基于访问树的策略隐藏文件层次属性加密方案

许盛伟[1,2] 郭春锐[1,2] 袁 峰[1] 任雄鹏[1,2] 杨 森[1]

[1](北京电子科技学院 北京 100070)

[2](西安电子科技学院通信工程学院 陕西 西安 710071)

摘 要 针对具有多级层次特点的文件,提出一种高效的多机构授权的策略隐藏的属性加密方案。采用分层级的树形结构实现文件的加密,可有效抵抗合谋攻击,同时在标准假设下证明了方案的安全性。在该方案中,用户私钥由中央授权机构和多个属性授权机构共同生成,可防止私钥泄露带来的危害影响;采用分层级的树形结构加密既节省了密文存储空间又减少了加密的时间成本。该方案在文件数目较多的情况下,在加解密方面具有很高的效率。

关键词 文件多级层次 属性加密 多授权机构 策略隐藏

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2021.02.052

ENCRYPTION SCHEME OF POLICY HIDDEN FILE HIERARCHY ATTRIBUTE BASED ON ACCESS TREE

Xu Shengwei[1,2] Guo Chunrui[1,2] Yuan Feng[1] Ren Xiongpeng[1,2] Yang Sen[1]

[1](*Beijing Electronic Science & Technology Institute*, *Beijing 100070*, *China*)

[2](*School of Telecommunications Engineering*, *Xidian University*, *Xi' an 710071*, *Shaanxi*, *China*)

Abstract Aiming at the files with multi-level characteristics, this paper proposes an efficient attribute encryption scheme with multi- agency authorization policy hiding. The scheme used hierarchical tree structure to encrypt files, which could effectively resist collusion attacks. The security of the scheme was proved under standard assumptions. The user's private key was jointly generated by the central authority and multi-agency authorization, which could prevent the harmful effects of private key disclosure. The hierarchical tree structure could save the storage space of ciphertext and reduce the time cost of encryption. In the case of large number of files, the scheme has high efficiency in encryption and decryption.

Keywords File hierarchy Attribute encryption Multi-authority Policy hiding

0 引 言

近年来,随着云计算的流行,大量计算以及存储从物理本机被挪至云端[1],为用户节约了大量的存储空间,受到了广大用户的喜爱。但是将数据存储在云服务器上,并不是特别安全,可能会由于云提供商搜集用户存储的消息,导致重要信息的泄露。怎样解决云存储中数据的安全问题,已经成为人们急需解决的重要问题之一[2]。近年来,基于属性加密方案的出现不仅解决了云中所存数据的安全问题,同时也实现了用户的细粒度授权,因此受到了越来越多的关注。

Sahai 等[3]最先提出了基于属性的加密方案(Attributed-Based Encryption,ABE)。在该方案中,数据属主通过设定访问策略,根据属性完成加密,在解密过程中,不用获得数据访问者的具体身份信息,只用关注解密者的属性是否满足加密者设定的加密策略。Goyal 等[4]又将 ABE 划分为两种加密方案,一种是基于密文策略,简称 CP-ABE,另一种是基于密钥策略,简称 KP-ABE[5]。最早提出的 CP-ABE 加密体制中,访问结构

收稿日期:2019 - 05 - 23。国家重点研发计划项目(2018YFB0803600)。**许盛伟**,副教授,主研领域:信息安全,密码应用。**郭春锐**,硕士生。**袁峰**,助理研究员。**任雄鹏**,硕士生。**杨森**,硕士生。

直接以明文形式存在,从而导致重要信息暴露。Nishide 等[6]提出了一种加密方案,可以实现数据属主将数据加密的同时,也完成了策略隐藏,防止了敏感信息的泄露。近年来,文献[7-8]又结合已有方案提出了新的方案,解决了隐藏策略过程中遇到的问题。

在大多数 CP-ABE 加密体制中,密钥只是由单一的可信的权威机构生成,这种做法不仅非常不安全,同时也不能实现用户的跨域访问,一旦权威机构被攻破,敌手获得密钥后,就可以从密文中获得明文数据。Chase[9]提出了一种 ABE 加密方案,将单个权威机构变为多个授权机构,很好地解决了上述问题。Waters[10]提出了一种分布式的 CP-ABE 加密方案,首次通过 LSSS 矩阵完成了 ABE 加密。后续文献[11-12]提出了分布式的属性基加密方案,其优点是密文为定长的。文献[13]在多机构授权的基础上,将策略进行了隐藏。

在现有的针对云文件属性加密的方案中,针对多个层次结构文件的研究还不是特别深入,但是也有学者们提出了一些方案[14-18],但是加解密效率不是特别理想。文献[19]提出了一种多级层次结构的 CP-ABE 方案。该方案通过使用分层的访问结构模型解决多层次文件共享的难题,但是其将树形的访问结构以明文的形式发送给用户,容易造成一些敏感信息的泄露。

本文针对具有多级层次结构特点的文件,提出一种采用分层级的树形结构且策略隐藏的属性加密方案,同时在本方案中有多个授权机构共同工作。采用分层级的树形结构可以减少加密成本,同时访问策略的隐藏防止了敏感信息的泄露。文中用户密钥是由中央授权机构和多个属性授权机构共同生成,防止了单个授权机构被攻击导致密钥泄露的难题。

1 预备知识

1.1 双线性映射

设 G 和 G_T 分别是阶为素数 p,生成元为 g 的乘法循环群,其双线性映射 $e:G\times G\rightarrow G_T$,$e$ 满足以下性质:

(1) 双线性。对 $\forall\mu,\nu\in G,a,b\in \mathbf{Z}_p$,都有 $e(\mu^a,\nu^b)=e(\mu,\nu)^{ab}$。

(2) 非退化性。存在 $\mu,\nu\in G$,使得 $e(\mu,\nu)\neq 1$。

(3) 可计算性。对所有 $\mu,\nu\in G$,存在有效计算 $e(\mu,\nu)\neq 1$。

1.2 复杂性假设 DBDH

设群 G、G_T 为乘法群,阶为 p,生成元为 $g\in G$,随机整数 $a,b,c\in \mathbf{Z}_p$,并将四元组 $g,g^a,g^b,g^c\in G$ 和随机数 $T\in G_T$ 发送给敌手 A,由敌手 A 判定 T 是否等于 $e(g,g)^{abc}$。当 $T=e(g,g)^{abc}$ 时,A 输出 1;否则输出 0。

定义敌手判断出上述问题的优势是:

$$Adv_{\mathrm{DBDH}}=\Pr[A(g,g^a,g^b,g^c,e(g,g)^{abc})=1]-\Pr[A(g,g^a,g^b,g^c,T)=1]$$

式中:Pr 表示概率或者优势。

如果没有时间多项式算法通过不能忽略 Adv_{DBDH} 打破 DBDH 假设,则该假设成立。

1.3 具有层次结构的访问树

假设用 T 表示具有分层结构的访问树,在 T 中,具有 k 个访问层次,树中的节点用 (x,y) 表示,其中:x 表示节点在树中的行位置(从上而下);y 表示节点在树中的列位置(从左到右)。$R(x,y)$ 表示根节点,$att(x,y)$ 表示叶子节点。

图 1 为具有 2 个层次结构的访问树,树中圆圈表示阈值门限,如“OR”“AND”“n-of-m($n<m$)”,方框表示属性,树中从上而下,从左至右各节点的坐标分别为(1,1)、(2,1)、(2,2)、(3,1)、(3,2)。

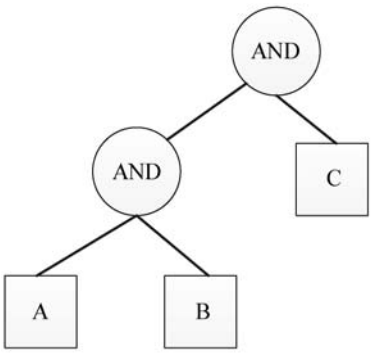

图 1 具有 2 个层次结构的访问树

针对访问树,有如下定义:

(x_i,y_i):表示访问树中的级节点,最高节点为根节点 $R(x_1,y_1)$,其余的依次递减。$parent_{(x,y)}$:表示节点 (x,y) 的父节点。$child_{(x,y)}$:表示节点 (x,y) 的子节点。$att_{(x,y)}$:表示与叶子节点相关联的属性。$index_{(x,y)}$:表示返回一个与节点 (x,y) 相关联的唯一值。

2 系统模型及安全模型

2.1 系统模型

在本方案中,主体包括 5 部分,分别为中央授权机构(Central Authority,CA)、属性授权机构(Attribute Authority,AA)、数据属主(Data Owner,DO)、用户(Us-

er)和云服务提供商(Cloud Service Provider,CSP)[7]。

各主体的主要功能如下:

1) CA 为可信机构,通过输入安全参数,产生主公钥和主私钥,同时为 AA 和 User 生成身份标签,当用户注册完成后,为 User 生成密钥组件。

2) AA 根据 User 属性生成部分密钥组件。

3) DO 在本地加密需要共享的文件,由于直接采用 CP-ABE 加密文件,会花费比较长的时间,因此在本文中,DO 首先通过 AES 或 SM4 算法生成文件密文,再采用 CP-ABE 算法加密文件密钥,最终把完整的密文上传至云端。

4) User 用户从云服务端下载完密文数据,当用户属性满足数据属主定义的属性时获得属性加密的密钥,再解密文件数据。

5) CSP 是"诚实但好奇"的文件存储机构,能够为用户提供足够的文件存储空间,然而,为了获取利益,还是会尽可能多地收集所存储的数据信息。

2.2　安全模型

在本方案中,由敌手 Adversary 和挑战者 Challenger 二者通过交互式的游戏,构建敌手挑战模型[20],具体描述如下:

1) 初始化操作(Initialization)。Adversary 将选择的访问结构 W 发送给 Challenger。

2) 系统建立(Setup)。Challenger 在游戏过程中通过方案中的初始化算法得到系统公钥和密钥主私钥,主私钥由 Challenger 保存,将公钥发送给 Adversary。

3) 查询阶段 1(QueryPhase1)。Adversary 选择属性 $S_i, S_i \notin W$,并重复从 Challenger 处获得私钥 SK,同时 Challenger 通过运行 KeyGen 生成私钥 SK。

4) 挑战阶段(Challenge)。Adversary 选择两条等长的消息 M_0 和 M_1,Challenger 通过访问结构 W 加密消息 M_η,其中 $\eta \in \{0,1\}$,再将密文 CT 发送给 Adversary。

5) 查询阶段 2(QueryPhase2)。重复查询阶段 1。

6) 猜测阶段(Guess)。Adversary 猜测 $\eta' \in \{0,1\}$。如果 $\eta = \eta'$,Adversary 在游戏中获得成功,Adversary 成功概率为:$Adv_A = |\Pr[\eta = \eta'] - \frac{1}{2}|$。

3　方案构造

3.1　初始化算法

(1) CA 初始化。CA 输入安全参数 1^λ,生成群 G,由第 1 节可知,g 为其生成元,CA 随机选择 $\alpha, \beta \in \mathbf{Z}_p$,计算 $Y = e(g,g)^\alpha$ 和 $h = g^\beta$,并根据相应的签名方案,生成签名密钥 $Signkey$ 和验证密钥 $Verifykey$。

公钥 $GPK = (p, g, G, G_T, e, Y, h, Verifykey)$　(1)

主私钥 $GSK = (\beta, g^\alpha)$　(2)

(2) 用户注册。User 首先向 CA 发出申请,完成注册。然后 CA 为每个 User 生成全局标识符 GID。在本方案中,用户不能是长期合法的,必须要有一定的期限限制,因此 CA 必须为 User 设定有效期限 T_{pov}。最后,为了能够辨别 User 身份的真伪,生成标签 $Usign$。$Usign = (GID \| L \| T_{pov}, Signkey)$,其中 L 为 User 属性集。

(3) AA 初始化。CA 为每个 AA 设定一个类似于用户 GID 的标识符 AID,为了保证每个 AA 都是合法的机构,CA 为 AA 生成签名 $Asign$。$Asign = (AID \| U_{AID}, Signkey)$,其中 U_{AID} 为 AA 负责管理的属性集。

为属性集中的每个属性元素随机选择 $a_{ij} \in \mathbf{Z}_p$,计算 $A_{ij} = g^{a_{ij}}$。其中公钥 $APK = \{Asign, \{A_{ij}\}\}$,私钥 $ASK = a_{ij}$。

3.2　加密算法

数据拥有者采用 k 个密钥 $\{k_1, k_2, \cdots, k_k\}$ 利用对称加密算法加密文件 $M = \{m_1, m_2, \cdots, m_k\}$,文件密文为 $E(M) = \{E_{k_1}(m_1), E_{k_2}(m_2), \cdots, E_{k_k}(m_k)\}$,再用 CP-ABE 加密文件密钥。文件密钥加密过程如下:

数据拥有者首先确定好分层级访问树 T,输入公钥 GPK、APK、k 个文件密钥,输出密文 CT。

在访问树中,设置级节点 $(x_i, y_i)(i = 1,2,\cdots,k)$,每个级节点都对应一个级别的密文,根据上文所提,根节点级别最高,从上至下,依次递减。每个级节点被分配一个随机数,共有 k 个,依次为 $s_1, s_2, \cdots, s_k \in \mathbf{Z}_p$,对所有的 $i = 1,2,\cdots,k$ 计算 C_i, C'_i。

$$C_i = k_i Y^{s_i} = k_i e(g,g)^{\partial s_i} \quad (3)$$

$$C'_i = h^{s_i} = g^{\beta s_i} \quad (4)$$

在分级访问树中,每个 (x,y) 都对应一个多项式 $q_{(x,y)}$,从 $R(x,y)$ 开始,每个 (x,y) 的 $q_{(x,y)}$ 阶为:$d_{(x,y)} = k_{(x,y)} - 1$。对于分级节点,$q_{(x,y)}(0) = q_{(x_1,y_1)}(0) = s_i$,多项式 $q_{(x,y)}$ 的其他系数随机选择。比如根节点 R,$q_R(0) = q_{(x_1,y_1)}(0) = s_1$。对于非分级节点,$q_{(x,y)}(0) = q_{parent(x,y)}(index(x,y))$。

集合 Y 为树中叶子节点的集合,对于任意的 $(x,y) \in Y$,有:

$$C_{(x,y)} = A_{ij}^{q_{(x,y)}(0)} = g^{a_{ij} \cdot q_{(x,y)}(0)} \quad (5)$$

$$C'_{(x,y)} = g^{q_{(x,y)}(0)} \tag{6}$$

对于其他节点,则有:

$$C_{(x,y)_i} = e(g,g)^{\partial(q_{(x,y)}(0)+q_{childj}(0))} \tag{7}$$

因此密文 $CT = \{C_i, C'_i, C_{(x,y)}, C'_{(x,y)}, C_{(x,y)_i}\}$。

3.3 密钥生成

用户注册完成以后,CA 为 User 随机选择 $r \in \mathbf{Z}_p$ 并提供部分私钥组件 $D = g^{\frac{\partial+\gamma}{\beta}}$。

用户向 AA 发出私钥请求后,AA 首先验证用户信息检查其是否在有效期范围内,如果身份有效,则根据用户属性生成私钥组件。

为每个属性值随机选择 $\lambda_i \in \mathbf{Z}_p$,则:

$D_i = g^r A_{ij}^{\lambda_i} = g^r g^{a_{ij}\lambda_i} \quad D'_i = g^{\lambda_i}$

用户私钥为 $SK_L = \{D, D_i, D'_i\}$。

3.4 解密运算

用户从云端下载完密文后,需要得到共享文件的密钥 K 才能解密文件,首先是采用 CP-ABE 算法解密得到对称密钥,再通过对称算法解密共享文件。

类似于 CP-ABE[21],解密运算如下:

① 若节点 (x,y) 为叶子节点时,令 $i = att(x,y)$,如果 $i \notin S$,$DecryptNode(CT,SK,(x,y)) = \text{null}$。

如果 $i \in S$,则有:

$$DecryptNode(CT,SK,(x,y)) = \frac{e(D_i,C_{(x,y)})}{e(D'_i,C'_{(x,y)})} = \frac{e(g^r g^{a_{ij}\lambda_i}, g^{q_{(x,y)}(0)})}{e(g^{\lambda_i}, g^{a_{ij}q_{(x,y)}(0)})} = e(g,g)^{rq_{(x,y)}(0)} \tag{8}$$

② 若 (x,y) 为非叶子节点时,设 Z 为节点 x 的子节点,令 $F_z = DecryptNode(CT,SK,Z)$,$S_{(x,y)}$ 为节点 x 的子节点集。

$$S'_{(x,y)} = \{index(Z) : Z \in S_{(x,y)}\} \quad i = index(Z)$$

$$F(x,y) = \prod_{Z \in S_{(x,y)}} F_z^{\Delta i, S'_{(x,y)}(0)} = \prod_{Z \in S_{(x,y)}} (e(g,g)^{r \cdot q_z(0)})^{\Delta i, S'_{(x,y)}(0)} = \prod_{Z \in S_{(x,y)}} (e(g,g)^{r \cdot q_{(x,y)}(i)})^{\Delta i, S'_{(x,y)}(0)} = e(g,g)^{rq_{(x,y)}(0)} \tag{9}$$

式中:$\Delta i, S'_{(x,y)}(0)$ 为拉格朗日系数。

③ 如果 S 满足整个或者部分访问树,则:

$$DecryptNode(CT,SK,(x_i,y_i)) = e(g,g)^{rq_{(x_i,y_i)}(0)} = e(g,g)^{rs_i} \tag{10}$$

④ 最后得到相关的密钥:

$$\frac{e(C'_i,D)}{e(g,g)^{rs_i}} = \frac{e(g^{\beta S_i}, g^{\frac{\partial+\gamma}{\beta}})}{e(g,g)^{rs_i}} = e(g,g)^{\partial S_i} \tag{11}$$

$$\frac{C_i}{e(g,g)^{\partial s_i}} = \frac{k_i e(g,g)^{\partial s_i}}{e(g,g)^{\partial s_i}} = k_i \tag{12}$$

⑤ 利用 k_i 解密 $E_{k_i}(m_i)$ 得到文件 m_i。若用户满足部分访问树,则可得到文件 M 中部分;若满足整个访问树,则可得到文件 M 的所有内容。

4 安全性分析

4.1 密钥的安全性

系统密钥由 CA 和 AA 共同生成,在以往的 CP-ABE 方案中,系统密钥只由 CA 生成,一旦 CA 被攻击,就会造成密钥泄露。在本方案中,如果 CA 被攻破,只会使得私钥的部分组件 D 被泄露,完整的私钥不会被泄露。如果部分 AA 机构被攻破,只会获得 k 个 D_i,解密几率还是非常小的,因此本方案中系统的密钥是安全的。

4.2 抵抗合谋攻击

密文信息为 $C_i = k_i Y^{s_i} = k_i e(g,g)^{\partial s_i}$,若要解密密文得到明文 k_i,必须恢复出 $e(g,g)^{\alpha s_i}$。对于一个不具备属性 y 的攻击者 u_1,即使与具备该属性的用户 u_2 共谋,也不能得到密钥组件 D;因为 CA 为每个用户产生的随机数 r 是不一致的。如果出现授权中心合谋攻击的情况时,只要 CA 中心的私钥组件 D 没有被泄露,方案仍旧是安全的。

4.3 安全性证明

根据第 2 节中设计的安全模型,对本文所提出的方案进行安全性证明。

定理 1 如果在任意的时间多项式算法中,Adversary 不可能以不可忽略的优势 ξ 赢得挑战,则称本方案是选择明文攻击安全的。

证:构造模拟器 B,B 在随机元组中能以 $\frac{\xi}{2}$ 的优势区别出 DBDH 元组。

选取双线性映射 $e: G \times G \to G_T$,随机选择 a、b、c,其中 $a,b,c \in \mathbf{Z}_p$。$\eta \in \{0,1\}$,$R \in G_T$。若 $R = e(g,g)^{abc}$ 时,$\eta = 1$,否则 $\eta = 0$。

1) 初始化操作(Initialization)。Adversary 将选择的访问结构 W 发送给 Challenger。

2) 系统建立(Setup)。Challenger 通过初始化算法 setup,为 Adversary 提供公钥 PK,Challenger 随机选择 $a' \in \mathbf{Z}_p$,$a = a' + ab$,则 $Y = e(g,g)^a$,$h = g^\beta = B = g^b$。为每个属性值随机选择 $a_{ij} \in \mathbf{Z}_p$,$A_{ij} = g^{a_{ij}}$,将 PK 发送给 Adversary。

3) 查询阶段 1(QueryPhase1)。Adversary 选择属

性 $S_i(S_i \notin W)$,并重复从 Challenger 处获得私钥 SK。Challenger 随机选择 $r' \in \mathbf{Z}_p, r = r' - a, D = g^{\frac{\partial+\gamma}{\beta}}$。为每个属性值属性 S_i 随机选择 $\lambda_i \in \mathbf{Z}_p, D_i = g^r A_{ij}^{\lambda_i} = g^r g^{a_{ij}\lambda_i}, D'_i = g^{\lambda_i}$。

4) 挑战阶段(Challenge)。Adversary 选择两条等长的消息 M_0 和 M_1,Challenger 通过访问结构 W 加密消息 M_η,其中 $\eta \in \{0,1\}$,再将密文 CT 发送给 Adversary。

$$C = M_\eta Y^s = M_\eta e(g,g)^{as}$$

$$C' = h^s = g^{\beta s}$$

5) 查询阶段 2(QueryPhase2)。重复查询阶段 1。

6) 猜测阶段(Guess)。Adversary 输出对于 η 的猜测 $\eta'(\eta' \in \{0,1\})$。

如果 $\eta = \eta'$,Challenger 输出 1,则 $R = e(g,g)^{abc}$,否则输出 1。

若 $\eta = \eta'$,则 Adversary 的优势为 $\Pr[\eta = \eta'] = \frac{1}{2} + \xi$。

若 $\eta \neq \eta'$,则 Adversary 的优势为 $\Pr[\eta \neq \eta'] = \frac{1}{2}$。

最后赢得挑战游戏的优势为:

$$Adv = \frac{1}{2}\Pr[\eta = \eta'] + \frac{1}{2}\Pr[\eta \neq \eta'] - \frac{1}{2} = \frac{1}{2}\left(\frac{1}{2} + \xi\right) + \frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} = \frac{\xi}{2}$$

5　性能分析

本文方案针对具有层次结构的文件提出多机构授权且隐藏树形访问结构的 CP-ABE 方案,本节从密文长度、用户密钥长度和加解密时间几个方面展开,同时与文献[7]的方案进行对比分析。

为了便于说明,定义以下符号:k 表示文件分级个数;L_* 表示 $*$ 的长度;$|*|$ 表示 $*$ 的元素个数;A_T 表示除叶子以外的子节点集;i 为 A_T 中节点的子节点;A_u 为用户的属性集;A_S 为系统属性集;S 表示具有层次结构访问树中的最小内部节点;t_b 表示双线性对运算;t_e 表示群中的指数运算和乘法运算时间。

密文长度为 $(2|A_S| + k)L_G + (i|A_T| + k)L_{G_T}$。

用户密钥长度为 $(2|A_u| + 1)L_G$。

加密时间为 $(2|A_S| + k)t_e + (i|A_T| + 2k)t_e$。

解密时间为 $(2|A_u| + 1)t_b + (2|S| + j|A_T| + 2k)t_e$。

在文献[13]中,密文长度为 $(2|A_S| + 1)L_G + L_{G_T}$,用户私钥长度为 $(2|A_u| + 1)L_G$,加密时间为 $(2|A_S| + 2)t_e$,解密时间为 $(2|A_u| + 1)t_b$。

若解密一个文件时,文献[13]中密文略短于本文生成的密文,用户私钥一样长,加密时间和解密时间也略低于本文方案。而本文方案可以同时加密 K 个文件,此时,本文方案明显优于文献[13]。且本文方案能够实现文件的分级访问控制。

6　结　语

本文利用多层次的树形访问结构加密文件,实现了文件的分级访问控制,同时,策略的隐藏防止了敏感信息的泄露,研究成果在 DBDH 假设下被证明是安全的。通过与其他方案的对比,本文方案在加密多个文件时具有明显的优势,同时多授权机构的使用不仅可以保护用户密钥的安全,也可实现用户的跨域访问。下一步,将重点研究如何减少解密运算量。

参　考　文　献

[1] 洪澄,张敏,冯登国. 面向云存储的高效动态密文访问控制方法[J]. 通信学报,2011,32(7):125 - 132.

[2] 杨腾飞,申培松,田雪,等. 对象云存储中分类分级数据的访问控制方法[J]. 软件学报,2017,28(9):2334 - 2353.

[3] Sahai A, Waters B. Fuzzy identity-based encryption[C]// 24th Annual International Conference on Theory and Applications of Cryptographic Techniques,2005.

[4] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//13th ACM Conference on Computer and Communications Security, 2006:89 - 98.

[5] 胡思路,陈燕俐. 一种基于属性的固定密文长度广播加密方案[J]. 计算机应用研究,2016,33(6):1780 - 1784.

[6] Nishide T, Yoneyama K, Ohta K. Attribute-based encryption with partially hidden encryptor-specified access structures [C]//International Conference on Applied Cryptography and Network Security,2008:111 - 129.

[7] 李新,彭长根,牛翠翠. 隐藏树型访问结构的属性加密方案[J]. 密码学报,2016,3(5):471 - 479.

[8] 陈丹伟,汤波. 基于 LSSS 的隐藏策略属性基加密方案[J]. 计算机技术与发展,2018,28(2):119 - 124.

[9] Chase M. Multi-authority attribute based encryption[C]//4th Conference on Theory of Cryptography,2007.

[10] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[C]// 14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography,2011.

[11] 赵志远,王建华,徐开勇. 定长密文且快速解密的分布式属性基加密方案研究[J]. 电子与信息学报,2017,39(11):2724 - 2732.

(下转第 333 页)

表 3　检测时间对比　　ms

检测特征	本文 6 元组	文献[12] 8 元组	文献[13] 4 元组
决策树	468	527	430
KNN	441	467	414
BayesNet	235	257	218

5　结　语

本文提出一种在 SDN 网络环境中的基于交叉熵的分阶段多层次 DDoS 攻击检测模型,采用基于交换机设备 CPU 使用率的初检方法,检测转发进程 CPU 的使用率,减轻计算资源使用率,又可快速定位异常交换机;引入交叉熵值的理论,将正常与攻击流量在特征分布上的相似性定量分析,有效增加数据间的信息距离,提升检测准确度;预警检测模块使用目的 IP 交叉熵值及 PACKET_IN 数据包联合检测,降低了漏报率。实验结果验证了检测特征的良好表现。

后期的工作将对特征筛选进行研究,使用优化算法选取最优特征集,同时考虑对比更多的特征,根据攻击报告进行攻击溯源研究。

参　考　文　献

[1] 张朝昆,崔勇,唐翯祎,等. 软件定义网络(SDN)研究进展[J]. 软件学报,2015,26(1):62 – 81.

[2] Dayal N, Srivastava S. Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN[C]//2017 9th International Conference on Communication Systems and Networks(COMSNETS), 2017: 274 – 281.

[3] Dayal N, Maity P, Srivastava S, et al. Research trends in security and DDoS in SDN[J]. Security and Communication Networks, 2016, 9(18): 6386 – 6411.

[4] Giotis K, Argyropoulos C, Androulidakis G, et al. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments [J]. Computer Networks, 2014, 62:122 – 136.

[5] Basicevic I, Ocovaj S, Popovic M. Use of tsallis entropy in detection of SYN flood DoS attacks[J]. Security and Communication Networks, 2015, 8(18):3634 – 3640.

[6] Mousavi S M, St-Hilaire M. Early detection of DDoS attacks against SDN controllers[C]//2015 International Conference on Computing, Networking and Communications (ICNC), 2015:77 – 81.

[7] Ma X, Chen Y. DDoS detection method based on chaos analysis of network traffic entropy[J]. IEEE Communications Letters, 2013, 18(1):114 – 117.

[8] Jun J H, Lee D, Ahn C W, et al. DDoS attack detection using flow entropy and packet sampling on huge networks [C]//The Thirteenth International Conference on Networks, 2014: 185 – 190.

[9] 武泽慧,魏强,任开磊,等. 基于 OpenFlow 交换机洗牌的 DDoS 攻击动态防御方法[J]. 电子与信息学报,2017,39(2):397 – 404.

[10] 姚琳元,董平,张宏科. 基于对象特征的软件定义网络分布式拒绝服务攻击检测方法[J]. 电子与信息学报,2017,39(2):381 – 388.

[11] Yan Q, Gong Q, Deng F A. Detection of DDoS attacks against wireless SDN controllers based on the fuzzy synthetic evaluation decision-making model [J]. Ad Hoc & Sensor Wireless Networks, 2016, 33(1): 275 – 299.

[12] 刘振鹏,贺玉鹏,王文胜,等. SDN 环境下的 DDoS 攻击检测方案[J]. 武汉大学学报(理学版),2019,65(2):178 – 184.

[13] 田俊峰,齐鎏岭. SDN 中基于条件熵和 GHSOM 的 DDoS 攻击检测方法[J]. 通信学报,2018,39(8):140 – 149.

(上接第 327 页)

[12] 李非非,韩笑,曾琦. 具有隐私保护的固定密文长度分布式属性基加密方案[J]. 计算机应用与软件,2018,35(5):323 – 327.

[13] 范运东,吴晓平. 基于策略隐藏属性加密的云存储访问控制方案[J]. 计算机工程,2018,44(7):139 – 144,149.

[14] Li J, Wang Q, Wang C, et al. Enhancing attribute-based encryption with attribute hierarch[J]. Mobile Networks and Applications, 2011, 16(5):553 – 561.

[15] Wang G J, Liu Q, Wu J, et al. Hierachical attribute-based encryption and scalable user revocation for sharing data in cloud servers[J]. Computers & Security, 2011, 30(5):320 – 331.

[16] Hur J. Improving security and efficiency in attribute-based data sharing[J]. IEEE Transactions on Knowledge and Data Engineering, 2013, 25(10):2271 – 2282.

[17] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts[C]//20th USENIX Conference on Security, 2011.

[18] Lai J, Deng R H, Guan C, et al. Attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(8): 1343 – 1354.

[19] Wang S L, Yu J P, Zhang P, et al. A novel file hierarchy access control scheme using attribute-based encryption[J]. Applied Mechanics and Materials, 2014, 701 – 702:911 – 918.

[20] 雷丽楠,李勇. 基于密文策略属性基加密的多授权中心访问控制方案[J]. 计算机应用研究,2018,35(1):248 – 252,276.

[21] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//2007 IEEE Symposium on Security and Privacy (SP'07), 2007:321 – 334.