ISSN 1004-9037,CODEN SCYCE4
Journal of Data Acquisition and Processing Vol. 38,No. 2,Mar. 2023,pp. 314－323
DOI:10. 16337/j. 1004-9037. 2023. 02. 008

http://sjcj. nuaa. edu. cn
E-mail:sjcj@nuaa. edu. cn
Tel/Fax:＋86-025-84892742

基于属性加密的DDS访问控制方案

任颖超，燕雪峰

(南京航空航天大学计算机科学与技术学院,南京 211106)

摘　要：数据分发服务(Data distribution service,DDS)是一种可靠的实时数据通信中间件标准,它是面向基于发布/订阅模型的分布式环境,在各个领域得到了广泛应用,但现有研究涉及DDS安全技术的成果较少,而在实际应用中发布订阅系统存在多种安全威胁。为了建立灵活可靠的安全机制来确保发布订阅信息的安全性,提出一种以数据为中心的访问控制方案。在属性加密的基础上,对访问树结构进行优化处理,结合发布订阅环境增加属性信任机制。之后采用制定属性连接式与授权策略的方式对发布订阅信息进行加密匹配,并建立DDS访问控制模型来控制发布订阅系统内信息的交互,实现数据的安全分发。经过实验验证,该方案既能够应对DDS存在的几种安全威胁,保障发布订阅信息的机密性,也能够实现系统对特定信息的访问控制,并且发布者订阅者不需要共享密钥,减少了密钥管理的开销。

关键词：访问控制;数据分发服务;数据安全;属性加密

中图分类号：TP309.2　　**文献标志码**:A

DDS Access Control Scheme Based on Attribute Encryption

REN Yingchao, YAN Xuefeng

(College of Computer Science and Technology, Nanjing University of Aeronautics & Astronautics, Nanjing 211106, China)

Abstract: Data distribution service(DDS) is a reliable real-time data communication middleware standard. It is oriented to a distributed environment based on the publish/subscribe model. It has been widely used in various fields. However, there are few achievements in existing research involving DDS security technology. There are many security threats to the publishing and subscribing system in practice. In order to establish a flexible and reliable security mechanism to ensure the security of publishing and subscribing information, a data-centric access control scheme is proposed. On the basis of attribute encryption, the access tree structure is optimized, and the attribute trust mechanism is added in combination with the publishing and subscribing environment. Afterwards, the publicating and subscripting information is encrypted and matched by formulating attribute connection and authorization strategies, and a DDS access control model is established to control the interaction of information in the publicating and subscripting system and realize the safe distribution of data. The experimental verification shows the solution can deal with several security threats in DDS, guarantee the confidentiality of publishing and subscribing information, as well as realize the system's access control to specific information, and publishers and subscribers do not need to share keys, reducing the overhead of key management.

Key words: access control; data distribution service; data security; attribute encryption

---

基金项目:国家重点研发计划(2018YFB1702702)。
收稿日期:2021-06-03;**修订日期**:2022-11-04

引 言

数据分发服务(Data distribution service,DDS)目前已经广泛应用于各种大型的分布式发布订阅系统,在多个领域有着广泛应用[1]。DDS通信技术极大地提高了各种发布订阅系统的数据通信效率与灵活性,同时,发布订阅系统的信息安全问题也变得尤为重要[2]。由于DDS的松耦合性,运用DDS技术的发布订阅系统存在多种安全威胁,大致可以分为以下几个方面:(1)域分离未受保护,攻击者可以轻松加入DDS发布/订阅系统中的任何其他域;(2)未授权的订阅,用户或应用程序未经系统允许订阅了不相关的数据;(3)消息的篡改与重放,存在恶意用户或程序会对DDS发布/订阅系统中的数据进行损坏或篡改的可能[3]。

DDS标准提出DDS 中存在的几种安全问题,如未授权的发布和订阅、未授权的数据访问等,但是并没有考虑DDS在实际发布订阅系统中存在的安全问题,也没有从用户的角度提出解决这些问题的方法。文献[4]提出了基于安全协商的DDS通信模型,在原DDS通信中间件的基础上增加了与安全相关的证书授权中心(Certificate authority,CA)、身份认证组件。文献[5]结合DDS数据分发的特点,设计了一种以身份认证为基础的安全组件。文献[6]通过分析DDS协议存在的不足,设计了一种新的高安全数据分发服务身份认证协议。文献[7]从服务质量(Quality of service,QoS)策略配置的角度,结合实际的DDS发布订阅系统,提出了"信息安全属性-信息安全策略-QoS策略"的安全体系。文献[8]通过数据挖掘算法查找可疑用户,对其进行限制实现对订阅攻击的有效防御。文献[9]提出一种无代理的基于身份验证的机密性和访问控制方案,通过细粒度的密钥管理,按照订阅属性的顺序排列等方法实现加密、解密和路由成本,该方案有可靠的安全性且系统开销较小。文献[10]提出了用于多域发布/订阅系统的基于公钥基础设施(Simple public key infrastructure,SPKI)的访问控制体系结构,通过应用分散的信任管理能够方便且可扩展地在跨越多个独立管理域的发布/订阅系统中实施访问控制,该方案基于SPKI更适合分布式的发布/订阅系统。文献[11]提出了一种新的发布/订阅系统的撤销技术,可以有效地删除无效或恶意的订阅者,而不需要重新生成和重新分配新密钥,减小了系统对密匙管理的额外开销。

现有关于DDS安全技术的研究大多基于传统的对称加密、非对称加密和数字证书等,运用这些传统的加密认证方法时,往往存在第三方认证中心授权中心(Certificate authority,CA)去集中管理密钥,这不符合DDS无中心、松耦合的特点,尤其是当系统中参与者较多时,会导致单点瓶颈。相比于传统对称加密与非对称加密算法,属性加密具有以下优势:(1)资源提供方仅需要根据属性加密消息,无需关注群里中成员的数量和身份,降低了多次加密的开销同时保护用户隐私;(2)只有符合密文或密匙属性要求的群体成员才能解密消息,很契合DDS的发布订阅机制,也保证了数据的机密性;(3)属性加密机制中用户密钥与随机多项式或随机数相关,不同用户的密钥无法联合,防止了用户的串谋攻击;(4)对属性进行管理的开销远远小于密钥管理。因此文本基于属性加密研究适用于DDS的安全访问控制方案。

本文的主要工作为:(1)在密文策略属性基加密算法(Ciphertext-policy attribute-based encryption,CPABE)的基础上,通过属性信任机制为访问树叶子节点赋予权值,并对树形访问结构进行优化,从而减少计算开销,尽可能降低对DDS实时性的影响;(2)提出一种基于密文策略属性基加密的DDS访问控制方案,通过制定属性连接式与授权策略的方式对发布订阅信息进行加密匹配,控制发布订阅信息的安全性。该方案相比于传统的加密认证技术,更加契合DDS的发布订阅机制,并且不需要进行集中的密钥管理。

1 DDS安全威胁

DDS作为高效的信息分发中间件,采用松耦合的以数据为中心的订阅-发布模型(Data-centric publish-subscribe,DCPS),已被用于各种分布式发布订阅系统中。在这些系统中,发布者只需要将对应主题的数据发布到DDS域中,而无需关注数据订阅者是谁,订阅者只需要从DDS域中订阅相关主题的数据,而无需关注该主题数据的发布者是谁,在实际应用系统中,数据从发布方到订阅方的过程是不安

全的,数据存在被窃听、被篡改的威胁[3]。任何关联特定主题的应用程序节点都能够获取到对应的数据,并可以对数据进行篡改。

图1所示,参与者Turdy是入侵者,它与其他代理程序节点连接到相同的网络,未经授权就加入了DDS数据域,并且可以未授权发布任意数据内容。参与者Eve是窃听者,它无权订阅有关主题Topic的内容,但是它利用已经连接到的网络窃取了该主题数据。参与者Mallory是恶意节点,它虽然授权订阅主题Topic上的数据,但是在未授权发布的情况下在主题Topic上发布并篡改信息。

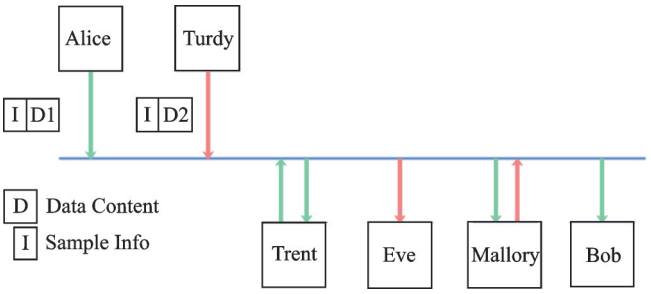

图1 威胁模型

Fig.1 Threat model

2 发布订阅环境下的属性加密方案模型

CPABE是一种灵活高效的加密机制,它不需要通信双方共享同一个密钥,密钥的生成可以根据用户的相关属性特征自动生成,这种机制很契合DDS的无中心、松耦合性的特点,能够满足DDS应用系统环境下的安全需求。但将CPABE运用到发布订阅系统的过程中,其灵活性与实时性仍需要进一步改善。本节主要介绍如何结合DDS技术的特点,对CPABE的访问树结构以及流程进行优化处理。

2.1 树形访问结构的构造与优化

定义1 访问结构[12]:设$\{P_1,P_2,\cdots,P_n\}$表示参与者的集合。对于一个访问结构A来说,它是P的一个子集$A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$,且$A$非空。如果有任意的集合$A$、$B$满足$B\in A$和$B\in C$,同时$C\in A$,那么访问结构$A$是单调的。

定义2 访问树:访问树为一棵多叉树T_r,树的非叶子结点表示阈值或者逻辑关系,叶子节点表示属性值。定义num_x表示x的的子节点数,k_x表示节点x的域值,$0<k_x<\mathrm{num}_x$。若$k_x=1$,则表示"或"门关系;若$k_x=\mathrm{num}_x$,则表示为"与"门关系;若$0<k_x<\mathrm{num}_x$,表示至少需要满足k_x个属性节点。此外,定义parent(x)表示x的父节点,attr(x)表示叶子节点x的属性值。对节点的子节点标记,从1到nums,index(x)表示节点x标记号。

定义3 信任值:规定发布订阅系统中的参与者的不同属性具有不同的信任程度,信任程度在访问树中以不同的权重值分配给各叶子节点。

图2是一个简单的树形访问结构,构造方式是从上到下、从左到右,树的叶子节点对应参与者的属性集,而非叶子节点是门限访问结构。根节点(2/3)表示3个子树要满足其中任意两个,根节点左边的子节点(3/3)表示要同时满足A_1、A_2、A_3这3个属性,其余节点类似。满足该访问结构的属性集合为$S=\{[A_1,A_2,A_3,B_1],[A_1,A_2,A_3,C_1],[A_1,A_2,A_3,C_2]\}$,以及$S$中各属性集与其他属性集的并集。

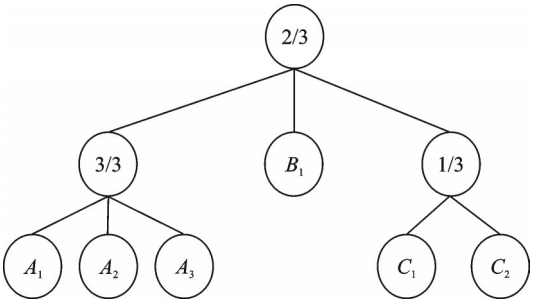

图2 访问树构造

Fig.2 Structure of access tree

该访问树的构造过程如下:根结点为2/3代表门限值为2,有3个子节点,每一个父节点parent(x)会对应一个随机的多项式,随机多项式由算法生成,父节点的门限值减一即为多项式的最高次数,多项式的常数项设置为秘密数。将父节点的子节点index(x)依

次代入多项式,所得值作为新生成的秘密值并保存到该子节点index(x)。对于所有的parent(x)都按照上述方式生成随机多项式,并将常数项设置为父节点传来的值,也按照上述方式生成新的秘密值传给子节点。对于叶子节点index(x),得到父节点的秘密值之后,用属性attr(x)对秘密值进行加密处理。

访问树结构是作为策略嵌入密文当中,在加密时,每个叶子节点都会进行两次指数运算,对访问树结构进行解密时,叶子节点会进行两次线性对运算,非根节点的父节点会进行指数运算。所以访问树结构的复杂度往往会影响加解密的开销,而且在实际的DDS发布订阅系统中,参与者拥有的属性类别也不相同,对大量的参与者制定统一的访问树策略,往往会形成比较复杂的结构。因此,在本文的安全模型中,对访问树结构进行优化处理。

图3为访问树结构优化的简单示例,不同子树的叶子节点可以根据信任权重值进行合并,同时,非根节点的父节点也可以根据特定情况进行门限值合并。化简后的授权集合与原先的访问树一致,但是结构更为简单,减少了计算。对于图3(a)的情形,两棵子树存在相同属性的叶节点A_3,左右两边的叶子节点A_3可以根据权重值与父节点门限值的乘积进行合并,权值为0的节点视为无关属性节点,合并后可以减少一个传输节点和两个叶子节点,优化前后的访问授权集合保持不变。对于图3(b)的情形,根节点(1/2)与两个传输节点的门限(1/2)可以相乘计算,最终合并为一个新门限值的根节点,减少了两个传输节点且原本的访问集合保持不变。对于图3(c)的情形,不同的是根节点为(n/n),此时需要将根节点(2/2)与传输节点(1/2)替换,并合并叶子节点修改其权重值,最终可以减少一个传输节点和一个叶子节点,且优化前后的访问集合保持不变。

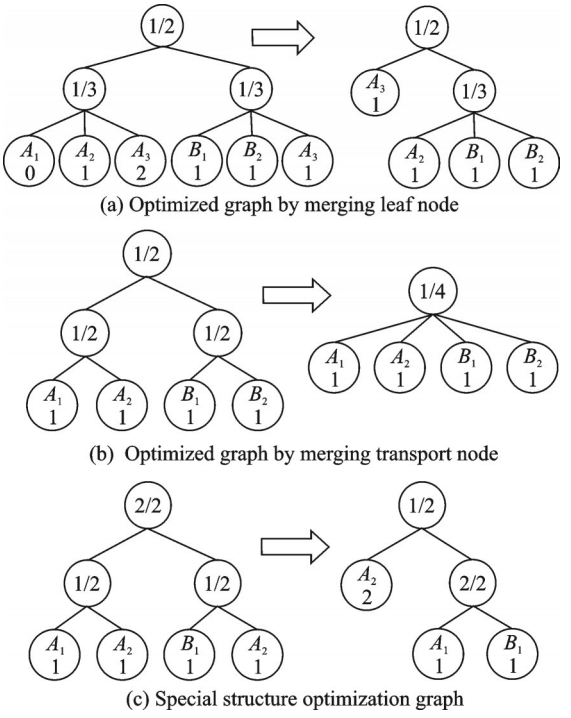

图3 访问树结构优化图

Fig.3 Structure optimization of access tree

2.2 增加属性权值的CPABE算法

在CPABE算法[13]的基础上,加密方案主要分为访问服务初始化阶段、属性信任计算阶段、访问树策略加密阶段、参与者属性密钥生成阶段和参与者解密阶段5步。增加属性信任阶段的目的是为了对参与者进行简单有效的认证计算,从而为其自动分配属性集,去除无关属性,同时为不同属性赋予权值,便于访问树的优化。

假设 G_1 是一个 p 阶的双线性群,其中 p 为素数,g 为群 G_1 中的一个生成元。有映射 e: $G_1\times G_1\rightarrow G_2$ 为双线性映射。每一个属性值表示为集合 Z_p 中的一个元素,定义拉格朗日系数 $\Delta_{i,s}$ 为

$$\Delta_{i,s}(x)=\prod_{j\in s,j\neq i}(x-i)/(i-j) \tag{1}$$

此外,使用一个哈希函数 H,输入为任意一个二进制的字符串,输出为随机群内的元素。

(1)访问服务初始化

Setup(k)→(P_K,M_K): 该算法输入系统公共参数 k,输出公共密钥 P_K 和主密钥 M_K。初始化选择素数阶为 p 的双线性群 G_1,g 为群 G_1 中的一个生成元,k 决定群大小。集合中随机选取2个值 $\alpha,\beta\in Z_p$,公共密钥 P_K 为

$$P_K=(G_0,g,g^{\beta},e(g,g_2)^{\alpha}) \tag{2}$$

(2)属性信任计算

Trust(V)→T:域中的参与者提交各项信息 V,算法对各项信息与全局属性集 U进行分类匹配,全局属性集U分为正面属性集U_p和负面属性集U_q,并具有对应权值w_i。匹配得到正面信息个数 m 与负面信息个数n为

$$m=\left|U_p\cap V\right| \tag{3}$$

$$n=\left|U_q\cap V\right| \tag{4}$$

再计算参与者信程度 T, T 采用二元组来表示 $[C,D]$,C和 D分别表示可信程度与不可信程度

$$C=\left(\sum_{i=1}^{m}w_{pi}+\sum_{j=1}^{n}w_{qj}\Big/2\right)\Bigg/\left(\sum_{i=1}^{m}w_{pi}+\sum_{j=1}^{n}w_{qj}\right) \tag{5}$$

$$D=\sum_{j=1}^{n}w_{qj}\Bigg/\left(\sum_{i=1}^{m}w_{pi}+\sum_{j=1}^{n}w_{qj}\right) \tag{6}$$

参与者的信任值 T 计算如下

$$T=w\times[C,D] \tag{7}$$

式中w为权重因子,$w\in(0,1)$。若 T 满足信任条件 $wC>a, wD<b$,则为其分配对应的正面属性集,去除冗余属性,否则不能加入DDS数据域中。

(3)访问树策略加密

Encrypt(P_{K}, M, T)→C_T: 加密算法在优化后的树形访问结构 T下加密消息M。该算法从根节点r开始由上往下,为每一个节点选取一个多项式q_x。访问树的节点的度d_x为该节点门限值k_x-1,有$d_x=k_x-1$,多项式为$q_x(0)=q_{\mathrm{parent}(x)}(\mathrm{index}(x))$。设树 T中叶子节点的集合为 Y,则可以计算生成密文C_T为

$$C_T=(T,\tilde{C}=Me(g,g_2)^{\alpha s}, C=h^s, \forall y\in Y) \tag{8}$$

$$C_y=g^{q_y(0)}, C'_y=H(\mathrm{attribute}(y)^{q_y(0)}) \tag{9}$$

(4)参与者属性密钥生成

KeyGen(M_{K}, S)→S_{K}: 算法的输入为DDS参与者的属性集 S,生成与DDS参与者属性关联的密钥。对每一个属性$j\in S$都选择一个随机数$r\in Z_p$,生成参与者的密钥S_{K}为

$$S_{\mathrm{K}}=(D=g^{\frac{\alpha+\gamma}{\beta}}, \forall j\in S: D_j=g^r\cdot H(j)r_j, D'_j=g^r) \tag{10}$$

(5)参与者解密密文

Dec(C_T, S_{K}, x)→M: 算法的输入包含密文$C_T=(T,\tilde{C},C,\forall y\in Y: C_y, C'_Y)$,解密密钥$S_{\mathrm{K}}$和优化后的访问树节点$x$。设$i=\mathrm{att}(x)$,如果$i\in S$,则

$$\mathrm{Dec}(C_T,S_{\mathrm{K}},x)=e(D_i,C_x)/e\left(D'_j,C'_x\right)=e(g,g)^{rq_x(0)} \tag{11}$$

经过如下计算就可以输出明文

$$M=\tilde{C}/(e(C,D)/A)=\tilde{C}\Bigg/\left[e\left(h^s,g^{\frac{\alpha+\gamma}{\beta}}\right)\Big/e(g,g)^{rs}\right] \tag{12}$$

3 基于属性授权策略的DDS访问控制

3.1 属性授权策略

本文的方案采用基于属性的授权策略,属性$w=(nm,\mathrm{val})_1$,表示属性nm具有值val,这些属性可以

用连写形式写:$w_1 \wedge w_2 \wedge \cdots \wedge w_m$,表示一个参与者具有所有属性$w_1, w_2, \cdots, w_m$,同时需要保证属性的连接形式具有相同的规范,连接的属性具有固定顺序。给定事件主题tp,此主题数据的发布者可以使用属性策略来指定有资格访问主题tp数据的订阅者。

定义4 授权策略:基于优化的访问树结构,一个策略可表示为$T_{tp}=(w_{11} \wedge w_{12} \wedge \cdots \wedge w_{1m}) \vee \cdots \vee (w_{n1} \wedge w_{n2} \wedge \cdots \wedge w_{nm})$,该形式代表如果参与者具有至少一组从$w_{11} \wedge w_{12} \wedge \cdots \wedge w_{1m}$到$w_{n1} \wedge w_{n2} \wedge \cdots \wedge w_{nm}$的连接属性,就可以访问该结构控制的资源。例如,订阅者的属性表示为$\gamma=(w'_{11} \wedge w'_{12} \wedge \cdots \wedge w'_{1m}) \vee \cdots \vee (w'_{k1} \wedge w'_{k2} \wedge \cdots \wedge w'_{km})$,这意味着该订阅者具有$k$个不同的连接属性,如果$\gamma$中至少有一组连接属性也出现在tp中,那么$\gamma$就满足tp的策略,订阅者的属性就会链接到其属性私钥,属性私钥可以解密对应tp的密文,并获取对应的数据或资源。

3.2 访问控制模型

在DDS发布订阅系统中,发布者和订阅者之间存在多对多的关系,本节将以一个发布者和一个订阅者的通信来描述方案的DDS访问控制模型。图4为DDS访问控制模型,包含访问控制服务,域参与者以及数据域。其中访问控制服务拥有该发布订阅系统所有参与者的属性集合U,可以对尝试加入DDS域的参与者进行属性信任认证,去除无关属性并为其分配合适的属性集A_i,同时,该访问控制服务可以初始化系统的公共密钥P_K和主密钥M_K,并将P_K和M_K传给加入DDS域中的参与者。其余两个节点是经过属性信任的DDS参与者,参与者在加入DDS域之前,访问控制组件根据参与者的信息和自身属性进行信任计算得到参与者的信任值,若信任值满足一定条件,方可加入DDS数据域并获得属性集A_i,公共密钥P_K和主密钥M_K。若参与者创建了数据发布者,可以根据属性集生成访问树T,并将访问树T作为访问策略嵌入密文中;若参与者创建了数据订阅者,可以根据属性集生成自己的属性密钥,若密钥匹配密文的属性策略,方可解密。

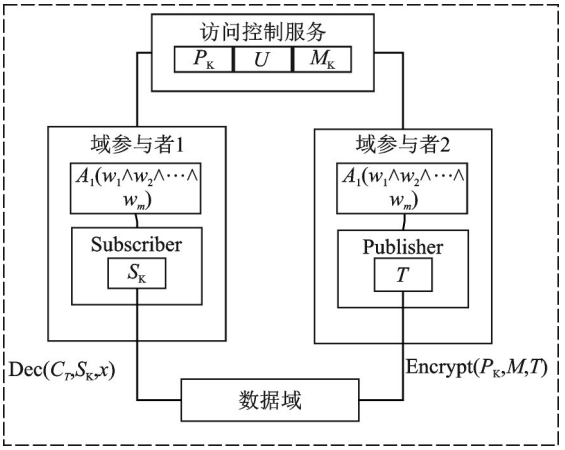

图4 访问控制模型

Fig.4 Access control model

3.3 访问控制交互

图5描述了单点通信的DDS与访问控制服务交互过程,大致流程如下:

(1)访问控制服务初始化,生成系统公共密钥P_K和主密钥M_K。

(2)参与者初始化,向DDS域创建自己的主题类型,注册各种数据类型参与者向访问控制服务申请信任,访问控制服务根据参与者的主题和数据类型进行信任计算,若信任值满足条件,则向该参与者分配

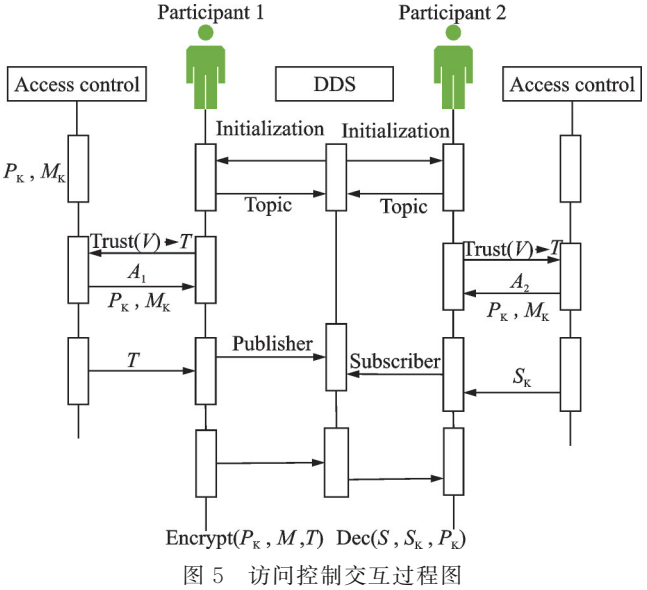

图5 访问控制交互过程图

Fig.5 Access control interaction process diagram

属性集A_i、P_K、M_K。

(3)参与者1要进行信息发布,创建一个发布者,访问控制服务根据其属性集A_1生成访问树结构的访问策略T。参与者2要订阅主题tp的秘密信息,创建一个订阅者,并调用属性密钥生成算法根据其属性集A_2生成自身的属性密钥S_K。发布者选择需要加密的秘密信息M,调用访问控制服务加密该信息并将访问控制策略T嵌入密文C_T中,之后发布密文信息。订阅者接收到密文信息后,用属性密钥S_K对其进行解密,若S_K能够匹配T,则能够解密出密文消息C_T获得明文M。

4 实验与分析

4.1 安全性分析

针对DDS存在的3种威胁来讨论,对于域分离未受保护这个威胁,访问控制服务能够提供属性信任的服务,可以根据主题和数据类型对试图加入DDS域的参与者进行有效验证,主题数据类型经过信任计算后满足信任条件,则可以加入DDS域,反之不能加入,可以阻拦恶意加入DDS域的节点应用。对于未授权的订阅,由于发布者发布的信息是经过访问策略T加密的,当订阅者拥有满足访问结构T的属性密钥S_K,才能够获得发布者的信息,因此信息发布者可以决定哪些订阅者获取到信息。对于消息的篡改与重放,方案中主题和数据类型都关联了对应的属性集,一种主题和一类数据都对应唯一的属性集,假设恶意节点的参与者订阅到了主题T的数据,但属性集不对应T的属性,则它发布到的信息也不会被订阅者接收,有效防止了恶意节点对消息的篡改。

4.2 仿真实验验证

实验环境在Intel(R) Core(TM) i5-10400 CPU @2.90 GHz主频2.90 GHz,内存16.0 GB,基于Windows 10操作系统安装的Ubuntu虚拟机上。在OpenDDS开发的拥有多个节点的发布订阅系统中进行模拟验证,该系统初始化建立5个参与者,分别为数据发布者A、数据订阅者B、数据入侵者C、数据窃听者D、数据篡改者E。定义系统的全局属性集合$U=\{w_1,w_2,w_3,w_4,w_5,w_6\}$,其中$w_1$表示属性名主题属性对为(Topic,$T$);$w_2$表示属性名类型,属性对为(type, red);$w_3$表示属性名端口,属性对为(port,6000);$w_4$表示属性名域id,属性对为(id,1);$w_5$表示属性名读权限,属性对为(read,1);$w_6$表示属性名写权限,属性对为(write,1)

如表1所示,在该系统中,参与者A的属性集为$w_1\wedge w_2\wedge w_3\wedge w_4\wedge w_5\wedge w_6$,参与者$B$的属性集为$w_1\wedge w_2\wedge w_3\wedge w_4\wedge w_5$,参与者$C$的属性集为$w_2$,参与者$D$的属性集为$w_1\wedge w_2\wedge w_4$,参与者$E$的属性集为$w_2\wedge w_4\wedge w_6$。属性集所对应的属性密钥为$S_{K_i}(i=a,b,c,d,e)$。

如表2所示,A作为数据发布者,制定访问策略$T_{tp}=(w_1\wedge w_2\wedge w_4\wedge w_5)\vee(w_1\wedge w_3\wedge w_4\wedge w_5)\vee(w_2\wedge w_3\wedge w_4\wedge w_5)$,将访问策略$T_{tp}$嵌入主题$T$的数据中进行发布。$B$作为数据订阅者,属性密钥$S_{K_b}$可以匹配$T_{tp}$,因此能够解密主题$T$的消息。$C$作为数据入侵者,属性不满足信任条件,被阻止加入该系统的数据域中。D作为数据窃听者,获取了系统的读权限,试图窃听主题T的数据,但D的属性密钥S_{K_d}

表1 参与者属性对比

Table 1 Comparison of participant attributes

参与者	主题	类型	端口	域	读	写
A	T	red	6000	1	1	1
B	T	red	6000	1	1	0
C	P	red	7000	2	0	0
D	T	red	6001	1	1	0
E	P	red	7000	1	0	1

表2 各参与者仿真结果

Table 2 Simulation results of each participant

参与者	属性集	结果
A	$w_1\wedge w_2\wedge w_3\wedge w_4\wedge w_5\wedge w_6$	合法发布
B	$w_1\wedge w_2\wedge w_3\wedge w_4\wedge w_5$	合法订阅
C	w_2	被阻止加入
D	$w_1\wedge w_2\wedge w_4$	无法读取T
E	$w_2\wedge w_4\wedge w_6$	无法篡改T

不能匹配T_{tp},因此无法解密出主题T的数据内容。E作为数据篡改者,获取了系统的写权限,由于主题T只对应一种访问策略T_{tp},E的属性集不足以生成访问策略T_{tp},即使E试图将主题T的数据篡改为主题P的数据,其他订阅者也不会接受该内容。

经过实验验证,本文的方案可以有效地应对DDS存在的域分离未受保护、数据窃听、数据篡改3种安全威胁,保障系统数据的安全性。

4.3 开销分析

本节通过两种方式对本文方案的性能进行评估:(1)与文献的方案进行对比;(2)分析本文方案对DDS发布订阅系统的开销影响。

相关符号说明:P表示双线性对运算,E表示指数运算,H表示乘法运算,N_{at}表示属性个数,即叶子节点个数,N_{par}表示非根节点的父节点个数,m表示参与者满足解密需求的属性个数,x_1表示访问树优化后修剪的传输节点个数,x_2表示修剪的叶子节点个数。

由表3可以看出,通过访问树结构的优化以及添加属性信任计算去除冗余的属性后,本文的CPABE算法的加解密的计算性能相比于文献[14-15]的方案有了提升。

表3 计算性能比较

Table 3 Computing performance comparison

方案	加密	解密
文献[14]方案	$P+(N_{at}+1)E+N_{at}H$	$2N_{at}P+N_{par}E$
文献[15]方案	$N_{at}P+(3N_{at}+3)E+(N_{at}+2)H$	$(2m+2)P+mE+(2m+1)H$
本文方案	$P+(N_{at}+1-x_1)E+(N_{at}-x_2)H$	$(N_{par}-x_1)E+2(N_{at}-x_2)P$

图6,7为本文方案与文献[14]方案的加解密时间对比图。随着属性数量的增加,本文方案与文献[14]方案的加密时间都呈现线性增长。但本文使用优化后的访问树结构,相同属性个数情况下,比文献[14]的计算量小,加密时间短。解密算法性能有了显著提升,基本稳定在5 ms之内。

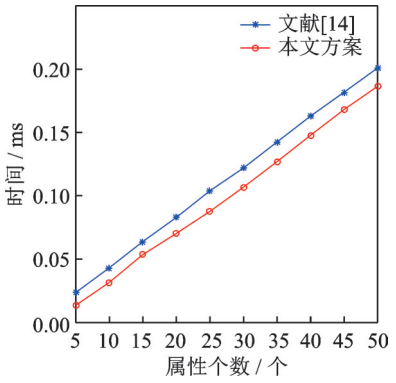

图6 加密时间对比

Fig.6 Encryption time comparison

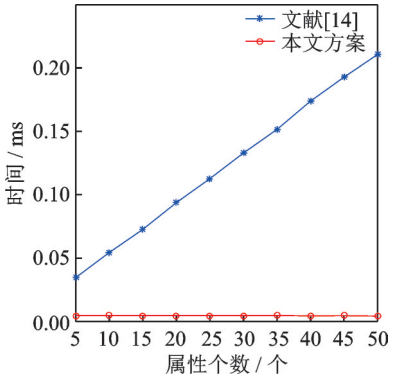

图7 解密时间对比

Fig.7 Decryption time comparison chart

本文优化后的CPABE方案有了一定的效率提升,原因在于影响加密算法的开销因素主要为访问树的叶子节点与传输节点个数,影响解密算法开销的因素为叶子节点中不同属性的个数和特定的访问树结构。通过对访问树结构的优化,增加属性信任阶段去除无关联的属性,并为属性制定权值,便于访问树的修剪以及门限值的合并操作。对访问树结构尽可能进行化简,减少了叶子节点与传输节点的个

数,从而降低加解密的计算量。

由表4可以看出,属性个数与属性密钥生成算法的开销成正比,属性信任计算的开销整体较小,属性个数对加解密算法的开销几乎没有影响。虽然keygen开销随属性个数线性增长,但在本文的方案中,属性密钥生成与更新在一个参与者进行发布订阅之前只调用一次,对于发布订阅的过程几乎没有任何影响。Trust的开销也随属性个数线性增长,而实际耗时在2 ms以内,且Trust算法在进行发布订阅之前只调用一次,对发布订阅过程影响较小。

由表5可以看出,访问树叶子节点个数与加密算法的开销成正比,在叶子节点个数为50以内的情况下,加密算法的开销对发布订阅过程的影响较小。叶子结点的个数不会影响解密算法的开销,而实际上,影响解密算法开销的因素为叶子节点中不同属性的个数和特定的访问树结构,无论访问结构与可用属性个数如何,解密算法的开销都比较小,通常都在5 ms左右。

表4 属性个数对访问控制各阶段算法的开销影响

Table 4 Impact of the number of attributes on the cost of the algorithm at each stage

属性个数/个	耗时/ms			
	Keygen	Trust	Encrypt	Dec
10	50	0.5	9.6	4.4
20	90	0.8	8.4	4.3
30	130	1.1	7.6	4.4
40	170	1.4	7.4	4.6
50	190	1.5	8.4	4.5

表5 访问树叶子节点对加解密开销影响

Table 5 Impact of the number of leaf nodes on the cost of encryption and decryption

叶子节点/个	耗时/s	
	Encrypt	Dec
10	0.043 1	0.007 6
20	0.082 8	0.004 5
30	0.121 9	0.004 5
40	0.162 7	0.004 4
50	0.200 1	0.004 3

综上所述,本文的方案在可控范围内,不会加大发布订阅系统的开销,能够确保DDS的实时性,具有良好的性能。

5 结束语

本文针对DDS数据分发服务在实际应用系统中存在的几种安全威胁,提出了一个以数据为中心的基于密文策略属性加密的机密性和访问控制方案,通过密文策略属性加密实现对DDS发布订阅的访问控制服务,可以确保实际发布订阅系统信息传输的机密性,实现安全细粒度的访问控制。同时,为了尽可能不影响发布订阅系统的实时性,通过优化的访问树结构减少加解密的计算开销,增加属性信任机制实现对参与者的属性认证及分配。方案不要求信息传输双方共享密钥,减少了密钥管理的开销。初步的分析和实验表明,本文的方案有可靠的安全性,在可控范围内不会影响发布订阅系统的性能。

参考文献:

[1] CASTELLOTE G P. OMG data-distribution service: Architectural overview[C]//Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops. Rhode Island, USA: IEEE, 2003: 200-206.

[2] MARISOL G V, JORGE D P, IMAD E T. Using DDS middleware in distributed partitioned systems[J]. ACM Sigbed Review, 2018, 14(4): 14-20.

[3] HE Z Y, LIANG Y. Study on the DDS network information security technology[J]. Applied Mechanics and Materials, 2015, 738-749: 1213-1216.

[4] 沈卓炜,高鹏,许心宇.基于安全协商的DDS安全通信中间件设计[J].信息网络安全,2021,21(6): 19-25.
SHEN Zhuowei, GAO Peng, XU Xinyu. Design of DDS secure communication middleware based on security negotiation[J]. Information Network Security, 2021, 21(6): 19-25.

[5] 甄超,邸海涛,郭秋丽.数据分发服务身份认证方法研究[J].电子技术,2015,44(6):44-48.
ZHEN Chao, DI Haitao, GUO Qiuli. Research on identity authentication method for data distribution service[J]. Electronic Technology, 2015, 44(6): 44-48.

[6] 李明娟,叶宏,王乐,等.面向高安全数据分发服务的身份认证协议设计[J].航空计算技术,2015,45(1):103-107.
LI Mingjuan, YE Hong, WANG Le, et al. Design of authentication protocol for high-security data distribution service[J]. Aeronautical Computing Technique, 2015, 45(1): 103-107.

[7] 陈开放.基于DDS舰载通信系统的信息安全分析研究[J].信息网络安全,2016,16(3):47-52.
CHEN Kaifang. Research on information security analysis based on DDS shipborne communication system[J]. Information Network Security, 2016,16(3): 47-52.

[8] 郭成,张洋.基于OpenFlow的发布/订阅系统的管理与安全[J].软件,2014,35(9):31-37.
GUO Cheng, ZHANG Yang. Management and security of publish/subscribe system based on Openflow[J]. Software, 2014, 35(9): 31-37.

[9] TARIQ M A, KOLDEHOFE B. Securing broker-less publish/subscribe systems using identity-based encryption[J]. IEEE Transactions on Parallel And Distributed Systems, 2014, 25(2): 518-528.

[10] PESONEN L I W, EYERS D, BACON J. Access control in decentralised publish/subscribe systems[J]. Journal of Networks, 2007, 2(2): 57-67.

[11] BELGUITH S, CUI S, ASGHAR M R, et al. Secure publish and subscribe systems with efficient revocation[C]//Proceedings of the 33rd Annual ACM Symposium on Applied Computing. New York, USA: Association for Computing Machinery, 2018: 388-394.

[12] BENALOH J, LEICHTER J. Generalized secret sharing and monotone functions[C]//Proceedings of Advances in Cryptology CRYPTO99. New York,USA: Springer,2000: 27-35.

[13] SOWJANYA K, DASGUPTA M. Secure ambient assisted living system using elliptic curve cryptography based CPABE[C]//Proceedings of 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). Kanpur, India : IEEE,2019: 1-7.

[14] ION M, RUSSELLO G, CRISPO B. Design and implementation of a confidentiality and access control solution for publish/subscribe systems[J]. ComputNet,2012,56(7): 2014-2037.

[15] ZHAO W, DONG X, CAO Z. A revocable publish-subscribe scheme using CP-ABE with efficient attribute and user revocation capability for cloud systems[C]//Proceedings of 2019 IEEE 2nd International Conference on Electronics and Communication Engineering (ICECE). Xi'an, China: IEEE,2019: 31-35.

作者简介:

任颖超(1997-),男,硕士研究生,研究方向:中间件技术,E-mail: ryc18018027175@163.com。

燕雪峰(1975-),**通信作者**,男,教授,博士生导师,研究方向:MBSE、军事智能、建模与仿真,E-mail: yxf@nuaa.edu.cn。

(编辑:陈珺)