卫星通信网中一种新的实体认证与访问控制方案

祝烈煌[1]，王龙[1]，李嘉盛[1]，张川[1]，原卫华[2]
（1. 北京理工大学计算机学院，北京 100081；2. 61345 部队，陕西 西安 710100）

摘 要：随着全球卫星通信需求的日益增长，卫星通信网的实体认证和访问控制问题亟待解决。为解决该问题，提出了一种多中心实体认证与跨域访问控制方案。该方案采用两级认证中心实现分层认证，此外，采用权限映射实现跨域访问控制。仿真实验表明，所提方案能够支持上亿实体的身份认证，并支持百万实体的并发访问。

关键词：身份认证；权限管理；访问控制；卫星通信网
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018103

New entity authentication and access control scheme in satellite communication network

ZHU Liehuang[1], WANG Long[1], LI Jiasheng[1], ZHANG Chuan[1], YUAN Weihua[2]
1. Computer Science, Beijing Institute of Technology, Beijing 100081, China
2. 61345 Army , Xi'an 710100, China

Abstract: With the increasing global demand for satellite communications, the problem of entity authentication and access control of the satellite communication network needs to be solved urgently. To solve this problem, a new multiple center-based entity authentication and cross-domain access control scheme was proposed. The scheme divided the multiple centers into two layers for entity authentication, and maped the authorization of the multiple domains to achieve access control. Simulation experiments show that the proposed scheme support the entity authentication for 100 million users. Furthermore, it also allows 1 million users to access in parallel.

Key words: identity authentication, authority management, access control, satellite communication network

1 引言

随着卫星技术和无线通信技术的不断进步和应用以及国家安全、航空航天、灾害预警等需求的日益紧迫，卫星通信网络作为重要的对应技术之一迅速发展[1]。卫星通信网络由多个骨干节点，如低轨卫星关口站、中轨卫星关口站、高轨卫星关口站、网络服务中心、低轨卫星、中轨卫星、高轨卫星、域认证中心及多种用户终端组成，重点实现按需服务能力。卫星通信网存在接入访问请求实体规模大、实体类型多等特点，导致传统的单中心实体认证与访问控制方案无法直接被应用。有别于传统网络，卫星通信网能实现全球通信，通信信道具有开放性的特点，信号发送地附近的所有用户在拥有一定设备的情况下都可以接收到信息，这就使接入实体更易遭受实体假冒、非授权访问、信息窃取、跨网攻击等安全威胁。

卫星通信网身份认证需满足多种接入请求实体及大量用户终端不间断使用，身份认证方案必须能够克服接入访问实体规模大、终端类型多样化、终端地域跨度大的问题。传统的身份管理方案分为松耦合解决方案、集中解决方案和代理解决方案。松耦合解决方案，一般就是通过填表的方式来实现单点登录，以实时同步的方式实现用户统一，这种

收稿日期：2017-10-27；**修回日期**：2018-03-22
基金项目：国家重点研发计划基金资助项目（No.2016YFB0800301）
Foundation Item: The National Key Research and Development Program of China (No.2016YFB0800301)

方案的特点是对现有系统影响较少，但是该方案容易形成访问瓶颈，当用户数量多时，需要使用多台服务器做集群[2]。集中解决方案主要采用集中式认证中心的方法，用户在登录时，统一到一个登录地址，在登录后，获得票据，然后以该票据登录各应用系统，这种方案服务器投入小，但是大多应用需要改动，维护不便[3]。代理方案部署认证代理在应用服务器上，通过安装代理，把认证服务器上的会话信息直接带给应用系统[4]，这种方案只支持某些特定的中间件，通用性较弱。综上所述，现有的身份管理方案均无法直接应用于卫星通信网的实体认证需求。

由于卫星通信网包含多种用户终端，不同的终端具有的功能也各不相同，且在卫星通信网中存在多个域，如移动、联通、电信等，因此对终端进行访问控制也是一个需要解决的难题。同一个用户终端在不同的域中具有不同的权限，因此，访问控制方案必须能够实现多种终端的权限管理，并满足用户终端的跨域访问需求。传统的权限管理模式主要有自主访问控制（DAC）、强制访问控制（MAC）和基于角色的访问控制（RBAC）。自主访问控制根据访问者的身份和授权来决定访问方式，访问主体对访问控制具有决定权，这种权利在信息移动的过程中很容易产生安全漏洞[5]。强制访问控制是系统将主体和客体分级，根据级别来决定访问模式，过于偏重机密性，不利于管理[6]。基于角色的访问控制是对前两者的改进，它基于用户在系统中的作用规定其访问权限，解决了管理难的问题，但是无法解决用户终端跨域访问的问题[7]。综上所述，传统的方案无法满足卫星通信网的访问控制需求。

针对卫星通信网中实体规模大、终端类型多的问题，本文设计了一种新的实体认证方案，建设一个主认证中心，并在每个域单独设立域认证中心，由主认证中心对低轨卫星关口站、中轨卫星关口站、高轨卫星关口站、网络服务中心、低轨卫星、中轨卫星、高轨卫星、域认证中心等关键节点进行 ID、密钥、IP 和 MAC 的管理。再由各域认证中心对各自域内的终端进行 ID、密钥、IP 和 MAC 的管理，按照两级管理的方式对所有访问请求实体进行管理。

针对卫星通信网中终端所属域多、权限复杂的特点，本文设计了一种新的访问控制方案，每个域分别管理自身终端，其中，不同终端具有不同的角色，按照角色确定其权限，在每个域分别建立分级跨域的属性协同映射表，当终端拜访域动态变化时，注册域首先确定终端角色，并根据角色确定终端在注册域的权限，注册域认证中心将终端权限信息发送到访问域认证中心，访问域认证中心根据权限映射表对权限进行动态映射，封装后返还注册域认证中心，完成用户终端的权限动态管理。

针对上述问题，本文基于卫星通信网提出一种新的实体认证及访问控制方案。

2 相关工作

本文对国内外的实体认证和访问控制方案进行调研并概述如下。

2.1 实体认证方案

王迎[8]提出了基于松耦合的身份认证系统。该系统在实现接入集成时比较容易，身份认证系统可以实现应用系统用户身份的统一管理，提高了用户身份管理效率与安全性，能够作为企业的基础应用。但是这种方案代码会分散在整个系统中，这种分散为管理和扩展带来不必要的困难。

孔强等[9]提出了一个用户集中管理的实体认证系统。该系统描述了基于角色的实体认证流程, 最后对授权管理基础设施系统与该文作者提出的系统做了对比，在一般的组织机构内部应用环境中使用，该系统可以提高管理效率和验证效率。但是该方案只能满足企业级用户使用，无法解决海量用户信息读取的问题。

Wullems 等[10]提出了一种基于公钥密码体制的认证方案。该方案将地面控制中心作为可信第三方，当某卫星节点与地面用户通信时，地面控制中心首先生成该卫星节点的一对公私钥。然后用控制中心的私钥对其签名（即用私钥对信息加密）后通过安全信道（用预共享密钥加密）发送给卫星。卫星通过验证控制中心的签名信息（即用控制中心的公钥解密）确保获得公私钥的真实性。最后卫星用自己的私钥对发送给用户的信息进行签名并广播自身公钥。该方案认证协议结构简单、可用性强，选择地面控制中心作为认证中心，可以发挥控制中心计算和存储能力强的优势，减轻了其他节点证书管理的负担。但是该方案由于用户终端并不直接与控制中心通信，因此用户端无法获取自己的公私钥，用户与卫星的认证关系仅限于单向认证。

2.2 访问控制方案

马康等[11]针对现有访问控制策略和机制复杂的特点，结合标签机制和多级安全的策略，以强制

访问控制为基础，提出了一种新的访问控制机制。该机制的思想是根据客体的访问密钥来最终决定主体对客体有何种访问权限。基于这种思想将访问控制策略和机制进行了设计，给出一种在 LSM（Linux 安全模块）框架下基于密钥对文件进行访问的策略实现方法。该访问控制方法将用户权限放置于密钥之中，用户权限容易被仿冒，安全性不够。

王永涛[12]提出了一个基于身份的多方密钥协商协议。该协议可用于多域访问控制中的密钥协商问题，即该协议解决了基于身份密码系统中处在不同域下的多个实体之间密钥协商问题，参与协商的实体不受某个域的限制，可以来自不同的域，随后给出了一种把原协议转化成广播协议的方案。但是该方案程序繁琐，无法满足大规模用户的日常使用。

3　卫星通信网中实体认证及访问控制模型

大规模实体认证与访问控制依据生成访问请求时认证中心、高轨卫星节点、低轨卫星节点、访问请求实体、域、资源、角色—权限分配等要素获取相应权限。从技术方案来看，实体身份及访问控制模型如图 1 所示。

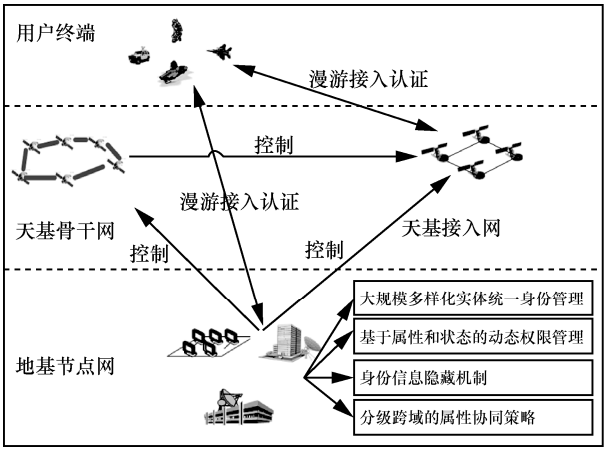


图 1　实体身份及访问控制模型

1) 认证中心

认证中心（IV）负责各接入实体的身份及权限管理，记为 $<n^{\mathrm{IV}},g^{\mathrm{IV}},s^{\mathrm{IV}},c^{\mathrm{IV}}>$，其中，$n^{\mathrm{IV}}$ 表示认证中心编号，为一个确定的认证中心；g^{IV} 表示网络服务系统的通用属性；s^{IV} 表示网络服务系统的安全属性；c^{IV} 表示网络服务系统的控制属性。设网络服务系统的数量为 IM，网络服务的集合记为

$$V=\{<n_i^{\mathrm{IV}},g_i^{\mathrm{IV}},s_i^{\mathrm{IV}},c_i^{\mathrm{IV}}>|\, n_i^{\mathrm{IV}}\in N^{\mathrm{IV}},\ g_i^{\mathrm{IV}}\in G^{\mathrm{IV}},s_i^{\mathrm{IV}}\in S^{\mathrm{IV}},c_i^{\mathrm{IV}}\in C^{\mathrm{IV}},i<IM\}$$

2) 高轨卫星节点

高轨卫星（GV）表示高轨卫星网络中的节点，记为 $<n^{\mathrm{GV}},g^{\mathrm{GV}},s^{\mathrm{GV}},c^{\mathrm{GV}}>$，其中，$n^{\mathrm{GV}}$ 表示高轨卫星编号，为一个确定的高轨卫星；g^{GV} 表示高轨卫星的通用属性；s^{GV} 表示高轨卫星的安全属性、加密类型；c^{GV} 表示高轨卫星的控制类型和管控信息。

3) 低轨卫星节点

低轨卫星（LV）表示低轨卫星网络中的低轨卫星，记为 $<n^{\mathrm{LV}},g^{\mathrm{LV}},s^{\mathrm{LV}},d^{\mathrm{LV}}>$，其中，$n^{\mathrm{LV}}$ 表示低轨卫星节点编号，唯一标识一个低轨卫星；g^{LV} 表示低轨卫星的通用属性；s^{LV} 表示的是低轨卫星的安全属性、加密类型；d^{LV} 表示低轨卫星的受控类型，如姿态控制、轨道控制、动力控制等。

4) 访问请求实体

资源访问的发起方为接入网络的请求实体（Q），记为 $<u^{Q},a^{Q},s^{Q},r^{Q}>$，其中，$u^{Q}$ 表示用户的唯一身份标识；a^{Q} 表示访问终端的唯一标识；s^{Q} 表示实体的安全信息；r^{Q} 表示实体的角色信息。

5) 域

资源访问请求实体在发起访问请求时接入网络系统所属域为 L。接入系统通过域标识区分不同访问，域标识记为 $l=<i^{L},p^{L},w^{L}>$，其中，i^{L} 表示接入点所属域 $i^{L}\in I^{L}$；$p^{L}=<x\ y,z>\in P^{L}$ 表示三维空间位置坐标，例如，x 表示经度，y 表示纬度，z 表示高度；$w^{L}\in W^{L}$ 表示网络接入唯一标识，如 MAC、IP 等。

6) 资源

访问的对象资源（O）记为 $<c^{o},g^{o},s^{o}>$，其中，$c^{o}\in C^{o}$ 表示资源的内容；$s^{o}\in S^{o}$ 表示资源的通用属性，指资源的类别、来源等属性；$g^{o}\in G^{o}$ 表示资源的安全属性，指资源允许执行的操作、是否允许转发、销毁方式等。

7) 角色—权限分配

角色—权限分配方案（RP），指对资源访问角色 r 分配权限 p 的过程，rp 的集合记为 RP。

在该系统模型中，主认证中心（IV）对卫星及关口站进行密钥分发时，根据密钥分发协议 $C^{\mathrm{IV}_{ks}}$ 将生成的密钥 $s^{Q_{pw}}$ 发送给卫星、关口站，对原有密钥进行更新。访问请求实体 Q 在所属域 L 进行注册，

提交实体信息，所属域需根据用户的角色 R 为其分配不同的权限 P。

当访问请求实体 Q 通过网络向系统提出资源 O 的访问请求时，系统在得到访问请求的同时对实体请求进行认证，确定实体 Q 的角色 R，再通过角色 R 确定权限 P。角色确定的权限为 $RP \subseteq R \times P$，根据接入点的所属域 L 确定的权限为 $LRP \subseteq L \times RP$，服务器判断用户权限 P 是否与域下角色权限 LRP 相符合[13]。若相符，则该次访问请求被允许，否则访问请求被拒绝。以 p''表示发起访问请求的某个特定的实体则会话 se 具有权限 $U_{rp \in r(se_t)}\{p \mid (q'', p) \in LRP]\}$。

4 卫星通信网中实体认证与访问控制方案

实体认证与访问控制方案分为实体身份管理和分级跨域的动态权限属性协同映射 2 种子方案。

4.1 实体身份管理子方案

卫星通信网需要支持低轨卫星关口站、中轨卫星关口站、高轨卫星关口站、网络服务中心、高轨卫星、低轨卫星等骨干节点和多种用户终端的统一身份管理。各骨干节点与用户终端所具有的功能与管理模式完全不同，对其进行统一管理的技术难度很大。如果采用传统的用户管理方式，动辄需要存储十亿甚至百亿的数据，对用户信息进行一次比对的时间开销巨大，必然会对用户的认证带来较大时延。

因此，本文方案采用一个主认证中心负责各骨干节点的管理，在各域分别建设域认证中心对所属终端进行管理的模式，并对骨干节点和用户终端进行区分化管理。针对亿级用户和多样化网络实体的身份标识管理的难题，为了解决终端信息存储数据量大、查询时延长的问题，本文方案通过建立分域索引方法对用户及终端数据进行管理，如图 2 所示。

实体统一身份管理技术方案如图 3 所示。为了实现实体统一身份及权限管理，首先由主认证中心对所有低轨卫星关口站、中轨卫星关口站、高轨

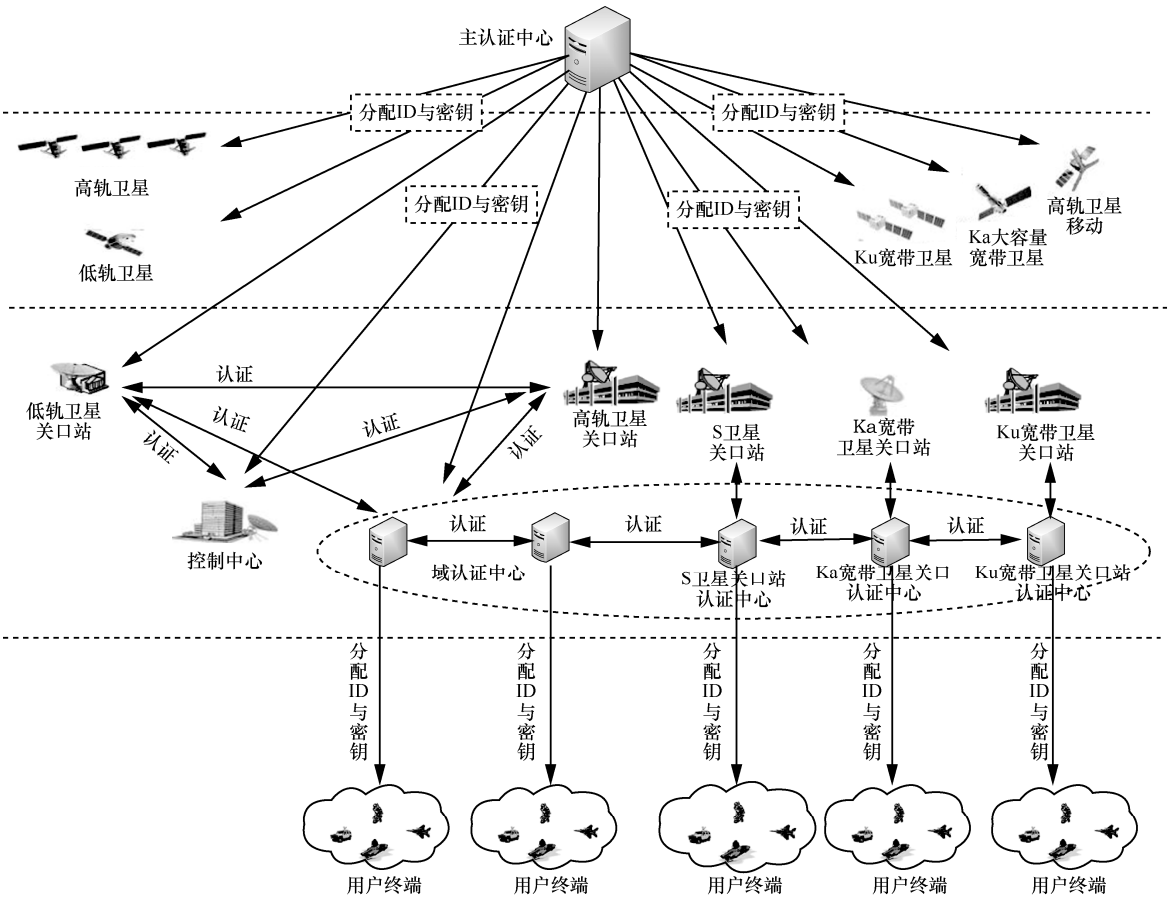


图 2 实体身份管理架构

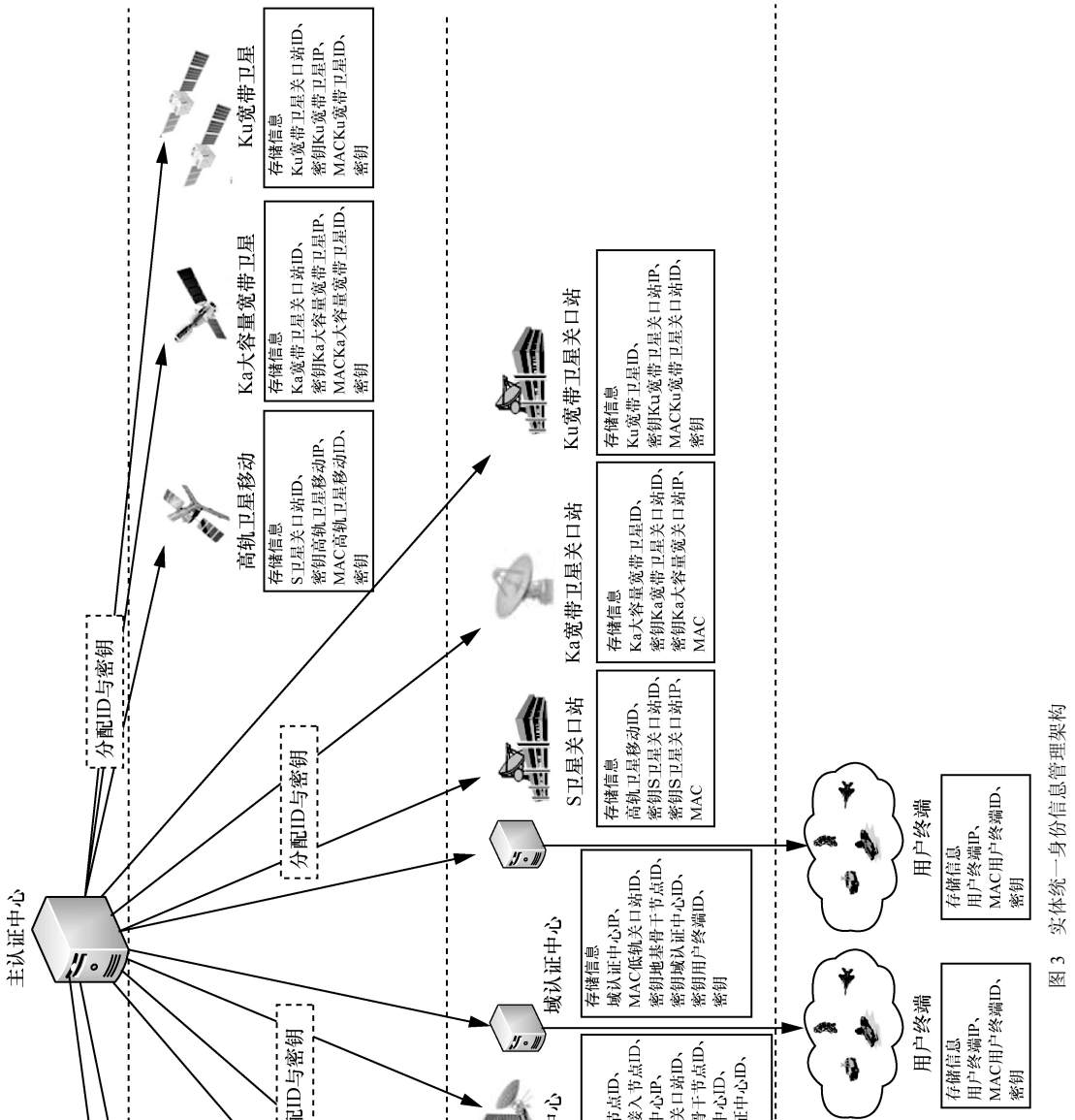


图 3　实体统一身份信息管理架构

卫星关口站、网络服务中心、高轨卫星、低轨卫星等骨干节点进行 ID、密钥、IP 和 MAC 的分发和管理。当骨干节点需要进行身份信息更新时，由主认证中心重新生成并发布到骨干节点，对原有身份信息进行更新。各域认证中心为所属域用户终端进行 ID、密钥、IP 和 MAC 的分发和管理，实现用户及终端身份的细致化管理。对所有用户及终端进一步细化存储表，最终采用索引表和数据表联合查询的方式缩减实体信息的查询时间，有效降低各认证中心的数据压力和维护难度，并保证信息的安全传输。

4.2 分级跨域的动态权限属性协同映射子方案

为了实现动态权限管理，本文方案采用基于角色的访问控制方式，为每个域认证中心分别设置角色与权限对应表。系统在维护时只需对角色权限进行变更就可实现所有该角色实体的权限更新，只需对某个权限进行变更就可以实现所有具有该权限的角色的权限更新。每个实体可以拥有多个角色，根据实体所属场景确定当前角色，最终通过角色确定实体权限。以超级管理员、高级用户、普通用户为例则动态权限管理如图 4 所示。

为了实现分级跨域的属性协同映射，对不同域的权限等级进行协同映射，即在每个域建立权限跨域映射表，将其他域的权限与自身域的权限进行映射。当用户终端的访问域不是注册域时，访问域认证中心首先将用户终端访问请求发送给注册域认证中心，注册域查询确认用户终端角色，进而确定用户终端在注册域的权限，将用户终端的注册域权限信息进行封装后加密发送到访问域认证中心，按照权限跨域映射表进行映射，查询确认用户终端在访问域的权限。以超级管理员、高级用户、普通用户为例则分级跨域的属性协同映射架构图如图 5 所示。

5 性能分析

模拟实验使用了包括压测工具 loadrunner、MySQL 数据库服务器、Web 服务器等对提出方案进行压力测试。服务器采用 32 核 CPU、140 GB 内存、万兆网卡。在一台服务器上部署 loadrunner，模拟用户请求，把用户请求发送到 Web 服务器上，由该服务器来处理用户 HTTP 请求，并由 Web 服务器获取数据库服务器数据。

在数据库服务器添加用户，采用目录表查询的

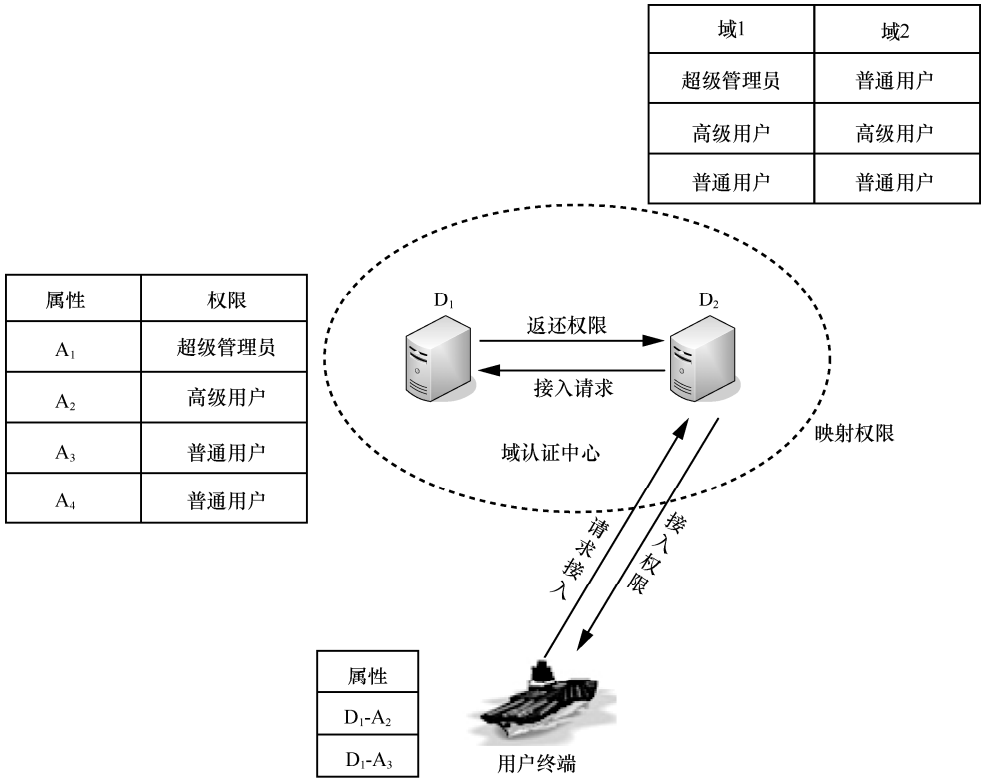


图 4 动态权限管理

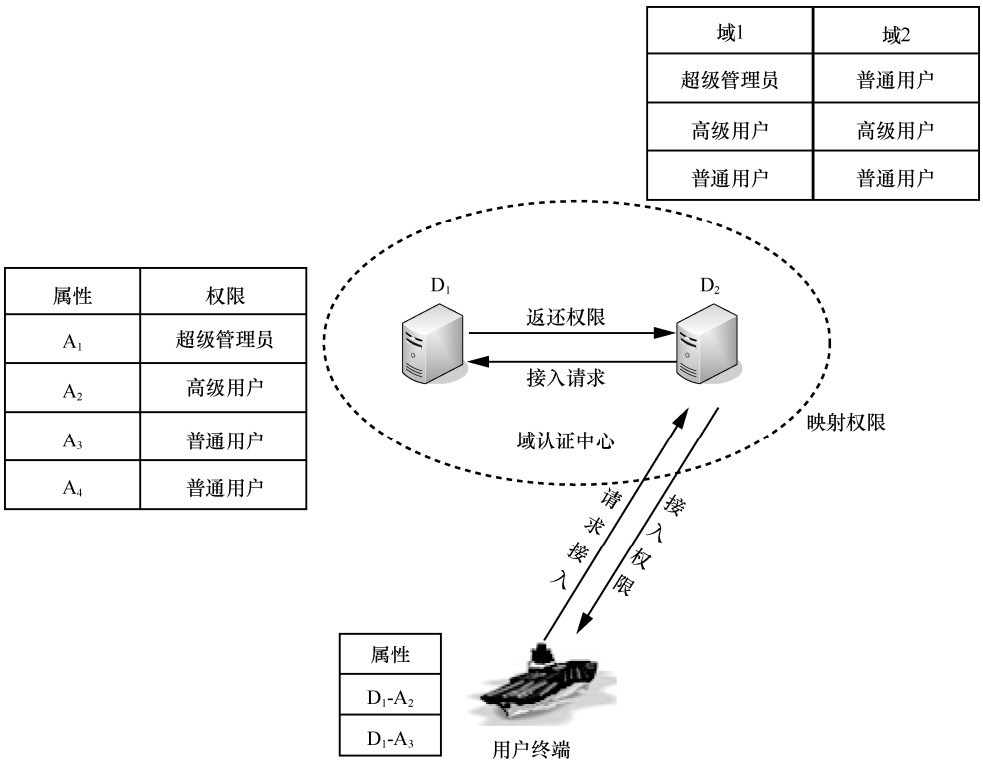


图 5　分级跨域的属性协同映射

方式进行用户信息存储，由目录表存储每个表的特征信息和对应的表信息，每个用户表存储 1 万用户，500 个表共计存储 500 万用户。

数据库服务器将用户数据存储在内存中进行操作，以提高数据读取速度，压力测试服务器使用 loadrunner 工具模拟 6.5 万个虚拟用户队服务器发出认证请求。测试计划配置为每秒启动 50 个虚拟用户，当虚拟用户数达到 6.5 万时进行 2 min 的并发保持，而后每秒释放 100 个用户请求，完成整个压力测试过程。实验结果如图 6 所示。

由图 6 可知，系统在 42 min 内并发用户数稳定提升，到 42 min 后开始维持在 6.5 万虚拟用户同时并发，且性能保持稳定。为了保证实验结果的可靠性，本文对虚拟用户请求重复次数进行分析，实验结果如图 7 所示。

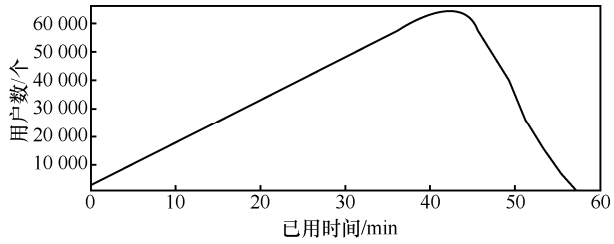


图 6　并发请求实验

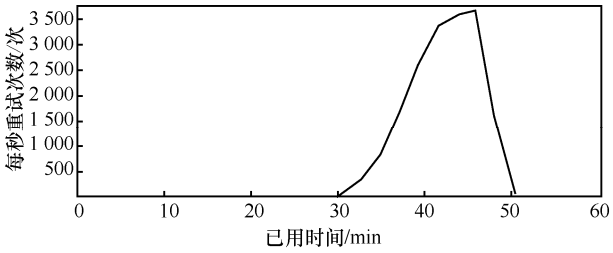


图 7　虚拟用户重复请求实验

由图 7 可知，系统在 30 min 出现重复请求，32 min 重复请求数量急速提高，重复请求数量过高会影响到用户的使用体验，每台服务器保持在 5 万并发时可以保证较好的用户体验，且性能保持稳定。

6　结束语

为了解决亿级用户实体认证管理和多样化实体权限管理，本文提出一种新的实体认证与访问控制方案。本文方案采用主认证中心和域认证中心两级管理的方式来进行实体的身份认证，采用基于角色跨域权限映射的方式解决多样化接入实体的权限跨域管理，整个系统由 20 台服务器共同提供服务即可满足上亿用户的身份和权限管理及百万并发的需求。

参考文献：

[1] 李凤华, 殷丽华, 吴巍, 等. 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报, 2016, 37(11): 156-168.
LI F H, YIN L H, WU W, et al. Research status and development trends of security assurance for space-ground integration information network[J]. Journal on Communications, 2016, 37(11):156-168.

[2] 徐振亚. 一种基于 SOA 架构的统一身份认证系统的研究及实现[D]. 上海: 上海交通大学, 2007.
XU Z Y. Research and implementation of a unified identity authentication system based on SOA architecture and implementation[D]. Shanghai : Shanghai Jiao Tong University, 2007.

[3] 刘雪晖, 尹超, 何彦, 等. 网络化制造集成平台集中式身份认证策略研究[J]. 计算机集成制造系统, 2005, 11(6): 885-890.
LIU X H,YIN C,HE Y, et al. Centralized identity authentication strategy in networked manufacturing integrated platform[J].Computer Integrated Manufacturing Systems,2005, 11(6): 885-890.

[4] 孙超, 陈钢. 基于 Agent 技术的统一身份认证系统[J]. 计算机应用研究, 2005, 22(3): 138-140.
SUN C, CHEN G. Uniform identity authentication system based on Agent technologies[J]. Application Research of Computers,2005, 22(3): 138-140.

[5] 顾少慰, 梁洪亮, 李尚杰, 等. 一种增强的自主访问控制机制的设计和实现[J]. 计算机工程与设计, 2007, 28(8): 1781-1784.
GU S W, LIANG H L, LI S J, et al. Design and implementation of enhanced discretionary access control mechanism[J]. Computer Engineering and Design,2007, 28(8):1781-1784.

[6] 李立新, 陈伟民, 黄尚廉. 强制访问控制在基于角色的安全系统中的实现[J]. 软件学报, 2000, 11(10): 1320-1325.
LI L X, CHEN W M, HUANG S L. Realizing mandatory access control in role-based security system[J]. Journal of Software,2000, 11(10): 1320-1325.

[7] 李孟珂, 余祥宣. 基于角色的访问控制技术及应用[J]. 计算机应用研究, 2000, 17(10): 44-47.
LI M K, YU X X. Technique and application of role-based access control[J]. Application Research of Computer,2000, 17(10):44-47.

[8] 王迎. 统一身份认证在企业信息化中的应用研究[J]. 计算机光盘软件与应用, 2015(2):109-110.
WANG Y. Application of unified authentication in enterprise informationization[J]. Computer CD Software and Applications, 2015(2): 109-110.

[9] 孔强, 李学农, 伊里. 用户集中管理和访问控制系统的设计实现[J]. 计算机应用与软件, 2007, 24(2): 75-78.
KONG Q, LI X N,YI L. Design and implementation of a principal integrated administration and access control system[J]. Computer Applications and Software, 2007, 24(2):75-78.

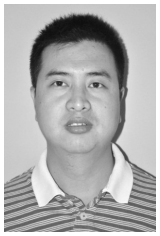
[10] WULLEMS C, POZZOBON O, KUBIK K. Signal authentication and integrity schemes for next generation global navigation satellite systems[C]//European Navigation Conference. 2005:1.

[11] 马康, 陈松政. 基于密码的访问控制研究[J]. 计算机应用研究, 2012, 29(1):305-307.
MA K, CHEN S Z. Research on cryptography based access control[J]. Application Research of Computers,2012, 29(1):305-307.

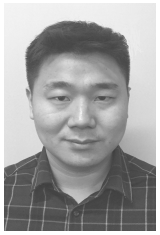
[12] 王永涛. 基于身份的密码体制的密钥管理方案研究[D]. 成都: 西华大学, 2007.
WANG Y T. Research on key management scheme of identity - based cryptosystem[D]. Chengdu: Xihua University,2007.

[13] 李凤华, 王彦超, 殷丽华, 等. 面向网络空间的访问控制模型[J]. 通信学报, 2016, 37(5): 9-20.
LI F H, WANG Y C, YIN L H, et al. Novel cyberspace-oriented access control model[J]. Journal on Communications,2016, 37(5):9-20.

[作者简介]

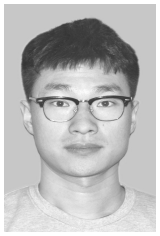


祝烈煌（1976-），男，浙江衢州人，博士，北京理工大学教授、博士生导师，主要研究方向为密码算法及安全协议、天地一体化网络安全、物联网安全、云计算安全、大数据隐私保护、移动互联网安全、可信计算。



王龙（1988-），男，河北衡水人，北京理工大学硕士生，主要研究方向为天地一体化网络安全、移动互联网安全等。

李嘉盛（1995-），男，天津人，北京理工大学硕士生，主要研究方向为信息安全。



张川（1991-），男，河北邯郸人，北京理工大学博士生，主要研究方向为天地一体化网络安全、物联网安全、云计算安全。

原为华（1988-），男，陕西蒲城人，61345部队助理工程师，主要研究方向为光有线通信网络。