_i\in Z_p\}_{i\in I}$ 使得 $\sum_{i\in I}\omega_i\lambda_i=s$。

### 2.3 访问结构

$\{P_1,P_2,\cdots,P_n\}$ 是一个实体集，集合 $A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$，若对于 $\forall B,C$，当 $B\in A$ 且 $B\subseteq C$ 时有 $C\in A$，则称集合 $A$ 为单调的。一个访问结构（通常指单调访问结构）是 $\{P_1,P_2,\cdots,P_n\}$ 的一个非空子集 $A$，即 $A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}\setminus\{\emptyset\}$。包含于 $A$ 中的集合为授权集合，不包含于 $A$ 中的集合为非授权集合。

## 3 构造解密计算外包的 KP-ABE 方案

文中的方案包含以下步骤：Setup，Encrypt，$\text{KeyGen}_{\text{out}}$，$\text{Transform}_{\text{out}}$，$\text{Decrypt}_{\text{out}}$，具体如下：

$\text{Setup}(\lambda,u)\to(PK,MK)$。输入安全参数 $1^\lambda$、属性集 $U=\{0,1\}^*$，随机选择一组 $h_1,h_2,\cdots,h_n\in G$ 和 $\alpha\in Z_p$，输出系统公钥 $PK=(G,p,g,e(g,g)^\alpha,h_1,h_2,\cdots,h_n)$，$MK=(PK,\alpha)$。

$\text{Encrypt}(PK,m,S)\to CT$。输入公钥 $PK$、消息 $m(m\in G_T)$ 和属性集 $S$，选择一个随机值 $s\in Z_p$，输出 $CT=(S,C,\overset{\wedge}{C},\{C_x\}x\in S)$，$C=m\cdot e(g,g)^{\alpha s}$，$C'=g^s$，$\{C_x=h_x^s\}x\in S$。

$\text{KeyGenout}\ (MK,A(M,\rho)))\to SK$。秘钥生成算法是将主密钥和线性访问结构作为输入，其中函数 $\rho$ 与 $M$ 矩阵的每一行相关，访问结构 $A$ 与线性的秘密分享矩阵 $M$ 相关。该算法首先选择一个向量 $\vec{v}=(\alpha,y_2,y_3,\cdots,y_n)\in Z_p^n$，这些值是为了分享主钥 $\alpha$，对于 $i\in[1,l]$，有 $\lambda_i=\vec{v}\cdot M_i$，$M_i$ 是秘密分享矩阵第 $i$ 行所对应的向量（$M$ 是一个 $l\times n$ 的矩阵），然后该算法定义一个 $\Gamma$ 来表示在矩阵 $M$ 中的可区分属性集，并且 $\Gamma=\{d:\exists i\in[1,l],\rho(i)=d\}$，然后该算法随机选择 $r_i\in Z_p$，得到 $SK'=(K_i',R_i',Q_i')$，其中 $k_i'=g^{\lambda_i}\cdot h_{\rho(i)}^{r_i}$，$R_i'=g^{r_i}$，$\forall d\in\Gamma/\rho(i)$，$Q_i'=h_d^{r_i}$，$i\in[1,l]$。随机选择一个值 $z\in Z_p^*$，得到转换密钥 $TK=(PK,K_i,R_i,Q_i)$，其中 $k_i=g^{\frac{\lambda_i}{z}}\cdot h_{\rho(i)}^{\frac{\lambda_i}{z}}$，$R_i=g^{\frac{\lambda_i}{z}}$，$Q_i=h_d^{\frac{r_i}{z}}$，$\forall d\in\Gamma/\rho(i)$，$i\in[1,l]$，输出私钥 $SK(z,TK)$。

$\text{Transform}_{\text{out}}Tk,CT\to CT'$。转换算法将与访问结构 $(M,\rho)$ 相关的转换密钥 $TK$ 和与属性集 $S$ 相关的密文 $CT$ 作为输入，如果访问者的属性集不满足访问结构 $A$，那么访问被终止；否则，令 $I\subseteq\{1,2\cdots,l\}$，根据秘密分享方案 $\text{LSSS}(M,\rho)$ 的性质，存在 $\{\omega_i\}_{i\in I}\in Z_p$ 使得下面的式子成立：

1）对于所有的 $i\in I$，$\rho(i)\in S$。

2）$\sum_{i\in I}w_i\cdot M_i=(1,0,0,\cdots,0)$。

定义 $\Delta=\{x:\exists i\in I,\rho(i)=x\}$，$I$ 表示一个可能用来解密密文矩阵中的相关行的集合，而 $\Delta$ 是与这些行有关的可以区分的属性集合，即 $\Delta\subseteq S$，$S$ 是用来加密密文的属性集，$\Delta\subseteq\Gamma$，$\Gamma$ 是用来产生私钥的属性集。为了减小 $I$，定义一个函数 $f(\cdot)$ 使得一个属性集转换成群 $G$ 的元素，$f(\Delta)=\prod_{x\in\Delta}h_x$。

在解密之前还要将私钥和密文进行预处理，对于 $i\in I$，处理为：

$$\overset{\wedge}{k}_i=k_i\cdot\prod_{x\in\Delta/\rho(i)}Q_{i,x}=g^{\frac{\lambda_i}{z}}f(\Delta)^{\frac{r_i}{z}}$$

$$L=\prod_{x\in\Delta}C_x=\prod_{x\in\Delta}h_x^s=f(\Delta)^s$$

转换算法可以通过下面的式子恢复出 $e(g,g)^{\alpha s/z}$：

$$e(\overset{\wedge}{C},\prod_{i\in I}\overset{\wedge}{k}_i^{\omega_i})/e(\prod_{i\in I}R_i^{\omega_i},L)=e(g^s,\prod_{i\in I}g^{\lambda_i\omega_i/z}f(\Delta)^{r_i\omega_i/z})/e(\prod_{i\in I}g^{r_i\omega_i/z},f(\Delta)^s)=e(g,g)^{\alpha s/z}\cdot e(g,f(\Delta))^{s/z\sum_{i\in I}r_i\omega_i}/e(g,g)^{s/z\sum_{i\in I}r_i\omega_i}=e(g,g)^{\alpha s/z}$$

输出密文 $CT'$ 为 $(C,e(g,g)^{\alpha s/z})$。

$\text{Decrypt}_{out}(SK,CT)\to m$。解密算法将私钥 $SK(z,TK)$ 和密文 $CT$ 作为输入，如果密文没有被部分解密，那么算法先执行 $\text{Transform}_{\text{out}}$，如果执行结果输出为 $\perp$，那么解密算法输出也为 $\perp$，如果执行结果输出正确，那么已知密文 $(T_0,T_1)$ 并计算 $T_0/T_1^z$，最后输出消息 $m$。

## 4 方案分析

这一部分给出了快速外包解密的属性基加密方案的正确性、安全性以及它的性能的分析。

### 4.1 正确性分析

当用户的访问结构满足密文中的属性集时，用户可以对密文进行解密，根据密文 $(T_0,T_1)$，通过计算 $T_0/T_1^z$，得出正确的消息 $m$，其中 $T_0=me(g,g)^s$，$T_1=e(g,g)^{\frac{s}{z}}$，过程如下：

$$\frac{T_0}{T_1^z}=\frac{me(g,g)^s}{e(g,g)^{\frac{s}{z}\cdot z}}=\frac{me(g,g)^s}{e(g,g)^s}=m$$

因此，文中的方案是正确的。

### 4.2 安全性分析

定理 1 若 DBDH 假设成立，那么攻击者在多项式时间内不能攻破我们的系统。

本方案具有在标准模型下的选择明文攻击的安全性，利用反正法证明。假设存在一个攻击者 $A$ 在游戏 $GM_1$ 和 $GM_2$ 中以不可忽略的优势 $\varepsilon$ 赢得了游戏。构造一个模拟器 $B$，只要证明模拟器 $B$ 利用攻击者 $A$ 以不可忽略的概率 $\frac{\varepsilon}{2}$ 区分了 $Z=e(g,g)^{abc}$ 和 $Z=e(g,g)^z$，即解决了 DBDH 困难问题，得

出矛盾，于是证明了文中的方案是安全的。挑战者给模拟器的挑战为$(g,A,B,C,Z)=(g,g^a,g^b,g^c,g^z)$。过程如下：

首先，将安全参数$K$作为输入，输出系统公钥参数，包括$G_0$、$G_T$、$G_0$生成元$g$以及双线性映射$e:G_0\times G_0\rightarrow G_T$，挑战者随机选择$a,b,c,z\in Z_p^*$，令$A=g^a$，$B=g^b$，$C=g^c$。挑战者随机抛出一枚硬币，得到随机值$u\in\{0,1\}$，如果$u=0$，令$Z=e(g,g)^{abc}$，选择是$GM_1$游戏，如果$u=1$，令$Z=e(g,g)^z$，选择是$GM_2$。定义属性的全域为$U$。

1）初始化：攻击者$A$选择一个属性集$S^*$交给模拟器$B$。

2）建立阶段：模拟器B设置$Y=e(A,B)=e(g,g)^{ab}$，令$\alpha=ab+a^{q+1}$，则$e(g,g)^\alpha=e(g,g)^{ab}e(g^{a^q},g^a)$，选择随机值$z_1,z_2,\cdots,z_{|u|}\in Z_p$，对于属性集中所有的属性$1\leqslant x\leqslant|u|$，有$h_x=\begin{cases}g^{z_x}, & x\in S^*\\ g^{z_x}g^{a^x}, & x\notin S^*\end{cases}$，把公钥参数发送给攻击者$A$，由于$z_x$和$ab$的存在，参数都是随机分布的。

3）查询阶段1：攻击者$A$对模拟器$B$进行私钥的问询。访问结构为$(M,\rho)$，$M$是一个$l\times n$矩阵，假设属性在$S^*$中的行表示为$T(i\in T,\rho(i)\in S^*)$，否则表示为$T'$。定义一个$n$阶的向量$\vec{v}=(v_1,\cdots,v_n)\in Z_p^{n^*}$，令$v_1=1$且对于所有$\rho(i)\in S^*$，有$\vec{v}\cdot M_i=0$，根据$LSSS$这样的向量是存在的，如果$S^*$不满足$M$，那么向量$(1,0,0,\cdots,0)$一定不在$M$行中，这些向量值是为了分享主密钥$\alpha$，对于$i\in[1,l]$，得到$\lambda_i=(\vec{\alpha v})\cdot M_i$。由于$i\in T,\lambda_i=0$，因此所有部分都是单位元素$K_i=R_i=g^0$。下面考虑$i\in T'$，令$t_i=\vec{v}\cdot M$，则$\lambda_i=t_i\cdot\alpha=t_i\cdot(ab+a^{q+1})$，令$R_i=g^{\frac{-c_ia^{q+1}-\rho(i)}{z}}$，$r_i=-c_ia^{q+1-\rho(i)}$，随机选择$z\in Z_p^*$模拟器计算$K_i$为：

$$\begin{aligned}K_i&=g^{\frac{c_i^{ab}}{z}}\cdot R_i^{z_i}\\&=g^{\frac{c_iab}{z}}\cdot g^{\frac{-z_ic_ia^{q+1}-\rho(i)}{z}}\\&=g^{\frac{c_iab}{z}}\cdot g^{\frac{c_ia^{q+1}}{z}}\cdot g^{\frac{-z_ic_ia^{q+1}-\rho(i)}{z}}\cdot g^{\frac{-c_ia^{q+1}}{z}}\\&=g^{\frac{c_i\alpha}{z}}\cdot(g^{z_i})^{\frac{r_i}{z}}\cdot(g^{a^{\rho(i)}})^{\frac{r_i}{z}}\\&=g^{\frac{c_i\alpha}{z}}\cdot h_{\rho(i)}^{\frac{r_i}{z}}\end{aligned}$$

接下来计算帮助值。对于所有$x\in\Gamma/\rho(i)$，令$Q_{i,x}=h_x^{\frac{r_i}{z}}$，过程如下：

$$h_x^{\frac{r_i}{z}}=$$

$$\begin{cases}(g^{z_x})^{\frac{r_i}{z}}=g^{\frac{-z_xc_ia^{q+1}-\rho(i)}{z}}, & x\in S^*\\ (g^{z_x})^{\frac{r_i}{z}}(g^{a^x})^{\frac{r_i}{z}}=g^{\frac{-z_xc_ia^{q+1}-\rho(i)}{z}}\cdot g^{\frac{-c_ia^{q+1}-\rho(i)+x}{z}}, & x\notin S^*\end{cases}$$

将私钥返回给攻击者$A$。

4）挑战阶段：攻击者$A$选择两个长度相等的明文$M_0$、$M_1$发送给模拟器$B$，随机选择一个$v\in\{0,1\}$，对$M_v$进行加密：$C=M_vZ$；$C'=g^c$；若每个属性满足访问结构$M$，则有$C_{w_i}=h_{w_i}^c(w_i\in M)$，否则$C_{w_i}$为随机值。

如果$v=0$，则$Z=e(g,g)^{abc}$，如果令$s=c$，则$Y^s=(e(g,g)^{ab})^c=e(g,g)^{abc}$，$C'=g^s=g^c$，$C_{w_i}=h_{w_i}^s=h_{w_i}^c(w_i\in M)$，因此密文是对$M_v$的有效随机加密。

如果$v=1$，则$Z=e(g,g)^z$，$C=M_vZ=M_ve(g,g)^z$，由于$z$是$G_2$随机产生的，攻击者不能得到消息的信息。

输出密文$CT=\{C,C',C_{w_i},w_i(1\leqslant i\leqslant n)\}$。

5）查询阶段2：重复第1阶段的过程。

6）猜测阶段：攻击者$A$输出对$v$的猜测$v'$。攻击者$A$猜出$v'=v=0$的概率为$\mathrm{pr}[v'=v=0]=\frac{1}{2}+\varepsilon$，攻击者$A$猜出$v'=v=1$的概率为$\mathrm{pr}[v'=v=1]=\frac{1}{2}$，那么模拟者在与挑战者之间的游戏中成功的概率为：$Adv_s=\frac{1}{2}(\mathrm{pr}[v'=v=0]+\mathrm{pr}[v'=v=1])-\frac{1}{2}=\frac{1}{2}\times(\frac{1}{2}+\varepsilon+\frac{1}{2})-\frac{1}{2}=\frac{\varepsilon}{2}$。

### 4.3 效率分析

本文提出了一种快速外包解密的属性基方案，解密时只需要两个线性对和两个指数的操作，文中的$|\Gamma|$是矩阵$M$中可区分属性集，$|\Gamma|\leqslant l$，因而有$|\Gamma\cdot l\leqslant l^2$。为了缩小密文的长度，本文在解密阶段采用了$\Delta$(可区分属性集)，并对私钥做了预处理工作，与文献[2]方案相比，提高了解密时的效率。本文方案与文献[2]方案的对比情况如表1所列。

表1 本文方案与文献[2]方案的对比情况

| 方案 | ABE类型 | 安全类型 | 密文的大小 | 解密操作 | 外包密文大小 | 外包解密操作 |
|---|---|---|---|---|---|---|
| GPSW[2] | KP | CPA | $\|G_T\|+(1+s)\|G\|$ | $\leqslant(1+1)P+21E_0$ | — | — |
| 本文方案 | KP | CPA | $\leqslant\|G_T\|+(1+s)\|G\|$ | $\leqslant(1+1)P+21E_0$ | $2\|G_T\|$ | $E_T$ |

其中，$s$表示属性集的长度，$l$表示LSSS访问结构$l\times n$矩阵中的行数，$P$代表计算双向性对的最大时间，$E_G$代表在$G$中计算指数的最大时间，$E_T$代表在$G_T$计算中指数的最大时间，对比中忽视了一些次要的操作。

结束语 随着通信技术与计算机网络的不断发展，迎来了大数据时代，而云计算支撑着大数据的处理，因此云计算成为众人追捧的工具，信息的传播主要依靠网络，在存储和传播的过程中，信息安全也顺势成为一个重中之重的研究热点。本文提出了一种快速外包解密的属性基方案，该方案将密文外包给云服务器，在“Transform”算法中，通过转换密钥将密文转为一个更简单的密文给授权解密的用户，客户解密中间密文并获得明文的计算量很小，从而减轻了解密者的负担。为了节约用户的计算消耗，云服务器增加了效率，减轻了用户直接解密时移动设备以及台式机的负担。本方案的研究在高效性和安全性方面表现出现实的意义。

## 参考文献


[1] Sahai A, Waters B. Fuzzy identity-based encryption[M]// Cramer R, ed. EUROCRYPT 2005. Springer, Heidelberg, 2005: 457-473

[2] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine grained access control of encrypted data[C]// ACM Conference on Computer and Communications Security. 2006: 89-98

[3] Waters B. Ciphertext-Policy Attribute-Baded Encryption: An Expressive, Efficient, and Provably Secure Realization[C]// Public

Key Cryptography(PKC 2011). 2011:53-70

[4] 马丹丹,陈勤,党正芹,等. 基于多属性机构的密文策略和加密机制[J]. 计算机工程,2012,38(10):114-116

[5] Lai Lun-zuo, Deng R H, Guan Chao-wen, et al. Attribute-Based Encryption With Verifiable Outsourced Decryption[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(8):1343-1354

[6] Green M, Hohenberger S, Waters B. Outsourcing the Decryption of ABE Ciphertexts[C]// Proceedings of the 20th USENIX Conference on Security. 2011

[7] Gamal T E. A public key encryptosystem and a signature scheme-based on discrete logarithms[M]// Advances in Cryptology: Proceedings of CRYPTO 84. 1985:10-18

[8] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// ACM Conference on Computer and Communications Security. 2006: 89-98

[9] 石岳蓉,郭俊,赵晶晶,等. 高效数据外包的基于多授权中心的ABE方案[J]. 信息技术,2015(2):97-100

[10] Beimel A. Secure Schemes for Secret Sharing and Key Distribution [D]. Israel Institute of Technology, Technion, Haifa, Israel, 1996

(上接第 334 页)

两种传统算法的对比结果可以看出,本文算法在去重率接近传统算法的基础上,具有较高的准确率(达 0.9 以上),同时显著提高了去重时间效率,具有很好的去重效果。

4.2.2 基于不同数据集的方法进行去重效果实验

在不同的情况下 Snort 产生重复告警的比例并不太一样,通常在有攻击行为发生时重复告警比例很高,而正常网络中的重复告警数量较少。为了验证在重复告警比例不同的情况下本文算法的有效性,采用 Dapar1999 第 1、3 周不包含任何攻击的正常纯净数据集、第 2 周中插入了包含 18 种类型的 43 次攻击实例的数据集和 DARPA2000 的 LLDOS 1.0 数据集中截取纯攻击数据集进行测试,实验结果如图 2 所示。

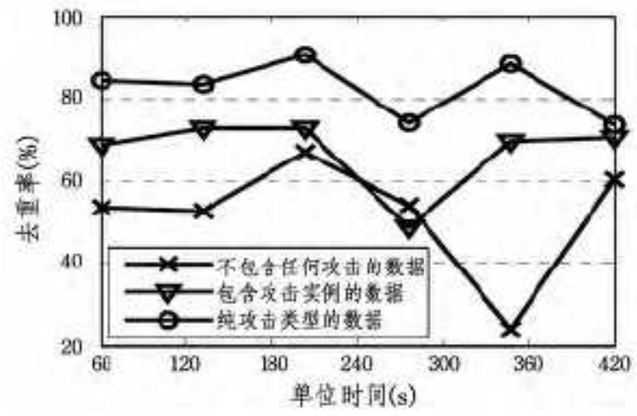


图 2 不同类型数据集在单位时间内的去重率

本文算法采用不同的测试样本,以去重率为指标对效果进行比较分析。对不包含任何攻击的正常纯净数据集的 Dapar1999 第 1、3 周数据来说,其去重率比较低;从 Snort 检测分析捕获的数据包匹配入侵行为的特征原理来说,网络中正常流量包的告警次数以及重复告警频率都远没有 DARPA2000 的 LLDOS 1.0 数据集中截取纯攻击数据集的高。通过分析 Snort 系统告警日志,本文方法去重率与测试样本中的重复日志比例基本一致。

结束语 本文针对大规模网络的安全态势感知系统中的告警日志去重问题,提出了采用基于属性哈希的日志去重方法,其充分考虑了告警日志去重操作的准确性、高效性和大量数据对存储内存容量的需求。实验结果表明,与传统属性比对算法相比,本文算法基本保持了原有算法的准确率、去重率等性能,并显著缩短了运行时间,有效降低了时间复杂度;同时,可处理大容量数据的特性使本文算法适用于大型网络的告警日志去重操作。

## 参 考 文 献

[1] 郭帆,叶继华,余敏. 一种分步式 IDS 告警聚合模型的设计和实现[J]. 计算机应用研究,2009,26(1):325-330

[2] 刘夏龙. 入侵检测告警数据的过滤与聚合技术研究[D]. 北京:中国科学院研究生院,2012

[3] Andersson D, Fong M, Valdes A. Heterogeneous Sensor Correlation: A Case Study of Live Traffic Analysis[C]// Proceeding of Third Ann. IEEE Information Assurance Workshop: IEEE Computer Society. StuartFeldman, MikeUretsky, New York, USA, June 2002:198-207

[4] Valdes A, Skinner K. Adaptive, Model-Based Monitoring for Cyber Attack Detection[C]// Proceeding of RAID2000 Conf: RAID 2000. 2000:204-217

[5] Valdes A, Skinner K. An Approach to Sensor Correlation[C]// Proceeding of Int'l Symp: Recent Advances in Intrusion Detection: IEEE Computer Society. 2000:197-201

[6] Valdes A, Skinner K. Probabilistic alert correlation[C]// Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID 2001). Davis, CA, USA, 2001, London, UK: Springer, 2001:54-68

[7] 王源. 一种基于 Simhash 的文本快速去重算法[D]. 吉林:吉林大学,2014

[8] 张曼等. 基于 SHA-1 的邮件去重算法[J]. 计算机工程,2008,34(11):270-272

[9] 黄思斯. 基于多 IDS 系统的攻击场景重建方法的研究[D]. 武汉:华中科技大学,2007

[10] 黄汉永,肖杰,张驹. 一种基于 Hash 函数抽样的数据集流聚类算法[J]. 计算机系统应用,2009,18(3):73-75

[11] Mit L L. DARPA 2000 intrusion detection evaluation datasets [OL]. (2000). http://ideval.ll.mit.edu/2000 index.html

[12] Mit L L. DARPA1999 intrusion detection evaluation datasets [OL]. (1999). http://www.ll.mit.edu/2st/ideval/data/1999/1999-data-index.html

[13] 尹美娟. 基于邮件正文的邮箱用户别名抽取[J]. 计算机科学,2011,38(12):200-202