doi:10.3772/j.issn.1002-0470.2020.11.004

基于改进 HABE 算法的层次化多中心 SDN 跨域传输系统研究①

周 波②* 王树磊**

(*南京信息职业技术学院电子信息学院 南京 210023)

(**常州工学院民航飞行学院 常州 213032)

摘 要 层次化多中心软件定义网络(HMC-SDN)是一种能够提高大规模网络服务质量和扩展性的有效架构。然而现有的 HMC-SDN 架构中的跨域通信缺少足够的安全保护,使其中的敏感数据十分容易泄露且不易察觉。本文提出一种基于可认证层次化的密文策略属性加密算法(VH-CP-ABE)。依托 HMC-SDN 的层次化控制器构建层次化的属性权。交换机利用授权私钥辅以访问策略来加密跨域传输的数据包,在保证密文长度常量化的同时实现跨域安全传输。此外,交换机持有的授权私钥嵌入了交换机本身和相关控制器的身份标识,可以在解密的过程中验证授权私钥的合法性,进一步提升了跨域传输的安全性。经证明,本方案能够在随机预言机模型下达到 IND-CCA2 安全等级。性能分析及仿真表明,该方案为 HMC-SDN 跨域通信提供了良好的安全性和高效性。

关键词 软件定义网络(SDN);跨域传输;属性加密(ABE);访问控制;密钥认证

0 引 言

软件定义网络(software defined network, SDN)[1]是一种集中化管理的新型网络架构。它继承了 ForCES 架构[2]的特性,在逻辑上将网络控制层与数据层分离,因此提供了灵活扩展部署的能力。经典的 SDN 架构依赖拥有全局视图的单一控制器,但在大规模网络环境中单一控制器难以快速处理大量的流请求[3]。层次化多中心软件定义网络(hierarchical multi-center SDN, HMC-SDN)[4,5]提供了一种提高网络服务质量和扩展的可靠方案,该方案将控制器分为若干个层次,第 1 层仅包含 1 个根控制器,其余层次由多个控制器组成,其中只有根控制器具有全局视图,而其余控制器只负责一定区域内的转发工作。确保 SDN 流量不被非法窃取[4]是保证 SDN 网络安全运行的关键问题之一。HMC-SDN 架构庞大,其中难免出现在若干个区域之间进行跨域传输的情形,然而现有的 HMC-SDN 架构难以保证跨域传输的安全性。一旦在控制层进行非法的规则插入或规则修改操作,就有可能将数据包转发给恶意用户,那么就很有可能导致其中的敏感信息泄露。因此,必须在跨域传输过程保证只有合法授权的设备才能获取数据包当中的信息,同时进行灵活的、细粒度控制方便 HMC-SDN 网络的部署和扩展。

针对 SDN 单一控制器架构在处理大量流请求时容易导致网络响应变慢、服务质量下降的问题,许多研究提出了多控制中心 SDN 架构,采用的策略不尽相同。文献[4]提出了一种 2 层控制器的 SDN 架构 Kandoo,将控制器划分为 2 层,第 1 层由根控制器组成,第 2 层由多个区域控制器组成,其中根控制器决定网络全局的转发规则。文献[5]提出了一种结合区域划分和域内控制器划分相结合的方法代替直接部署控制器的方法,提高了 HMC-SDN 的流表

① 国家自然科学基金(61571241),江苏高校品牌专业建设工程(PPZY2015C242)和江苏省高等学校自然科学研究(18KJB510024)资助项目。

② 男,1978 年生,硕士,讲师;研究方向:信息安全,无线传感网;联系人,E-mail: bozhou_njcit@126.com

(收稿日期:2019-10-12)

构建效率。文献[6]提出了一种面向 SDN 的访问控制系统,首先对 SDN 的各个组件进行逻辑层面的隔离,在用户试图对组件进行访问和控制时必须对用户进行身份认证。文献[7]对 SDN 网络组件的可执行指令集做出了不同程度的限制,以实现大型网络环境下的安全、快速访问控制。文献[8]介绍了一种面向 SDN 网络身份认证和访问控制方法,它将所有未授权的设备隔离起来以保证网络资源的安全性。目前为止,基于传统访问控制理论的 SDN 访问控制研究已有诸多成果,但是 SDN 网络在灵活性和扩展性方面的需求迫使其跨域通信方法必须具备相当的灵活性、安全性以及高效性。

属性加密[9](attribute-based encryption,ABE)能够从密码学原理上满足以上需求。ABE 算法在私钥或者密文当中分别嵌入了一套访问策略以及可描述身份的属性集合。只要属性集合能够满足访问策略的描述,那么就可以正确地得到消息明文,反之则绝对无法获取任何有用的信息。这样一来就能够在众多加密者与解密者之间实现安全的数据共享。目前有 2 种主要的 ABE 算法,一种是基于密钥策略的 ABE 算法[10](key policy attribute-based encryption,KP-ABE),别外一种是基于密文策略的 ABE 算法[11](ciphertext policy attribute-based encryption,CP-ABE)。CP-ABE 算法允许加密者自由制定访问策略,而密钥当中嵌入的属性集合又能够表征解密者的身份,因而 CP-ABE 更适合构建一种安全又灵活的通信方法。文献[12]提出了一种基于多权威 ABE(multi-authority attribute-based encryption,MABE)算法,每个属性权威拥有各自的主密钥,这不仅分散了属性权威的绝对解密能力,也分散每个属性权威的计算负担。文献[13]提出了一种基于安全双方计算的密钥生成机制,在最小化 ABE 算法模型的同时尽可能避免属性权威拥有过于强大的解密能力。文献[14]构造了基于 CP-ABE 的属性直接撤销方法,优化了 CP-ABE 密文、私钥和公钥的长度。文献[15]提出了一种分布式的 CP-ABE 密钥管理协议,结合外包解密技术使得终端用户只需进行简单的计算就可获取消息明文而不会降低密文的安全性,然而该方案所产生的密文尺寸非常大,而且整体计算负载也非常大。文献[16]提出了一种基于层次化 ABE(hierarchical attribute-based encryption,HABE)的 SDN 访问控制方案,将多个属性权威放置在一种层次化的结构当中,弱化了属性权威的权力同时降低了每一个属性权威的计算负载,因此 SDN 控制器能够有效地管理 SDN 的用户、设备和流表数据。文献[17]提出基于代理群的 ABE 算法,把复杂计算全部交给可信的代理节点群去处理,从而降低了 ABE 算法的计算门槛,但是系统整体的安全性在某种程度上更依赖于代理节点的可信等级。文献[18]缩短了 HABE 的密文长度,使密文长度常量化。该方案在大规模网络通信环境下可以有效降低传输开销,但由于缺乏一种层次化授权的认证机制,某些机构即使没有授权可以向下发布私钥,其仍然可以私自授权其他机构或者用户,向它们发布私钥。因此权力的滥用就会导致密文安全性的衰减。

本文对 HABE 算法进行了改进,提出一种可认证层次化密文策略属性加密算法(verifiable and hierarchical CP-ABE,VH-CP-ABE)。基于该算法构建了 HMC-SDN 的跨域安全通信系统,可有效防止跨域传输过程中泄露敏感信息。该算法利用层次化的 SDN 控制器构建层次化的属性权威,分散了控制管理的负担,还提高了系统的可扩展性。在此基础上,本方案使得消息密文的尺寸常量化,确保传输开销处于较低的水平。在对 SDN 交换机授权时嵌入了与交换机本身和所有相关控制器的身份标识,于是在解密过程中实现了私钥的合法性认证。因此,在保证系统整体可扩展性的同时,保证了其他非认证机构不可以充当控制器肆意授权其他交换机。理论分析证明,VH-CP-ABE 能够在随机预言机模型下达到 IND-CCA2 安全等级。性能分析以及仿真表明,该系统能够为 HMC-SDN 提供良好的跨域传输安全性和高效性。

1　基础知识

本节给出构建本方案的基础知识,包括访问策略、双线性映射以及困难假设。

1.1　双线性映射

定义 1　双线性映射。设$\mathbb{G}_1$和$\mathbb{G}_2$是 2 个阶为

大素数 p 的循环群，g 是$\mathbb{G}_1$的一个生成元，映射 $e:\mathbb{G}_1\times\mathbb{G}_1\rightarrow\mathbb{G}_2$ 是关于 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 的双线性映射，当且仅当 e 满足以下性质：

(1)双线性：对于任意的 $u,v\in\mathbb{G}_1$ 以及 $a,b\in Z_p$，都有 $e(u^a,v^b)=e(u,v)^{ab}$。

(2)非退化性：存在生成元 g，使得 $e(g,g)\neq 1$，其中 1 是$\mathbb{G}_2$的单位元。

(3)可计算性：对于任意的 $u,v\in\mathbb{G}_1$，存在多项式时间算法能够有效计算出 $e(u,v)$ 的值。

1.2 困难假设

定义 2 判定 q-并行双线性 Diffie-Hellman 假设(decisional q-parallel bilinear Diffie-Hellman exponent assumption，q-DBDH)。假设$\mathbb{G}_1$是素数阶的乘法循环群，$e:\mathbb{G}_1\times\mathbb{G}_1\rightarrow\mathbb{G}_2$是一个双线性映射，$\alpha\in Z_p^*$是一个秘密数。若已知$\mathbb{G}_1$中的 $2q+1$ 个参数 $\{g,h,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q},g^{\alpha^{q+2}},\cdots,g^{\alpha^{2q}}\}$，给定$\mathbb{G}_2$中的一个参数 Z，那么敌手难以判断 Z 是否等于 $e(g,h)^{\alpha^{q+1}}$。

2 系统模型与 VH-CP-ABE 算法框架

本节首先给出 HMC-SDN 跨域传输系统模型的各个组件，其次介绍本文提出的 VH-CP-ABE 算法的构成框架，结合以上 2 部分给出基于 VH-CP-ABE 算法的 HMC-SDN 跨域通信系统的工作流程，如图 1 所示。

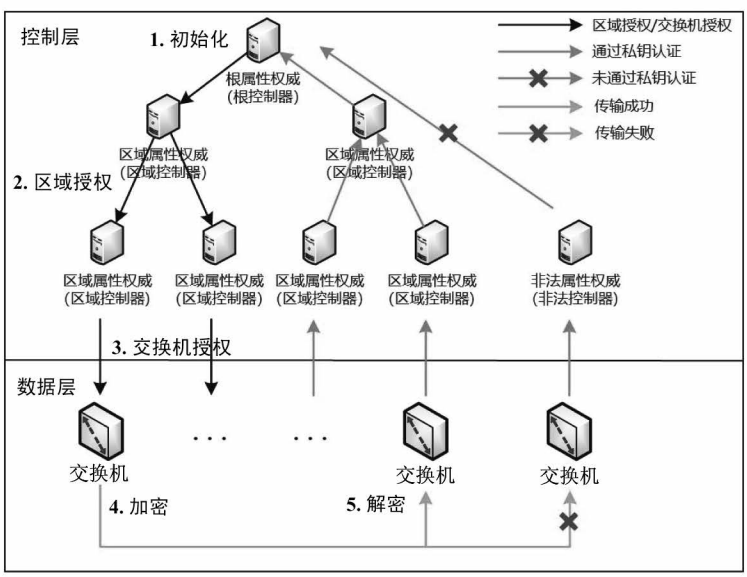

图 1 基于 VH-CP-ABE 算法的 HMC-SDN 跨域通信系统的工作流程

2.1 系统模型

基于 VH-CP-ABE 算法的 HMC-SDN 跨域通信系统模型主要由以下组件构成。

根属性权威 由 HMC-SDN 中的根控制器担任该角色，作为可信机构负责全局属性的注册以及公钥的发布，是所有区域属性权威的起点。

区域属性权威 由 HMC-SDN 中各个等级的区域 SDN 控制器担任该角色，负责与某一类属性有关的私钥授权工作，这类属性是全局属性集合的某个真子集。区域属性权威既可以对下一等级的控制器授权，也可以对交换机授权。此外，区域属性权威是半可信的，尽管可以发布或认证私钥的合法性，但也可能泄露私钥。

加密组件 位于 SDN 数据层的组件。在执行跨域传输时，交换机利用该组件加密数据包并辅以一定的访问策略，将其转发到相应的域。

解密组件 位于 SDN 数据层的组件。在执行跨域传输通信时，目标交换机通过该组件使用自己的授权私钥解密数据包。当且仅当授权私钥通过合法性认证，且授权私钥中的属性集合满足数据包密文中的访问策略，才可以成功获取数据。

2.2　VH-CP-ABE 算法框架

VH-CP-ABE 算法框架由初始化、区域授权、用户授权、加密以及解密共 5 个子算法构成,算法的框架描述如下。

初始化　该算法由根属性权威执行,输入一个安全参数 λ 以及全局的真实属性集合 Ω,输出公钥 PK 以及根密钥 RSK, 其中公钥 PK 向全网公开,而根密钥由根属性权威保存。

区域授权　该算法由等级为 $i-1$ 的属性权威执行,被授权的控制器将成为等级为 i 的区域属性权威,其中 $i \geqslant 1$。当 $i=1$ 时,算法由根属性权威执行,输入真实的区域属性集合 $\Omega_{1,real}$ 以及根密钥 RSK, 输出区域授权私钥 SK_1; 当 $i>1$ 时,算法由等级为 $i-1$ 的区域属性权威执行,输入真实的区域属性集合 $\Omega_{i+1,real}$ 以及区域授权私钥 SK_{i-1}, 最终输出新的区域授权私钥 SK_i。

交换机授权　该算法由等级为 i 的区域属性权威执行,输入真实的交换机属性集合 S_{real} 以及区域授权私钥 SK_i, 最终输出交换机授权私钥 SK_u。对于任意一个合法的交换机授权私钥 SK_u, 总能在 HNC-SDN 网络中找到唯一一条授权链。授权链的一端是根控制器,另一端是交换机,中间则是若干个区域控制器。

加密　该算法由交换机的加密组件执行,输入访问策略 $\gamma_{t,\mathbb{S}}$、数据包 M 以及公钥 PK, 最终输出数据包密文 CT。

解密　该算法由交换机的解密组件执行,输入消息密文 CT 以及用户私钥 SK_u, 如果私钥 SK_u 当中嵌入的属性集合 S_{real} 满足密文 CT 当中嵌入的访问策略 $\gamma_{t,\mathbb{S}}$, 那么最终输出正确的消息明文 M。

基于 VH-CP-ABE 算法的 HMC-SDN 跨域通信系统实现了 HMC-SDN 安全、高效的跨域通信。系统的具体工作流程如图 1 所示,根属性权威执行初始化算法输出公钥 PK; 各个区域的控制器按照等级向上一级申请授权,成为区域属性权威;区域内的交换机向该区域的属性权威申请授权,区域属性权威交换机发布对应的私钥 SK_u; 针对某一数据包 M 的跨域传输任务,交换机制定相应的访问策略 $\gamma_{t,\mathbb{S}}$ 并通过加密组件执行加密算法输出数据包密文;区域内的交换机收到数据包密文时,通过解密组件执行解密算法,在解密算法首先通过授权链验证当前交换机的授权私钥的合法性,验证通过后进行解密操作,否则无法解密数据包密文,也就无法成功传输。

3　VH-CP-ABE 算法

本节将给出 VH-CP-ABE 算法各个步骤的详细流程。

3.1　初始化

该算法由根属性权威执行,首先假设真实的全局属性集合为 $\Omega=\{att_1, att_2, \cdots, att_N\}$, 其中任意属性 att_j 均为 HMC-SDN 网络中各区域各交换机具备的某个真实网络特征。输入安全参数 λ 以及全局真实属性集合 Ω,输出公钥 PK 以及根密钥 RSK, 其中公钥 PK 向全网公开,而根密钥由根属性权威保存。初始化算法流程如下所示。

(1) 输入真实的全局属性集合 Ω,随机生成一个傀儡全局属性集合 $\Omega'=\{att_{N+1}, \cdots, att_{2N-1}\}$。

(2) 定义函数 index,对于任意属性 $att_j \in \Omega \cup \Omega'$,index($att_j$)返回索引 j。

(3) 选择 1 个哈希函数 $H:\{0,1\}^* \rightarrow Z_p^*$。

(4) 产生 1 组随机数 g_2, h_0, $h_2, \cdots, h_{2N-1}, \delta_1, \delta_2, \delta_3 \in \mathbb{G}_1$, $x \in Z_p^*$, 并计算 $g_1=g^x$ 以及 $Z=e(g_1, g_2)$。

(5) 定义根密钥 $RSK=x$, 保留根密钥并输出公钥 $PK=\{g, g_1, g_2, Z, h_0, \cdots, h_{2N-1}, \delta_1, \delta_2, \delta_3, H\}$。

3.2　区域授权

该算法由等级为 $i-1$ 的属性权威执行,被授权的控制器将成为等级为 i 的区域属性权威,其中 $i \geqslant 1$。

当 $i=1$ 时,算法由根属性权威执行,输入真实的区域属性集合 $\Omega_{1,real}$ 以及根密钥 RSK, 输出区域授权私钥 SK_1。具体流程如下。

(1) 根属性权威生成 1 个次数为 $N-1$ 的随机多项式 q, 使得 $q(0)=x$。

(2) 假设区域属性权威的身份标识为 $id_1 \in$

$\{0,1\}^*$，区域属性权威产生 1 个随机数 $s_1 \in \{0,1\}^*$ 作为主密钥，计算 $H(id_1 \| s_1)$ 并发送给根属性权威。

（3）根属性权威根据区域属性权威的真实区域属性集合 $\Omega_{1,real}$ 生成 1 个属性集合 $\Omega_1 = \Omega_{1,real} \cup \Omega'$。对于任意 $att_j \in \Omega_1$，根属性权威选择 1 个随机数 $r_{1,j} \in Z_p^*$ 并计算 $a_{1,j} = (g_2^{q(j)}(h_0 h_i)^{r_{1,j}})^{H(id_1 \| s_1)}$ 以及 $b_{1,j} = g^{r_{1,j} \cdot H(id_1 \| s_1)}$。

（4）对于任意 $att_j \in \Omega_1$，任意 $k \in [1,j] \cup [j+1,2N]$，计算 $c_{1,j,k} = h_k^{r_{1,j} \cdot H(id_1 \| s_1)}$。

（5）对于任意 $att_j \in \Omega_1$，生成该区域属性权威的授权私钥组件 $sk_{1,j} = \{a_{1,j}, b_{1,j}, \{c_{1,j,k}\}\}$。

（6）输出区域授权私钥 $SK_1 = \{sk_{i,j}\}_{att_j \in \Omega_1}$。

当 $i > 1$ 时，算法由等级为 $i-1$ 的区域属性权威执行，输入真实的区域属性集合 $\Omega_{i+1,real}$ 以及区域授权私钥 SK_{i-1}，最终输出新的区域授权私钥 SK_i。具体流程如下。

（1）假设区域属性权威的身份标识为 $id_i \in \{0,1\}^*$，等级为 $i-1$ 的授权私钥是 $SK_{i-1} = \{sk_{i-1}\}_{att_j \in \Omega_i}$，其中 $sk_{1,j} = \{a_{1,j}, b_{1,j}, \{c_{1,j,k}\}\}$。等级为 i 的区域属性权威选择 $s_i \in Z_p^*$ 作为主秘密，计算 $H(id_i \| s_i)$ 并发送给等级为 $i-1$ 的区域属性权威。

（2）等级为 $i-1$ 的区域属性权威根据 $\Omega_{i+1,real}$ 生成属性集合为 $\Omega_i = \Omega_{i,real} \cup \Omega'$，其中 $\Omega_{i,real} \subseteq \Omega_{i-1,real}$。对于任意 $att_j \in \Omega_i$，选择随机数 $r_{i,j} \in Z_p^*$ 并计算 $a_{i,j} = (a_{i-1,j}(h_0 h_j)^{r_{i,j}})^{H(id_i \| s_i)}$ 以及 $b_{i,j} = (b_{i-1,j} g^{r_{i,j}})^{H(id_i \| s_i)}$。

（3）对于任意 $att_j \in \Omega_i$ 和 $k \in [1,2N-1]/\{j\}$，计算 $c_{i,j,k} = (c_{i-1,j,1} h_k^{r_{i,j}})^{H(id_i \| s_i)}$。

（4）对于任意 $att_j \in \Omega_i$，生成该区域属性权威的授权私钥组件 $sk_{i,j} = \{a_{i,j}, b_{i,j}, \{c_{i,j,k}\}\}$。

（5）输出区域授权私钥 $SK_i = \{sk_{i,j}\}_{att_j \in \Omega_i}$。

3.3 交换机授权

该算法由等级为 i 的区域属性权威执行，输入真实的交换机属性集合 S_{real} 以及区域授权私钥 SK_i，最终输出交换机授权私钥 SK_u。具体流程如下。

（1）假设交换机的身份标识为 id_{i+1}，其产生 1 个随机数 $s_{i+1} \in Z_p^*$ 作为主密钥，计算 $H(id_{i+1} \| s_{i+1})$ 并发送给等级为 i 的区域属性权威。

（2）等级为 i 的区域属性权威根据 S_{real} 产生 1 个属性集合 $S = S_{real} \cup \Omega'$，其中 $S_{real} \subseteq \Omega_{i,real}$。对于任意 $att_j \in S$，选择 1 个随机数 $r_{i+1,j} \in Z_p^*$ 并计算 $a_{i+1,j} = (a_{i,j}(h_0 h_j)^{r_{i+1,j}})^{H(id_{i+1} \| s_{i+1})}$，$b_{i+1,j} = (b_{i,j} g^{r_{i+1,j}})^{H(id_{i+1} \| s_{i+1})}$。

（3）对于任意 $att_j \in S$ 和 $k \in [1,2N-1]/\{j\}$，计算 $c_{i,+1j,k} = (c_{i,j,1} h_k^{r_{i+1,j}})^{H(id_{i+1} \| s_{i+1})}$。

（4）对于任意 $att_j \in S$，生成该交换机的授权私钥组件 $sk_{i+1,j} = \{a_{i+1,j}, b_{i+1,j}, \{c_{i+1,j,k}\}\}$。

（5）输出用户私钥 $SK_u = \{sk_{i+1,j}\}_{att_j \in S}$。

3.4 加 密

该算法由交换机的加密组件执行，输入访问策略 $\gamma_{t,\mathbb{S}}$、数据包 M 以及公钥 PK，最终输出数据包密文 CT。加密算法具体执行流程如下：

（1）基于阈值门产生 1 个访问策略 $\gamma_{t,\mathbb{S}}$，其中 $\mathbb{S} \in \Omega$ 为访问策略 $\gamma_{t,\mathbb{S}}$ 所包含的属性集合，$t \in [1, |\Omega|]$ 为访问策略 $\gamma_{t,\mathbb{S}}$ 的阈值。

（2）选择 1 个傀儡属性集合 $\mathbb{W}$ 使得 $\mathbb{W} \in \Omega'$ 且 $\mathbb{W} = \{att_{N+1}, \cdots, att_{2N-t}\}$。

（3）选择 1 个随机数 $s \in Z_p^*$ 并计算 $C_0 = M \cdot Z^s$，$C_1 = g^s$，$C_2 = (h_1 \prod_{j \in \mathbb{S} \cup \mathbb{W}} h_j)^s$。

（4）选择随机数 $r \in Z_p^*$，计算 $C_3 = (\delta_1^c \delta_2^r \delta_3)^s$，其中 $c = H(\gamma_{t,\mathbb{S}} \| C_0 \| C_1 \| C_2)$。

（5）输出密文 $CT = \{r, C_0, C_1, C_2, C_3\}$。

3.5 解 密

该算法由交换机的解密组件执行，输入消息密文 CT 以及用户私钥 SK_u，如果私钥 SK_u 当中嵌入的属性集合 S_{real} 满足密文 CT 当中嵌入的访问策略 $\gamma_{t,\mathbb{S}}$，那么最终输出正确的消息明文 M。解密算法具体流程如下：

（1）获取密文后，验证以下等式是否成立。

$$e(g, C_2) = e(C_1, h_0 \prod_{j \in \mathbb{S} \cup \mathbb{W}} h_j) \tag{1}$$

$$e(g, C_3) = e(C_1, \delta_1^c \delta_2^r \delta_3) \tag{2}$$

如果上式均成立，则算法进入下一步，否则认为该数据包密文是非法密文并终止解密。

（2）按照以下公式计算得到 D_1 和 D_2：

$$D_1 = \prod_{att_j \in S_{real} \cup \mathbb{W}} \left(a_{i+1,j} \cdot \prod_{k \in \mathbb{S} \cup \mathbb{W},\ k \neq j} c_{i+1,j,k} \right)^{\Delta_{j,S'_{real} \cup \mathbb{W}'(0)}} \tag{3}$$

$$D_2 = \prod_{att_j \in S_{real} \cup \mathbb{W}} \left(b_{i+1,j} \right)^{\Delta_{j,S'_{real} \cup \mathbb{W}'(0)}} \tag{4}$$

(3) 按照以下公式计算得到 T_{i+1}:

$$T_{i+1} = \frac{e(C_1, D_1)}{e(C_2, D_2)} \tag{5}$$

(4) 在该交换机的授权链上以交换机为起始点,采用文献[19]的安全两方计算(two-party computation, 2PC)算法,让交换机和等级为 i 的区域属性权威共同计算参数 $T_i = T_{i+1}^{1/H(id_{i+1} \| s_{i+1})}$。S2PC 算法可以保证得到正确计算结果的同时防止计算双方泄露各自的主秘密。

(5) 对于授权链上其他任意的 2 个相邻控制器,按照上一步的计算方法进行迭代,直到生成参数 $T_0 = T_1^{1/H(id_1 \| s_1)}$。对于任意非法的授权链,交换机绝对无法获得正确的 T_0, 自然就无法正确解密数据包。

(6) 计算 $M = C_0 / T_0$ 获取原始数据包。

通过 VH-CP-ABE 算法的描述,给出如下定理。

定理 1　VH-CP-ABE 能够保证算法正确性。

证明　假设获取密文 $CT = \{r, C_0, C_1, C_2, C_3\}$ 和一个用户私钥 $SK_u = \{sk_{i+1,j}\}_{att_j \in S}$, 然后利用该私钥对密文进行解密操作。在交换机的属性集合满足访问策略 $\gamma_{t,\mathbb{S}}$ 时,算法可以保证总能获取正确的 D_1, 如式(6)所示。

$$\begin{aligned} &\prod_{att_j \in S_{real} \cup \mathbb{W}} \left(a_{i+1,j} \cdot \prod_{k \in \mathbb{S} \cup \mathbb{W},\ k \neq j} c_{i+1,j,k} \right)^{\Delta_{j,S'_{real} \cup \mathbb{W}'(0)}} \\ &= \prod_{att_j \in S_{real} \cup \mathbb{W}} \left(\begin{array}{l} g_2^{q(j) \prod_{l=1}^{i+1} H(id_l \| s_l)} \\ \cdot (h_0 h_j)^{\sum_{l=1}^{i+1} (r_{l,j} \sum_{m=l}^{i+1} (id_m \| s_m))} \\ \cdot \prod_{k \in \mathbb{S} \cup \mathbb{W},\ k \neq j} h_k^{\sum_{l=1}^{i+1} (r_{l,j} \sum_{m=l}^{i+1} (id_m \| s_m))} \end{array} \right)^{\Delta_{j,S'_{real} \cup \mathbb{W}'(0)}} \\ &= D_1 \end{aligned} \tag{6}$$

其次,在交换机的属性集合满足访问策略 $\gamma_{t,\mathbb{S}}$ 时,算法也可以保证总能获取正确的 D_2, 如式(7)所示。

$$\begin{aligned} &\prod_{att_j \in S_{real} \cup \mathbb{W}} \left(b_{i+1,j} \right)^{\Delta_{j,S'_{real} \cup \mathbb{W}'(0)}} \\ &= \prod_{att_j \in S_{real} \cup \mathbb{W}} \left(g^{\sum_{l=1}^{i+1} (r_{l,j} \sum_{m=l}^{i+1} (id_m \| s_m))} \right)^{\Delta_{j,S'_{real} \cup \mathbb{W}'(0)}} = D_2 \end{aligned} \tag{7}$$

再次,当得到正确的 D_1 和 D_2 之后,VH-CP-ABE 可以保证总能获取正确的 T_{i+1}, 如式(8)所示。

$$\begin{aligned} &\frac{e(C_1, D_1)}{e(C_2, D_2)} \\ &= e(g, g_2)^{s \cdot \prod_{l=1}^{i+1} H(id_l \| s_l) \cdot \sum_{att_j \in S_{real} \cup \mathbb{W}} (\Delta_{j,S'_{real} \cup \mathbb{W}'(0) \cdot q(j))} } \\ &= e(g, g_2)^{sx \cdot \prod_{l=1}^{i+1} H(id_l \| s_l)} = T_{i+1} \end{aligned} \tag{8}$$

当且仅当存在 1 条授权链连接着根属性权威、区域属性权威以及交换机时,才能经过迭代计算出 T_0, 如式(9)所示。

$$T_{i+1}^{\prod_{l=1}^{i+1} \frac{1}{H(id_l \| s_l)}} = e(g_1, g_2)^s = T_0 \tag{9}$$

当且仅当获取正确的 T_0 时,VH-CP-ABE 算法才能获取正确的原始数据包 M, 如式(10)所示。

$$\frac{C_0}{T_0} = \frac{M \cdot e(g_1, g_2)^s}{e(g_1, g_2)^s} = M \tag{10}$$

综上所述,VH-CP-ABE 能够保证算法正确性。

4　安全性分析与性能比较

4.1　安全性分析

定理 2　如果 q-BDHE 问题是难解的,那么不存在多项式时间的敌手能以不可忽略的优势破解 VH-CP-ABE。

证明　由于区域授权与交换机授权原理一致,因此只要证明在得到根属性权威的授权之后,算法具备安全性即可。基于文献[18]的证明思路,本文设计了一个挑战游戏,游戏涉及敌手、模拟器以及挑战者 3 种角色。经过下面的推导可以得到:如果存在敌手在进行有限次的密钥询问以及解密询问后,在多项式时间内至少以优势 ε 破解 VH-CP-ABE,那么一定存在某个模拟器能够在多项式时间内以优势 $\varepsilon' = \varepsilon/2$ 解决 q-BDHE 难题。

挑战游戏的流程如下所述。

初始化阶段　挑战者产生 q-BDHE 问题的参数 $\{g, h, g^{\alpha}, g^{\alpha^2}, \cdots, g^{\alpha^q}, g^{\alpha^{q+2}}, \cdots, g^{\alpha^{2q}}, Z\}$, 并将参数发送给模拟器。模拟器定义 1 个真实的全局属性集合

$\Omega = \{att_1, att_2, \cdots, att_N\}$ 以及 1 个傀儡属性集合 $\Omega' = \{att_{N+1}, att_{N+2}, \cdots, att_{2N-1}\}$，使得 $q = 2N - 1$。

启动阶段 对于任意属性 $att_j \in \Omega$，模拟器产生 1 个随机数 $r_j \in Z_p^*$ 并计算 $h_j = g^{r_j} g^{\alpha q - j + 1}$，之后选择另 1 个随机数 $r_0 \in Z_p$ 并计算 $h_0 = g^{r_0} \prod_{j \in \mathbb{S}^* \cup \mathbb{W}^*} h_j^{-1}$。随后模拟器再选择一个随机数 $\alpha' \in Z_p^*$ 并计算 $g_1 = g^x = g^{\alpha'} g^{\alpha q}$，这里暗示了 $x = \alpha' + \alpha^q$，但是模拟器并不知道 α 到底是多少。

此时模拟器选择 1 组随机数 $d_2, d_3, e_1, e_2, e_3 \in Z_p^*$ 并计算 $\delta_1 = g_2 g^{e_1}, \delta_2 = g_2^{d_2} g^{e_2}$ 以及 $\delta_3 = g_2^{d_3} g^{e_3}$，然后生成公钥 $PK = \{g, g_2, Z, h_0, h_1, \cdots, h_q, \delta_1, \delta_2, \delta_3, H\}$。其中，$Z = e(g^{\alpha'}, g^{\alpha}) e(g^{\alpha q}, g^{\alpha})$ 且 $H: \{0,1\}^* \rightarrow Z_p$ 为随机预言机。随后敌手产生 1 个挑战访问策略 $\gamma_{t^*, \mathbb{S}^*}$ 并发送给模拟器。

询问阶段 1 在本阶段，敌手随机地、有限次地对模拟器进行以下 2 种类型的询问。

（1）授权询问。在该询问过程中，敌手向模拟器申请授权，模拟器反馈给敌手 A 相应的授权私钥。假设敌手发出关于身份标识 id_k、属性集合 S_{real} 的授权询问，这里规定 S_{real} 必须满足 $| S_{real} \cap \mathbb{S}^* | < t^*$。敌手选择 1 个随机数 $s_1 \in Z_p^*$，并发送 $H(id_1 \| s_1)$ 给模拟器，此时模拟器定义 1 组属性集合 $(\mathbb{T}, \mathbb{T}', \mathbb{T}'')$，这组属性集合满足以下关系：

$$\mathbb{T} = (S_{real} \cap \mathbb{S}^*) \cup \mathbb{W}^*$$

$$\mathbb{T} \subseteq \mathbb{T}' \subseteq (\mathbb{S}^* \cup \mathbb{W}^*)$$

$$\mathbb{T}'' = \mathbb{T}' \cup \{0\}$$

对于任意的属性 $att_j \in S_{real} \cup \Omega'$，模拟器可以获取 1 个 $N-1$ 次的随机多项式 q，使得 $q(0) = x = \alpha' + a^q$。然后模拟器针对该属性计算并产生相对应的私钥组件 sk_j，计算过程如下：

- 如果 $att_j \in \mathbb{T}'$，模拟器产生 2 个随机数 t_j 和 $r'_{1,j} \in Z_p^*$，使其满足 $q(j) = t_j$，$r_{1,j} = \alpha^j + r'_{1,j}$，然后计算 $a_{a,j} = g_2^{q(j)} (h_0 h_j)^{r_{1,j} \cdot H(id_1 \| s_1)}$ 以及 $b_{1,j} = g^{r_{1,j} \cdot H(id_1 \| s_1)}$。同时对于任意的 $k \in [1, 2N-1]/\{j\}$，计算 $c_{1,j,k} = h_k^{r_{1,j} \cdot H(id_1 \| s_1)}$。最后模拟器输出对应的私钥组件 $sk_{1,j} = \{a_{1,j}, b_{1,j}, \{c_{1,j,k}\}\}$。
- 如果 $att_j \notin \mathbb{T}'$，模拟器产生 1 个随机数 $r'_{1,j} \in Z_p$ 并计算 $r_{1,j} = r'_{1,j} - \Delta_{0,\mathbb{T}''}(j) \alpha^j$，通过拉格朗日插值法可得 $q(j) = \Delta_{0,\mathbb{T}''}(j) q(0) + \sum_{i \in \mathbb{T}''} \Delta_{0,\mathbb{T}''}(i) q(j)$。然后，模拟器计算 $a_{a,j} = g_2^{q(j)} (h_0 h_j)^{r_{1,j} \cdot H(id_1 \| s_1)}$ 以及 $b_{1,j} = g^{r_{1,j} \cdot H(id_1 \| s_1)}$。对于任意的 $k \in [1, 2N-1]/\{j\}$，计算 $c_{1,j,k} = h_k^{r_{1,j} \cdot H(id_1 \| s_1)}$。最后模拟器输出对应的私钥组件 $sk_{1,j} = \{a_{1,j}, b_{1,j}, \{c_{1,j,k}\}\}$。

（2）解密询问。敌手请求模拟器解密密文 $CT = (r, C_0, C_1, C_2, C_3)$，这里游戏规定不可以提交关于挑战密文的解密请求。假设此时密文的访问策略为 $\gamma_{t,S}$，那么模拟器首先计算 $c = H(\gamma_{t,S} \| C_0 \| C_1 \| C_2)$，然后检验以下等式是否成立。

$$e(g, C_2) = e(C_1, h_0 \prod_{j \in \mathbb{S} \cup \mathbb{W}} h_j) \tag{11}$$

$$e(g, C_3) = e(C_1, \delta_1^c \delta_2^r \delta_3) \tag{12}$$

如果以上任意一个等式不成立，模拟器将返回符号 $\perp$，否则进一步校验式(13)是否成立。

$$c + r d_2 + d_3 = 0 \tag{13}$$

如果成立则返回一个随机的消息给敌手 A，否则按照式(14)计算并输出明文。

$$M = \frac{C_0}{e\left(\frac{C_3}{C_1^{ce_1 + re_2 + e_3}}, g_1^{(c + rd_2 + d_3)^{-1}}\right)} \tag{14}$$

挑战阶段 敌手将长度相同的挑战明文 M_0 和 M_1 发送给模拟器。模拟器选择 1 个随机的 $\beta \in \{0, 1\}$ 并计算 $C_0^* = M_\beta Z \cdot e(h, g_2^{\alpha'})$，$C_1^* = h$，$C_2^* = h^{r_0}$，$c^* = H(\gamma_{t^*, \mathbb{S}^*} \| C_0^* \| C_1^* \| C_2^*)$，$r^* = -(c^* + d_3)/d_2$ 以及 $C_3^* = h^{c^* e_1 + r^* e_2 + e_3}$。最终模拟器生成挑战密文 $CT^* = (r^*, C_0^*, C_1^*, C_2^*, C_3^*)$ 并发送给敌手。

询问阶段 2 本阶段与询问阶段 1 基本相同。

（1）授权询问。敌手继续向模拟器发送关于某一属性集合 S_{real} 的授权请求，模拟器根据该属性集合生成相应的授权私钥 SK_u 并返回给敌手。在本阶段，私钥询问依然需要满足 $| S_{real} \cap \mathbb{S}^* | < t^*$。

（2）解密询问。敌手继续向模拟器发送关于密文 CT 的解密请求，然后模拟器对密文 CT 进行解密操作并返回相应的结果。在本阶段，敌手 A 不可以提交关于挑战密文 CT^* 的解密请求。

猜测阶段 敌手输出 β' 作为对 β 值的猜测。如果 $\beta = \beta'$，模拟器就将 $u' = 0$ 发送给挑战者，表示其认为 $Z = e(g, h)^{\alpha q + 1}$。如果 $\beta \neq \beta'$，模拟器就将 u'

$=1$ 发送给挑战者,表示其认为 $Z \neq e(g,h)^{\alpha^{q+1}}$。

当 $Z \neq e(g,h)^{\alpha^{q+1}}$ 时,挑战密文 CT^* 实际上就是一段随机的密文,敌手无法从密文中获取任何有用的信息,因此有:

$$\Pr[\beta' = \beta \mid Z \neq e(g,h)^{\alpha^{q+1}}] = \Pr[\beta' \neq \beta \mid Z \neq e(g,h)^{\alpha^{q+1}}] = 1/2 \tag{15}$$

当 $Z = e(g,h)^{\alpha^{q+1}}$ 时,挑战密文 CT^* 与真实的密文相同。假设敌手破解真实 VH-CP-ABE 的优势为 ε,由此有:

$$\Pr[\beta = \beta' \mid Z = e(g,h)^{\alpha^{q+1}}] = \varepsilon + 1/2 \tag{16}$$

因此模拟器 β 解决 q-BDHE 难题的优势为

$$\begin{aligned}\varepsilon' &= \frac{1}{2}\Pr[u = 0 \mid Z = e(g,h)^{\alpha^{q+1}}] + \frac{1}{2}\Pr[u = 1 \mid Z \neq e(g,h)^{\alpha^{q+1}}] - \frac{1}{2} \\ &= \frac{1}{2}\left(\varepsilon + \frac{1}{2}\right) + \frac{1}{2}\cdot\frac{1}{2} - \frac{1}{2} \\ &= \frac{\varepsilon}{2}\end{aligned} \tag{17}$$

综上所述,假如敌手能够在多项式时间内以不可忽略的优势破解 VH-CP-ABE,那么一定存在某个模拟器可以在多项式时间内解决 q-BDHE 难题。这与 q-BDHE 难题本身的难解性矛盾,所以不存在多项式时间敌手能够以不可忽略的优势破解 VH-CP-ABE。

4.2　性能分析

本节将对基于 VH-CP-ABE 构建的 SDN 信息安全访问系统模型进行性能分析。首先从各项功能指标上对 Waters 方法[20]、He 方法[16]、Teng 方法[18]、Odelu 方法[21]以及 VH-CP-ABE 进行分析比较,比较结果如表 1 所示。

Waters 方法[20]的公钥长度复杂度为 $O(|\Omega|)$,即公钥长度随着全局属性的总数线性增长;私钥长度复杂度为 $O(|S|)$,即私钥长度随着用户属性个数呈线性增长;密文长度复杂度为 $O(2|\mathbb{A}|)$,即密文长度随着访问策略属性个数的 2 倍线性增长。因此该方案在公钥、私钥和密文长度上均随其中所包含的属性个数的增加而线性增长,但是该方案既不支持层次化的属性权威也不支持私钥合法性认证。He方法[16]虽然是一种基于层次化属性权威的方法,但属性权威的数量以及层次化深度 l 在初始化之后便无法更改,从而限制了方案的扩展性,而且该方法并不支持私钥的合法性认证。Teng 方法[18]也是一种基于层次化属性权威的方法,该方案实现了密文长度常量化,同时方案的安全等级达到了 IND-CCA2,但是该方法也不支持私钥的合法性认证。Odelu 方法[21]整体非常轻量化,同时也给出证明表明该方案的安全等级达到了 IND-CCA2,只是与门访问策略缺乏灵活性,并且也不支持层次化权威以及私钥联合认证。

表 1　性能分析

方案	公钥长度	私钥长度	密文长度	层次化权威	私钥合法性认证	安全等级
Waters 方法[20]	$O(\|\Omega\|)$	$O(\|S\|)$	$O(2\|\mathbb{A}\|)$	否	否	IND-CPA2
He 方法[16]	$O(l)$	$O(\|S\|)$	$O(3\|\mathbb{A}\|)$	是	否	/
Teng 方法[18]	$O(2\|\Omega\|-1)$	$O(2\|S\|(\|\Omega\|-1))$	$O(1)$	是	否	IND-CCA2
Odelu 方法[21]	$O(\|\Omega\|)$	$O(1)$	$O(1)$	否	否	IND-CCA2
VH-CP-ABE	$O(2\|\Omega\|-1)$	$O(2\|S\|(\|\Omega\|-1))$	$O(1)$	是	是	IND-CCA2

本方案在 Teng 方法[18]的基础上进行了进一步的扩展,所提出的 VH-CP-ABE 不仅保证密文长度常量化、层次化的属性权威可以在理论上无限扩展,还支持在解密过程中对私钥进行联合认证。在解密过程中,所使用的私钥必须经过所有与该私钥发布相关的属性权威的认证,只有通过认证才能最终获取消息明文。比如某机构经过授权获取了私钥,但是并没有授权可以向他人发布私钥,而该机构却肆意向他人发布私钥。在这样的情况下,即使有人获取该机构发布的私钥,那么他仍然不能正确地解密。此外经过安全性证明,本文提出的 VH-CP-ABE 的安全性达到了 IND-CCA2 等级。当然本方案与 Teng

方法[18]一样牺牲了私钥的长度，使得私钥长度复杂度上升至 $O(2|S|(|\Omega|-1))$。不过每个私钥都是存储在不同的用户手中，并不会对用户本身造成非常大的存储负担。

为了反映本文提出方案的性能，对基于 VH-CP-ABE 的 SDN 信息安全访问系统模型进行了仿真实验并与 He 方法[16]进行了比较。仿真平台选择为 Windows 10(Intel (R) Core (TM) i7-5600U@2.6 GHz,8 GB RAM)，选择的代码库 JPBC2.0，方案基于 512 位椭圆曲线，阶为 120 bit 大素数，仿真记录了在不同属性数量下的密钥长度、加密时间以及解密时间。

本方案模型在不同属性数量下的密文长度时间如图 2 所示。可以看到访问策略里的属性个数从 1 增加到 10 的过程中，密文的大小稳定在1.25 kB左右。Teng 方法[18]的密文大小则基本稳定在1.5 kB左右。与 Teng 方法[18]类似，随着属性的增加，密文长度基本没有变化。因此随着属性数量的增长，本方法的密文存储并不会对 SDN 控制层造成明显的负担。

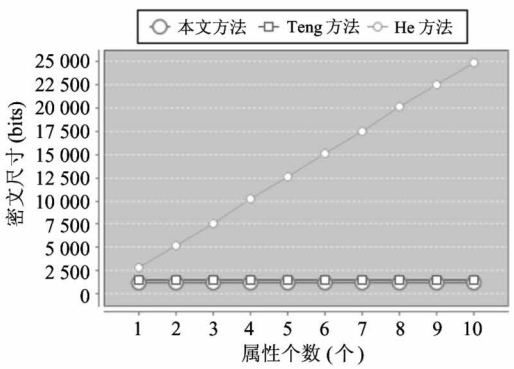

图 2　密文尺寸记录

图 3 记录了本方案在访问策略包含不同的属性数量下的加密时间。可以看到本方法与 Teng 方法[18]在加密时间上表现相当，且远优于 He 方法[16]。在访问策略里包含 1 个属性数量的情况下加密时间大约是 40 ms。随着属性数量的增长，可以看出加密时间呈现出了线性增长，终于在属性数量达到 10 个的时候加密时间达到了 131 ms。尽管加密时间呈现出了线性增长，但是在模型中，一般的 SDN 设备属性数量并不会超过 10 个，这与实际情况比较吻合。

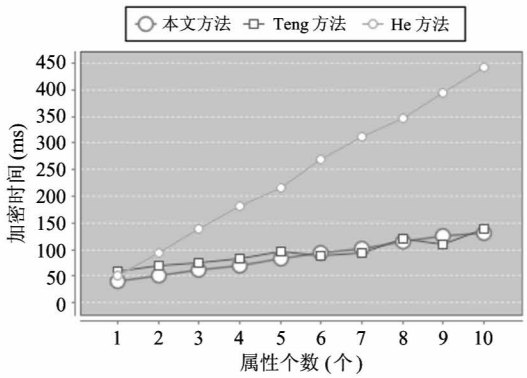

图 3　加密时间记录

在解密组件的属性集合包含不同属性数量情况下，记录了相应的密文解密时间，如图 4 所示。在属性集合包含 1 个属性的情况下，解密时间大约是 151 ms。但是随着属性数量的增加，解密时间呈现了指数型上升，主要是因为解密过程中计算 D_1 和 D_2 的时间复杂度几乎达到了 $O(|S|^2)$。He 方法[16]由于采用了线性秘密贡献方案(linear secret sharing scheme，LSSS)构造访问策略，在解密过程中需要根据线性秘密贡献矩阵进行高斯消元恢复秘密，因而随着属性数量增长解密时间迅速攀升。可以看到当属性不超过 10 个时，本方法与 He 方法[16]解密时间相当；而当属性超过 10 个之后本方法将逐渐展现性能优势；当属性数量达到 15 个时，本方法的解密时间相比 He 方法节省了约 1/3。而与 Teng 方法[18]相比，本方法的解密时间略高，这是因为本方法在解密过程中需要对私钥的合法性进行认证，这种计算开销上的牺牲换取了安全性的提升。

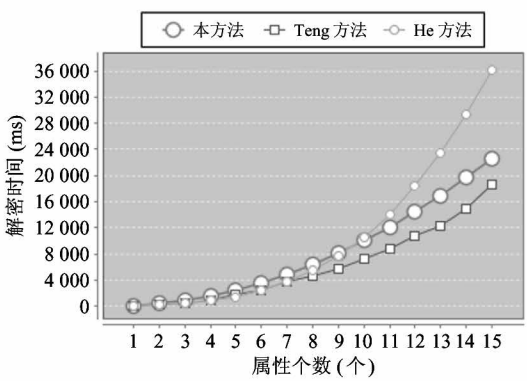

图 4　解密时间记录

综上所述,在安全性方面,基于 VH-CP-ABE 构建的 SDN 信息安全访问系统模型相比其他类似方案有显著地提升。同时结合实际情况考虑,本方案也保持了一定程度的高效性和可用性。因此其整体的性能较为可观。

5　结　论

软件定义网络作为一种控制与数据分离的新型网络架构,采用集中化控制降低了网络管理的成本,但同时由于缺少安全保护机制使得敏感信息极易被远程调用。为解决该问题,本文提出了基于可认证层次化的密文策略属性加密算法。采用层次化属性权威不仅削弱了属性权威过于集中的权力,也有效分散了计算负载。同时算法使得消息密文的尺寸常量化,可有效降低密文存储开销,有利于敏感信息的集中化管理。此外,授权私钥绑定了与授权相关的用户以及局部属性权威的唯一身份识别,使得算法支持在解密过程中对私钥的合法性认证,因此即使其他非认证机构擅自发布私钥,该私钥也无法用于解密。理论分析证明,本文提出的算法能够在随机预言机模型下达到 IND-CCA2 安全等级。基于该算法构建了 SDN 信息安全访问系统模型,性能分析以及仿真实验结果表明,本模型可以有效防止 SDN 设备或者用户的敏感信息泄露,使 SDN 信息管理具备良好的安全性和高效性。下一步的工作将重点优化局部属性权威以及用户的授权开销,降低私钥发布的计算量。同时优化解密的计算负载,使之对 SDN 各类应用更加友好。

参考文献

[1] Foerster K T, Schmid S, Vissicchio S. Survey of consistent software-defined network updates[J]. *IEEE Communications Surveys and Tutorials*, 2018, 21(2): 1435-1461

[2] Yang L, Dantu R, Anderson T, et al. Forwarding and control element separation (ForCES) framework, 10.17487/RFC3746[R]. Los Angeles: RFC, 2004

[3] Nayyer A, Sharma A K, Awasthi L K. Laman: a supervisor controller based scalable framework for software defined networks[J]. *Computer Networks*, 2019, 159: 125-134

[4] Hassas Yeganeh S, Ganjali Y. Kandoo: a framework for efficient and scalable offloading of control applications [C]//Proceedings of the 1st Workshop on Hot Topics in Software Defined Networks, Helsinki, Finland, 2012: 19-24

[5] 张栋, 郭俊杰, 吴春明. 层次型多中心的 SDN 控制器部署[J]. 电子学报, 2017, 45(3): 680-686

[6] Klaedtke F, Karame G O, Bifulco R, et al. Access control for SDN controllers[C]//Proceedings of the 3rd ACM SIGCOMM Workshop Hot Topics Software Defined Networking, Chicago, USA, 2014: 1325-1335

[7] Jäger B, Röpke C, Adam I, et al. Multi-layer access control for SDN-based telco clouds[C]//Proceedings of 20th Nordic Conference on Secure IT Systems, Stockholm, Sweden, 2015: 197-204

[8] Kamath A V, Sudarshan S, Kataoka K, et al. SAFE: software-defined authentication framework[C]//Proceedings of the 12th Asian Internet Engineering Conference, Bangkok, Thailand, 2016: 57-63

[9] Xue L, Yu Y, Li Y, et al. Efficient attribute-based encryption with attribute revocation for assured data deletion [J]. *Information Sciences*, 2019, 479: 640-650

[10] Li J, Yu Q, Zhang Y, et al. Key-policy attribute-based encryption against continual auxiliary input leakage[J]. *Information Sciences*, 2019, 470: 175-188

[11] Liu Z, Duan S, Zhou P, et al. Traceable-then-revocable ciphertext-policy attribute-based encryption scheme[J]. *Future Generation Computer Systems*, 2019, 93: 903-913

[12] Chase M, Chow S S M. Improving privacy and security in multi-authority attribute-based encryption[C]//Proceedings of the 2009 ACM Conference on Computer and Communications Security, Chicago, USA, 2009: 121-130

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

[14] 闫玺玺, 孟慧. 支持直接撤销的密文策略属性基加密方案[J]. 通信学报, 2016, 37(5): 44-50

[15] Lin G, Hong H, Sun Z. A collaborative key management protocol in ciphertext policy attribute-based encryption for cloud data sharing[J]. *IEEE Access*, 2017, 5: 9464-9475

[16] He S, Liu J, Mao J, et al. Hierarchical solution for access control and authentication in software defined networks[C]//Proceedings of the 8th International Conference on Network and System Security, Xi'an, China, 2014: 70-81

[17] Touati L, Challal Y, Bouabdallah A. C-CP-ABE: cooperative ciphertext policy attribute-based encryption for the Internet of Things[C]//Proceedings of 2014 International Conference on Advanced Networking Distributed Systems and Applications, Bejaia, Algeria, 2014: 64-69

[18] Teng W, Yang G, Xiang Y, et al. Attribute-based access control with constant-size ciphertext in cloud computing [J]. *IEEE Transactions on Cloud Computing*, 2017, 5 (4):617-627

[19] Li S D, Dai Y Q. Secure two-party computational geometry[J]. *Journal of Computer Science and Technology*, 2005, 20(2): 258-263

[20] Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization [C]//Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, 2011: 53-70

[21] Odelu V, Das A K, Rao Y S, et al. Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment[J]. *Computer Standards and Interfaces*, 2017, 54(1): 3-9

A research on inter-domain transmission system of multi-center SDN based on improved HABE algorithm

Zhou Bo*, Wang Shulei**

(*Electronic Information Technology School, Nanjing Vocational College of Information Technology, Nanjing 210023)

(**School of Civil Aviation Flight, Changzhou Institute of Technology, Changzhou 213032)

Abstract

Hierarchical multi-center software defined network (HMC-SDN) is an efficient architecture to improve service quality and scalability for large-scale network. However, inter-domain transmission among switches in existing HMC-SDN architecture is short of appropriate secure protection, which makes sensitive data leakage easy and undetectable. A verifiable and hierarchical ciphertext-policy attribute-based encryption (VH-CP-ABE) is proposed. Hierarchical attribute authorities are built based on hierarchical controllers. Switches encrypt data are packaged by the authorized private key and the access policy, which keeps the size of ciphertext constant and inter-domain transmission secure. Moreover, identities of the switch and corresponding controllers are embedded into its authorized private key, so it can verify the legitimacy of the authorized private key during decryption in order to improve security of inter-domain transmission. It can be proved that the proposed scheme achieves IND-CCA2 security in random Oracle model. The performance analysis and simulation show that it provides both good security and efficiency to inter-domain transmission in HMC-SDN.

Key words: software defined network(SDN), inter-domain transmission, attribute-based encryption (ABE), access control, key verification